



## **ClearVision Management System User's and Administrative Guide**

Version 3.0

### **Americas Headquarters**

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

Text Part Number:



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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

ClearVision Management System User's and Administrative Guide  
© 2012 Cisco Systems, Inc. All rights reserved.



**Chapter 1: ClearVision Introduction**

TR-069 Overview .....	1
What is TR-069? .....	1
How does TR-069 relate to ClearVision? .....	2
User Roles .....	2
Licensing .....	2

**Chapter 2: System Overview**

System requirements .....	3
Logging in and out of ClearVision .....	4
User Profile .....	5
Automatically refreshing device data .....	5
Viewing system messages .....	5
Logging out .....	5
Navigation overview .....	6
Dashboard overview .....	7
System messages overview .....	8
Viewing system messages .....	8
Labels overview .....	9
What are labels? .....	9
Using labels in ClearVision .....	9
Domains overview .....	10
Scripts overview .....	10
What is a script? .....	10
What can scripts do? .....	10
How do scripts run? .....	11

**Customer Support Representative Tasks****Chapter 3: Customer Support Overview**

Searching for and selecting subscribers and devices .....	14
How to search .....	15
Selecting subscribers or devices .....	16
Applying labels to multiple records .....	16
Creating new accounts .....	17
About saving changes .....	20

**Chapter 4: Working with Accounts**

Displaying an account .....	22
What happens when you display an account .....	23
Working with subscribers .....	23
Managing subscriber information .....	23
Identification information .....	23
Address and phone information .....	24
Managing control panel access .....	24
Managing subscriber labels .....	25
Deleting a subscriber .....	25
Managing devices .....	26
Assigning a device alias and icon .....	27



Working with device labels .....	27
Viewing device information .....	28
Rebooting a device.....	28
Adding and removing PPP credentials.....	28
Enabling or disabling bulk operations.....	29
Accessing and managing the control panel .....	29
Assigning the device to a domain .....	30
Removing the association between a device and a subscriber .....	30
Deleting a device .....	30
Managing the local network .....	31
Viewing local network status .....	31
Working with LAN devices .....	32
Viewing device status.....	33
Status .....	33
Line information.....	33
DSL or cable.....	34
WAN Interface statistics .....	34
<b>Chapter 5: Working with Services</b>	
Managing wireless settings.....	35
About wireless settings .....	36
Enabling and disabling wireless service .....	37
Managing port forwarding .....	38
Enabling and disabling port forwarding .....	38
Managing port forwards.....	39
Managing content filtering.....	40
About content filtering levels .....	41
How content filtering works .....	42
Examples .....	43
Enabling and disabling content filtering.....	44
Managing default content filtering settings .....	44
Managing content filtering for specific LAN devices.....	45
Managing time blocking.....	46
Enabling and disabling time blocking.....	46
Managing default time-blocking settings .....	47
Manage time blocking for specific devices .....	47
Adding bonus time.....	48
<b>Chapter 6: Performing Advanced Tasks</b>	
Working with event logs.....	51
About event logs .....	52
About event logging levels .....	53
Using the parameter browser .....	53
Managing device synchronization .....	55
Understanding synchronization status .....	55
Working with scripts .....	56
About scripts.....	56
Upgrading firmware.....	58



Replacing a device .....	59
Setting up local GUI access .....	60
<b>Chapter 7: Reports</b>	
About reporting .....	62
About included reports .....	63
About custom reports .....	63
Running existing reports .....	63
Creating custom reports .....	66
Working with sort order .....	68
Working with filters .....	68
Applying parameters .....	69
Editing parameters .....	69
Using Boolean logic .....	70
Working with Advanced Syntax .....	70
Running aggregate reports .....	71
Using Reports to understand your network .....	72
<b>Administrator Tasks</b>	
<b>Chapter 8: Administration Overview</b>	
Managing labels .....	76
Using the Label Editor .....	77
Managing users .....	78
Using the User Editor .....	79
Managing device types .....	80
Using the Device Type Editor .....	81
Managing firmware versions .....	82
Using the Firmware Editor .....	83
Managing services .....	84
Managing user interface groups .....	85
Using the Service Editor .....	86
Managing scripts .....	90
Using the Script Editor .....	92
Managing events .....	93
Using the Event Editor .....	94
Managing announcements .....	95
Using the Announcements Editor .....	96
<b>Chapter 9: Reviewing Audit Logs</b>	
<b>Chapter 10: Managing bulk operations</b>	
Creating bulk operations .....	100
Examples for bulk operations .....	100
Scenario: Update Firmware on All SR100G CPEs .....	100
Viewing bulk operation progress .....	103
Scenario: Enable Content Filtering on all CPEs .....	104
Best practices for working with bulk operations .....	106
Preparing for Bulk Operations .....	106
Troubleshooting failed bulk operations .....	106



---

Controlling maximum throughput/throttling .....	107
Preparing to run firmware update operations.....	108
Understanding bulk operation options.....	108
About Action options .....	109
About schedule options .....	109
About CPE selection options.....	110
<b>Chapter 11: Using Utilities</b>	
Utilities overview .....	111
Importing subscriptions .....	112
Using the RESTful service tool.....	113
<b>References</b>	
<b>Appendix A: Glossary</b>	
<b>Appendix B: Subscription Import File Format</b>	
Sample CSV file .....	118



# ClearVision Introduction

---

---

[TR-069 Overview 1](#)

---

[User Roles 2](#)

---

[Licensing 2](#)

---

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

This manual assumes familiarity with standard networking terms and procedures in the telecommunications industry.

## TR-069 Overview

### What is TR-069?

**TR-069** is a technical report published by the Broadband Forum which defines the CPE WAN Management Protocol (CWMP). The CWMP defines the application layer for remote management of end-user devices and is used by ClearVision 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 ClearVision. 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 ClearVision?

ClearVision is an Enterprise Application that manages and monitors TR-069 compliant subscriber devices. This system 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 have the ability to modify, create, and run actions based on CPE related events. ClearVision fills a critical need for cutting-edge Internet Service Providers.

## User Roles

Currently, ClearVision includes three roles that you can apply to a user account.

**Admin.** An admin account allows access to all the functions in ClearVision, except those limited by license settings.

**Customer Support Representative.** A customer support representative (CSR) can manage individual device and subscriber records.

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

	Customer Support	Admin
Customer Support	X	X
Dashboard		X
Administration		X
Audit		X
Bulk Operations		X
Reports		X
Utilities		X

**Note.** ClearVision is highly configurable. ClearVision administrators can assign access to tasks and parts of tasks to Admin or CSR roles. If a task in this manual is not available to you, ask your system administrator.

## Licensing

The content in this manual is subject to your licensing agreement with Cisco. You may not have access to all features and sections of ClearVision. 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.



## Chapter 2

# System Overview

---

---

[System requirements](#) 3

---

[Logging in and out of ClearVision](#) 4

---

[User Profile](#) 5

---

[Navigation overview](#) 6

---

[Dashboard overview](#) 7

---

[System messages overview](#) 8

---

[Labels overview](#) 9

---

[Domains overview](#) 10

---

[Scripts overview](#) 10

---

## System requirements

To access ClearVision, use one of these browsers:

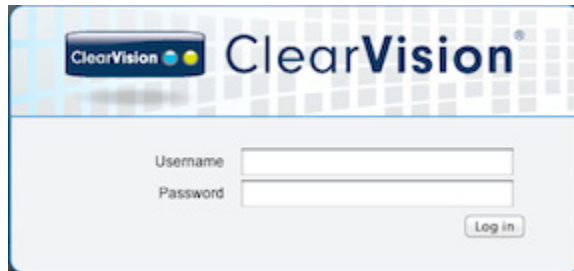
- [Chrome<sup>†</sup>](#) (recommended)
- [Internet Explorer version 8.0 or higher<sup>†</sup>](#)
- [Firefox<sup>†</sup>](#)
- [Safari<sup>†</sup>](#)



## Logging in and out of ClearVision

To log into the system

- 1 Go to the ClearVision URL. The login screen displays.



- 2 Enter your username.
- 3 Enter your password.
- 4 Click Log in.

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

---

**Note.** Both the login name and password are case sensitive.

---

Contact your system administrator for assistance if you cannot recall your username or password or receive an error message.

---

**Note.** Your system may have a set limit of session logins per license. If you have exceeded the amount of simultaneous logins, the message “The maximum number of users are already logged into the system. Another user must log out before you can log in,” may appear on the screen. You must either wait until another user logs out or request that a user log out for you to use ClearVision.

---

To log out of the system

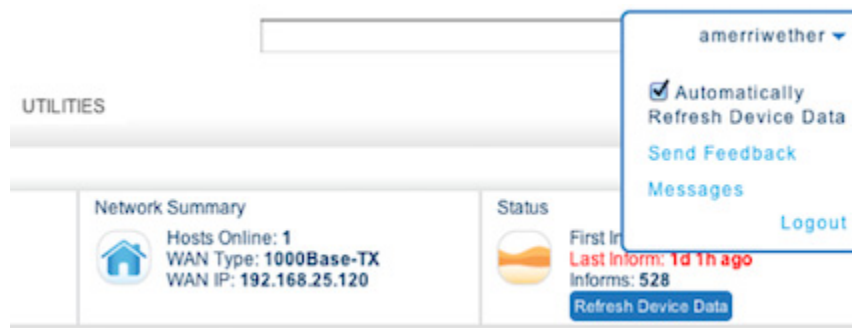
- 1 In the upper right corner of the page, click your username to display the user profile panel.
- 2 Click Logout.



## User Profile

Your user profile enables you to set an option to automatically refresh device data, view system messages, and log out of ClearVision.

To view the user profile, click your user name.



## Automatically refreshing device data

If you set the option to automatically refresh device data, viewing an account immediately polls the device and refreshes the display with the latest data from the device.

If you clear the option to automatically refresh device data, you must explicitly refresh the data by clicking the Refresh Device Data button.

Refreshing data takes time. If refreshing slows you down, you may want to clear this option.

ClearVision stores your selection in a browser cookie. You will need to reset your preference if you use a different computer.

## Viewing system messages

To view recent system messages, click [Messages](#).

## Logging out

To log out, click [Logout](#).



## Navigation overview

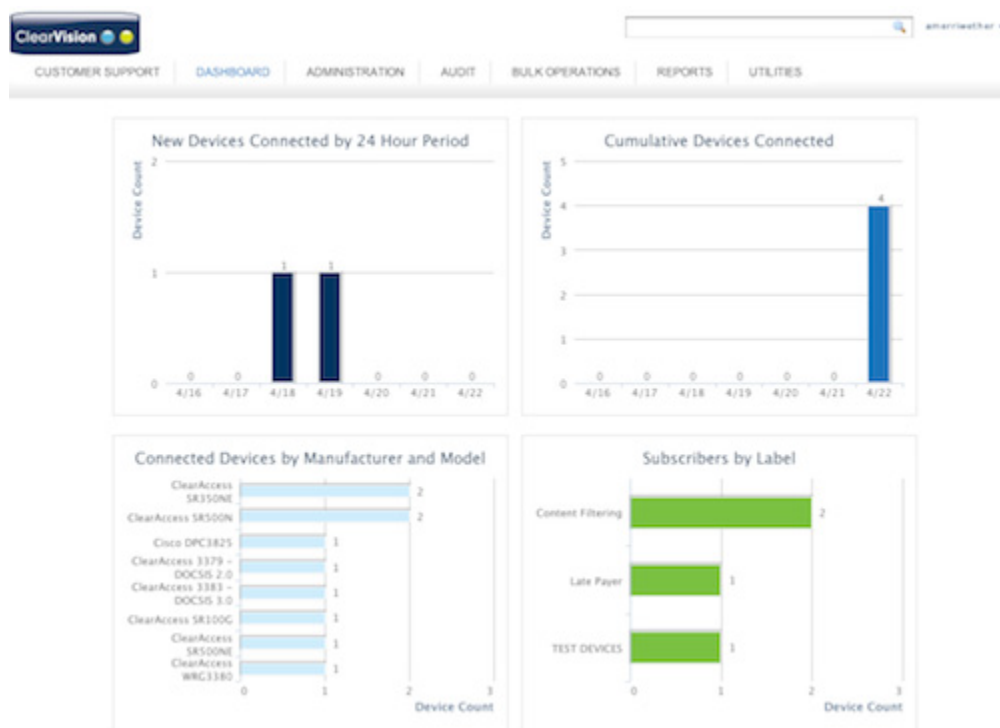
The Navigation tabs allow access to all of the features in ClearVision. The tab bar appears at the top of every page. The tabs that you see depend on your user role. The navigation area also enables quick access to system messages and a link to log out of the system.

The screenshot shows the ClearVision interface. At the top is a navigation bar with tabs: CUSTOMER SUPPORT, DASHBOARD, ADMINISTRATION, AUDIT, BULK OPERATIONS, REPORTS, and UTILITIES. Below the navigation bar is a search bar labeled "Find Subscriber or Device:". Below the search bar is a button labeled "Create New Subscriber/Device". Below the button is a table with columns: Subscriber Name, Subscriber Code, Email, Device Alias, Manufacturer, Model, Serial Number, WAN IP, Last Inform, Subscriber Labels, Device Labels, and Domain. The table contains 10 rows of data. At the bottom of the table is a pagination bar showing "View 10 per page" and "Page 1 of 2".

Subscriber Name	Subscriber Code	Email	Device Alias	Manufacturer	Model	Serial Number	WAN IP	Last Inform	Subscriber Labels	Device Labels	Domain
test	11111111	test@clearaccess.com	—	ClearAccess	WRG3380	001018801A68	192.168.51.136	52 minutes 11 seconds ago	TEST DEVICES	new	
Alice Merriwether	87654321	alicemerry@mac.com	—	ClearAccess	SR100G	00255E6E05EE	10.1.1.137	1 hour 29 minutes ago	Content Filtering		Domain One
Bhaskar Aluru	BA-B	baluru@clearaccess.com	—	ClearAccess	SR350NE	80A1D71EB0A4	10.1.1.98	1 hour 32 minutes ago	Late Payer		
newtest	33333333	newtest@clearaccess.com	—	ClearAccess	3383 - DOCSIS 3.0	0010188AF0F0	192.168.51.131	4 hours 25 minutes ago			
newtest	33333333	newtest@clearaccess.com	—	ClearAccess	3379 - DOCSIS 2.0	00101879F9C4	192.168.51.151	1 day 12 hours ago		TEST DEVICES	
Chris Divine	5035551212	cdvine@clearaccess.com	—	ClearAccess	SR500NE	80A1D7009D98	192.168.25.120	1 day 20 hours ago	Content Filtering		Domain Three
test	11111111	test@clearaccess.com	—	ClearAccess	SR350NE	80A1D7EE0879	192.168.51.241	2 days 8 hours ago	TEST DEVICES		
Chris Divine	5035551212	cdvine@clearaccess.com	—	Cisco	DPC3825	0022CE98BBA3	192.168.25.119	7 days 20 hours ago	Content Filtering		Domain Three
—	—	—	—	ClearAccess	SR500N	80A1D700965E	—	14 days 13 hours ago			
ssadasivam	12345677	ssadasivam@clearaccess.com	—	ClearAccess	SR500N	00255E71F5C9	192.168.51.250	16 days 12 hours ago			

## Dashboard overview

The Dashboard tab displays a summary of recent activity.





**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.

**Subscriber by Label.** The top six labels on the connected devices.



## System messages overview

ClearVision displays three types of messages: information, warnings, and errors. Each message includes an icon to easily identify it. System messages appear in the background, which means that the system constantly logs messages and does not ask you to act upon them.



**Information messages.** These messages display user feedback. For example, if a script enters the queue successfully, the system displays a message of "Script successfully added."



**Warning messages.** These messages display 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.

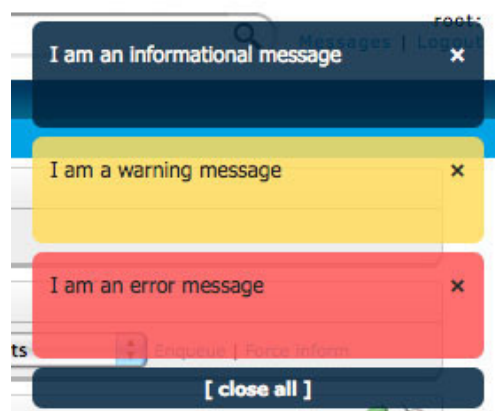


**Error messages.** These messages display when something fails. For example, if a script fails to run, the system returns an error message.

## Viewing system messages

There are two ways to view system messages. Messages appear either as instant notifications on the screen or as a log file in a pop-up window. Instant messages appear directly on the browser window in the right hand corner. They display the most recent activity recorded by the system. ClearVision color codes the three types of messages so you can quickly distinguish between the types of information the system displays for you.

Instant message windows appear similar to the following:



Instant messages only appear in the window for a few seconds and then they disappear. To access a record of all recent messages contained in the system, click the [Messages](#) link In your User Profile.

A pop-up window displays the messages. To close the pop-up window, click the close link in the upper right hand corner or press the ESC key.



## Labels overview

### What are labels?

Labels give you a flexible, customizable, and personal system to categorize elements in your system. You can apply labels to devices, subscribers, firmware, users, scripts, events, and announcements.

ClearVision enables you to create your own labels. You can think of a label as a digital bucket that you can put related items into. This label keeps 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 one or more devices or subscribers.

For example, you can create a label that groups all devices located in the same region together. 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 in ClearVision

You can use labels to do the following:

- Group devices, subscribers, or users together so you can find them more easily.
- Use them in conjunction with bulk operations. Use the labeling facility to further restrict devices to a particular operation.
- Apply them within 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.
- Use the search field to search for labels. If you type in the label name, everything that has that label will appear.

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

## Domains overview

You can assign devices, subscribers, or 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 may have a domain for each region.

CSR users who are assigned to one or more 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

### What is a script?

Scripts are implemented using a customized JavaScript-based environment which runs on the ACS. This environment supports complete manipulation of the customer premise equipment (CPE) via TR-069, as well as access to data models for subscribers and devices stored locally on the Automated Configuration Server (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 two primary types are:

**Scheduled scripts.** Scripts designed to run at specific times.

**Event-based scripts.** Scripts designed to run when a specific event occurs, such as an inform or reboot.

### What can scripts do?

Here are some things that scripts can do:

- Read and write device configuration parameters.
- Read and write subscriber information, such as phone number, physical address, IP address, and billing info.
- 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.

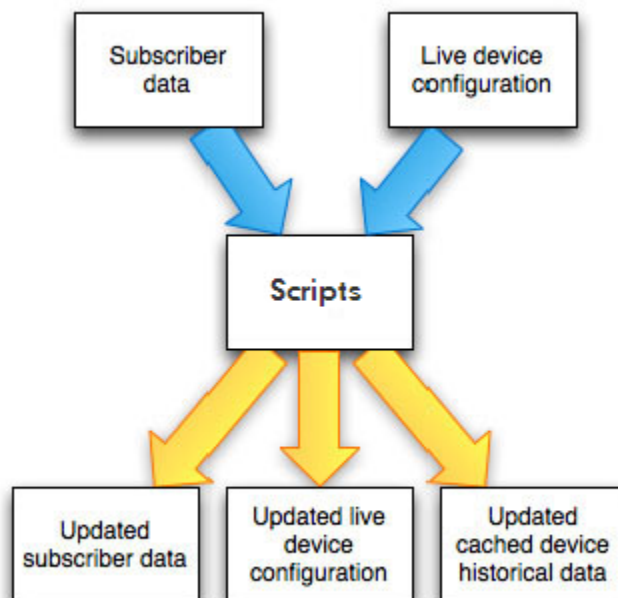


## How do scripts run?

Scripts get executed in one of four ways. These are:

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

After being put into a script queue, the script gets executed by the server. When the device checks in (either from its normal schedule or by an apply now request), the script gets applied to the device.



Scripts can enter the queue in one of three ways:

- Directly (via the Scripts pane and/or using the search results to apply to a batch of devices)
- Through bulk operations
- On a defined event, such as first connect or rebooting



---

## **Customer Support Representative Tasks**



# Customer Support Overview

---

---

[Searching for and selecting subscribers and devices](#) 14

---

[Applying labels to multiple records](#) 16

---

[Creating new accounts](#) 17

---

[About saving changes](#) 20

---

The Customer Support tab provides a central location for Customer Support Representatives to manage subscribers and devices. This chapter provides an overview of the Customer Support tab and explains how to work with subscribers and devices. Here are the customer service tasks you can perform:

- 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 of the tasks described in this section may be restricted to users assigned the Admin role. The tasks available to you depend on how your ClearVision installation is configured.

---



## Searching for and selecting subscribers and devices

Before you can view or make changes to a subscriber or device, you need to locate the item in the ClearVision database. ClearVision provides robust searching capabilities to help you locate information.

Once you have located all subscribers or devices that meet the search criteria, you can select one or more of them to operate on.

You can search for several different kinds of subscriber and device data. You must type 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.

Here are the things you can search for using free text:

<b>Firmware label</b>	<b>Firmware hardware version</b>	<b>Firmware manufacturer</b>
<b>Model</b>	<b>Product class</b>	<b>Software version</b>
<b>Report name</b>	<b>Script name</b>	<b>Script label</b>
<b>Subscriber primary email address</b>	<b>Subscriber name</b>	<b>Person label</b>
<b>Subscriber phone number</b>	<b>Subscriber code</b>	<b>Subscriber domain</b>
<b>WAN POP connection user name</b>	<b>Device domain</b>	<b>Device label</b>
<b>Device disposition</b>	<b>Device hardware version</b>	<b>Device manufacturer</b>
<b>Device model</b>	<b>Device OUI</b>	<b>Device product class</b>
<b>Device serial number</b>	<b>VOIP setting</b>	<b>VOIP user name</b>
<b>WAN IP address</b>		



## How to search

You perform a search by typing key words into the search field. You can simply 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.

This...	Finds this...
jack	Records that contain the term <code>jack</code>
jack london jack and london	Records that contain both terms <code>jack</code> and <code>london</code>
jack or london	Records that contain the term <code>jack</code> , the term <code>london</code> , or both
name: jack	Records that contain the term <code>jack</code> in the name property
name: jack city:not london	Records that have <code>jack</code> in the name property and do not have <code>london</code> in the city property
name:"jack london"	Records that contain the exact phrase <code>jack london</code> in the name property
jack*	Records that contain terms that begin with <code>jack</code>
*jack	Records that contain terms that end with <code>jack</code>
192.168.1.*	Has any IP in the range <code>192.168.1.0</code> to <code>192.168.1.255</code>
192.168.*.*	Has any IP in the range <code>192.168.0.0</code> to <code>192.168.255.255</code>

Here are some 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

- 1 On the Customer Support tab, type the search term in the Find Subscriber or Device field.
- 2 Click  or press Enter.

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



## Selecting subscribers or devices

After you have located 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

Select the check box to the left of the desired subscribers or devices.

---

**Note.** Depending on how your installation of ClearVision is set up, selecting multiple accounts may be restricted to Administrators.

---

To display a single subscriber or device

Click blue text in the search results for that record, such as the subscriber name or device model number.

## Applying labels to multiple records

When you have multiple records selected, you can apply one or more subscriber or device labels to all of the selected records. You can also remove labels. For more information about defining labels, see [Managing labels](#) on page 76.

To apply a label to multiple records

- 1 Search for the subscribers or devices you want to label.
- 2 Select the records you want to label.
- 3 Choose a label from the Add section of the Subscriber Labels or Device Labels menu.



---

**To remove a label from multiple records**

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

## Creating 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 installation of ClearVision is set up, the ability to create accounts may 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...**
  - and create a new device
  - and associate the subscriber with an existing device
  - without device information.
- **Create a new device...**
  - and a new subscriber
  - and associate the device with an existing subscriber
  - without subscriber information.

Creating a new subscriber establishes an account record for the subscriber and may associate the subscriber with a device. You must assign a unique subscriber code. All other information is optional.

**Subscriber code.** Unique code for the subscriber. You can use the subscriber's phone number or any other unique identifier.

---

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

---

**Name (optional).** The subscriber's full name.

**Email (optional).** The subscriber's email address. The email address must be unique.

**Control panel login and password.** These are the credentials the subscriber uses to log into their control panel. You can specify a password, or click Generate Password to generate a secure password.



Creating a new device sets up device information for a specific device and may 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 also need to specify PPP credentials or allow the device to connect to your network with default credentials.

#### To create a new subscriber/device account

- 1** On the Customer Support tab, click Create New Subscriber/Device.
- 2** In the Subscriber ID section of the Provisioning Page, make sure the Create New Subscriber tab is selected.
- 3** Enter subscriber identification information: subscriber code, full name, and email address.

---

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

---

- 4** Do one of the following:
  - Select the Disable Control Panel check box.
  - Provide a user name and password for the subscriber's Control Panel. If desired, click Generate Password to create a password.
- 5** In the Assign CPE section, make sure the Create New Device tab is selected.
- 6** In the New Device section, enter a unique device identifier for the device, using serial number/OUI, provisioning code, or control panel provisioning ID.



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

- Select the Use Default check box.
- Specify a user name and password for PPP access.

**8 (Optional) Select a domain.****9 Click Provision Device.**

ClearVision 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. For more information about working with accounts, see [Chapter 4, Working with Accounts](#).

If errors are encountered, 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.

**To create a subscriber and assign an existing device or no device****1 On the Customer Support tab, click Create New Subscriber/Device.****2 In the Subscriber ID section of the Provisioning Page, make sure the Create New Subscriber tab is selected.****3 Enter subscriber identification information: subscriber code, full name, and email address.****4 Do one of the following:**

- Select the Disable Control Panel check box.
- Provide a user name and password for the subscriber's control panel. If desired, click Generate Password to create a password.

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

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

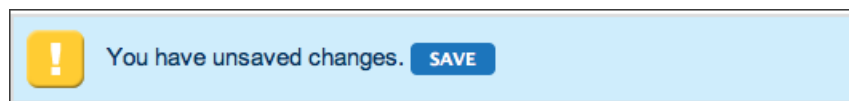
**6 (Optional) Select a domain.****7 Click Provision Device.****To create a device and assign an existing subscriber****1 On the Customer Support tab, click Create New Subscriber/Device.****2 In the Subscriber ID section of the Provisioning Page, do one of the following:**



- Select the No Subscriber Information check box.
  - Select the Assign Existing Subscriber tab.
    - a. In the Find Subscriber field, type search criteria to locate the subscriber.
    - b. Click Go.
    - c. Locate the subscriber in the search results, and click the subscriber information.
    - d. Verify that the correct subscriber is selected.
- 3 In the New Device section, enter a unique device identifier for the device, using serial number/OUI, provisioning code, or control panel provisioning ID.
  - 4 In the PPP credentials section, do one of the following:
    - Select the Use Default check box.
    - Specify a user name and password for PPP access.
  - 5 (Optional) Select a domain.
  - 6 Click Provision Device.

## About saving changes

If you make any changes to subscriber or device information, ClearVision displays a Save button. When you click Save, the changes are saved to the server and sent immediately to the device. If the server is not able to communicate with the device, changes will be sent to the device the next time it checks in.





# Working with Accounts

---

---

[Displaying an account 22](#)

---

[Working with subscribers 23](#)

---

[Managing devices 26](#)

---

[Managing the local network 31](#)

---

[Viewing device status 33](#)

---

Once you have created an account, you can manage the account. The tasks you can perform depend on the account and your user level. Some of the actions described in this section may be available only to Admin users.

Here are the account management tasks you can perform:

- Manage subscriber information
- Manage devices
- Manage local network
- View account status



## Displaying an account





To display an account

- 1 Select the Customer Support tab.
- 2 Enter search criteria.
- 3 In the list of search results, click blue text within the desired account.

An account page displays summary information about the account in the banner at the top of the page. If no subscriber or device is associated with the account, the banner displays clickable links that enable you to quickly make an assignment.

The left side of the screen contains a list of account management tasks. To select an item, click on it. For example, click ACCOUNT to manage accounts. To perform an account management task, click [view](#) next to the task.

Customer Support > 123456789 - ClearAccess SR300NE

<b>Subscriber Code: 123456789</b>  Name: <b>Peter Fine</b> Email: <b>peter.fine@calip.com</b> <span style="background-color: red; color: white; padding: 2px;">Frequent Caller</span> <span style="background-color: red; color: white; padding: 2px;">Late Payer</span>	<b>Device: ClearAccess SR300NE</b>  Serial Number: <b>00255EFCDDDB9</b> OUI: <b>00255E</b> Firmware version: <b>2.3.1.8_4.02L.03.wp1..d2...</b> <span style="background-color: purple; color: white; padding: 2px;">Ethernet Gateway</span> <span style="background-color: purple; color: white; padding: 2px;">OTT</span>	<b>Network Summary</b>  Hosts Online: <b>9</b> WAN Type: <b>100Base-TX</b> WAN IP: <b>64.30.100.228</b>	<b>Status</b>  First Inform: <b>503d 22h ago</b> Last Inform: <b>13s ago</b> Informs: <b>648</b> <span style="background-color: blue; color: white; padding: 2px;">Refresh Device Data</span>
--	---	---	--

▼ ACCOUNT

Device [view](#)

Local Network [view](#)

Status [view](#)

Subscriber

► SERVICES

► ADVANCED

SUBSCRIBER X

**Subscriber Identification**

Subscriber Code: **123456789**

Name:

Email:

**Control Panel Login**

☐ Disable Control Panel Login

Login:

Change Password

Send password: ☒ Notifications will be sent to **peter.fine@calip.com**

[Access Control Panel](#)



## What happens when you display an account

Here's what happens behind the scenes when you display an account:

- 1** Initial text and data are loaded from the server unless you have disabled automatic refresh in your User Profile.
- 2** The system attempts to contact the device(s) associated with this 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 onscreen is updated as needed. At the bottom of the Status section in the banner, the Refresh Device button appears.
  - If the device cannot be contacted, a message is displayed and the Status banner displays an alert.

## Working with subscribers

You use the Subscriber pane to manage individual subscriber data. The Subscriber pane contains several sections of subscriber data.

To display the Subscriber pane, click [view](#).

## Managing subscriber information

You can view subscriber identification, address, and phone information. You may or may not be able to edit these items, depending on the way your ClearVision system is set up.

### Identification information

Basic subscriber information includes the following:

**Subscriber code.** The unique subscriber 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 email address.

### To edit subscriber information

- 1** Click the desired field and add or change information.
- 2** Click Save.

### Address and phone information

The Subscriber pane displays addresses and phone numbers for the subscriber. A subscriber may have several addresses and phone numbers associated with their account.



To add an address or phone number

- 1 Click Add Address or Add Phone.
- 2 Enter the desired information.
- 3 Click Save.

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 customer access to their CPE device's control panel.

To disable or enable control panel login

Do one of the following:

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

To manage login credentials

- 1 In the Login field, enter the subscriber's login name.
- 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 password.

- 3 To enable the generated password to be sent to the subscriber, select the Notifications Will Be Sent To *subscriber@address.com* check box.

To access the subscriber's control panel

Click the Access Control Panel link.

## 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](#) on page 76.

To assign a label

- 1 From Add section of the Labels menu, choose a label.

The label appears in the Label section of the Subscriber pane.



- 2 Click Save.

#### To remove a label

- 1 From Remove section of the Labels menu, choose a label.

The label is removed from the Label section of the Subscriber pane.

- 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 will remain in the system after a subscriber is deleted.

---

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

---

#### To delete a subscriber

- 1 In the Delete section of the Subscriber pane, click Delete Subscriber.
- 2 In the confirmation dialog, click OK.



## Managing devices


You can use the Device pane to review device information or manage the CPE device. The specific tasks available to you depend on your user level (CSR or Admin) and the way your ClearVision installation was set up. Typical tasks can include:

- Assigning a device alias and icon
- Applying or removing device labels
- Reviewing device details
- Rebooting a device
- Adding PPP credentials to enable the DPE 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 capabilities available for managing devices depends on how your ClearVision installation is set up and your user level. Sections within the Device panel may appear in a different order.

To display the Device pane, click [view](#).


Subscriber Code: JG

 Name: Alice Test  
Email: alicemerry@mac.com  
test1


Device: **ClearAccess AG10-NA1**

 Serial Number: 001638FFF701  
OUI: 001638  
Firmware version: 2.3.0.19\_4...

Local Network

 Hosts Online: 0  
WAN Type:  
WAN IP:

Status

 First Inform: 6d 19h ago  
Last Inform: 15m 37s ago  
Informs: 137  
Step 4: Polling device. [21]

▼ ACCOUNT

**Device**

Local Network [view](#)

Status [view](#)

Subscriber [view](#)

► SERVICES

► ADVANCED

**DEVICE** ✕

**Device Identification**

Manufacturer: **ClearAccess**  
Model: **AG10-NA1**  
Serial Number: **001638FFF701**

**Labels**

**Device Details**

Firmware Version: **2.3.0.19\_4.02L.03.wp1.A2pB025c1.d21j2**  
WAN Type:  
WAN IP:

**Bulk Operations**

Participates in Bulk Operations ☒

**Control Panel**

[Access Control Panel](#)

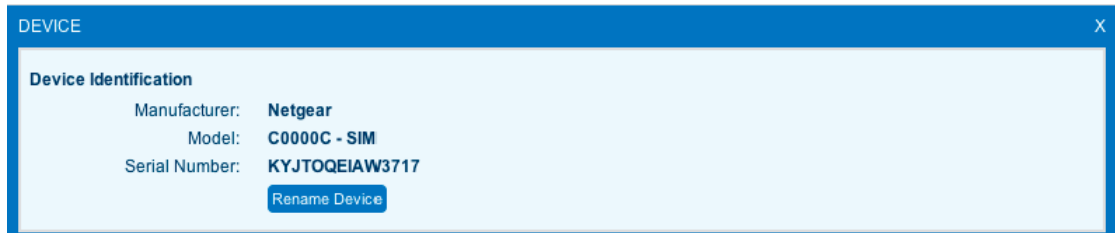


## Assigning a device alias and icon

You can specify an alias for the device and apply an icon to facilitate easy identification. If none of the supplied icons are appropriate, you can specify a URL to where an icon is located. The alias and icon appear in the Device section of the Account banner.

To set up an alias and icon for a device

- 1 In the Device Identification section, click Rename Device.



- 2 In the Device Alias field, enter the desired alias.
- 3 Click Change icon.
- 4 Do one of the following:
  - Select a device icon
  - Specify the URL to an icon
- 5 Click OK.

To remove a device alias and icon

- 1 In the Device Identification section, click Rename Device.
- 2 Click Remove Device Alias & Icon.
- 3 In the confirmation dialog, click Delete Alias & Icon.

## Working with device labels

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

To apply a device label

Click on the Labels menu and select a label from the Add section of the menu.

To remove a device label

Click on the Labels menu and select a label from the Remove section of the menu.



## Viewing device information

The device information pane displays device identification and detail information about the device, including the manufacturer, model, serial number, firmware version, and WAN type and IP.

## Rebooting a device

To immediately reboot a device

- 1 In the Device Reboot section, select the Reboot Device Now check box.
- 2 Click Save.

## Adding and removing PPP credentials

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

To add PPP credentials

- 1 In the PPP Credentials section, click Add PPP Credentials.
- 2 Enter a username and password.
- 3 Select the Resync PPP Information check box.
- 4 Click Save.

To remove PPP credentials

- 1 In the PPP Credentials section, click Remove.
- 2 Select the Resync PPP Information check box.
- 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 at once. 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 or disable bulk operations

Do one of the following:

- To enable bulk operations, select the Participates in Bulk Operations check box.
- To disable bulk operations, clear the Participates in Bulk Operations check box.

## Accessing and managing the control panel

You can enable or disable access to the device's control panel, set up login credentials for the customer, generate and send passwords to a customer, and access the control panel.

---

**Notes.** This is the control panel that is available for subscriber access. For more information about the subscriber control panel, see the *Control Panel User Guide*.

Depending on how your ClearVision installation is set up and your user role, you may or may not be able to set up login credentials. This capability may also appear on other panes, such as the Subscriber pane.

---

### To access the control panel

Click the Access Control Panel link.

### To disable control panel access

Select the Disable Control Panel Login check box.



#### To manage login credentials

- 1** In the Login field, enter the subscriber's login name.
- 2** Do one of the following:
  - To generate a password for the subscriber, click **Generate Password**. This generates a secure password.
  - Enter a password.
- 3** To enable the generated password to be sent to the subscriber, select the **Notifications Will Be Sent to subscriber@address.com** check box.
- 4** Click **Save**.

### Assigning the device to a domain

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

#### To assign the device to a domain

From the Domain menu, choose a domain.

### Removing the association between a device and a subscriber

You can remove the association between the device and the subscriber.

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

#### To remove the 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 the device

Click **Delete Device**.



## Managing the local network

The Local Network pane displays information about any LAN devices attached to the subscriber's CPE device. The LAN devices may be physically attached, or if wireless networking is enabled, may 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 and name devices, and delete disconnected devices from the LAN.

Some local network devices (such as webcams) may have a local interface web service that allows you to manage the device configuration. ClearVision can be used to set up a link to this interface that will appear within 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 will provide 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 pane can be useful for troubleshooting. For example, if the subscriber is running an unsecured wireless network, there may 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 WiFi (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 pane, click [view](#).

The screenshot shows the 'LOCAL NETWORK' pane with the following status information:

- Link Speed: 1205 kb/s up, 25416 kb/s down
- Known Hosts: 3
- Hosts Online: 2

The 'Devices' table lists the following information:

Device	IP Address	MAC Address	Status	Connections	Applied Services	Local Interface	Action
Alices Phone (Apple)	192.168.1.3	5c:59:48:1b:c7:f1	Online	WiFi g		Enable	
qa-blue	192.168.1.2	b8:70:54:66:44:b8	Online	Ethernet		Enable	
Alices-iPad (Apple, Inc)		d8:30:62:90:d5:59	Offline			Unavailable (device offline)	Delete



## Working with LAN devices

To name or rename a device

- 1 In the Local Network pane, click the icon in the Device column.
- 2 Type a name for the device.
- 3 If desired, select an icon for the device.
- 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.

To enable local interface access

- 1 Click Enable.
- 2 If applicable, enter the port number or path in the dialog box, and click OK.
- 3 Save the changes to see the new link.

**Edit Local Interface Access**

Local Interface URL: **192.168.0.10**

Port:  (Optional)

Enter a port number if the user's manual for your device specifies one. If a port number is given, the URL will look like 192.168.0.100:123. The numbers after the colon (123) are the port, and should be entered in the Port: box above.

Path:  (Optional)

Enter a path if the user's manual for your device specifies one. If a path is given, the URL will look like 192.168.0.100/admin/login. The text beginning with the first "/" (/admin/login) is the path and should be entered in the Path: box above.

**Security Alert :**

When the Local Interface Access is enabled, other Internet users are also able to access it. To ensure the security of your device and network, it is recommended that you:

- Change any username and password on the local interface from the default settings
- Disable the local interface access when you do not intend to use it.

Cancel OK



To disable local interface access

Click **Disable**.

To delete a device

- 1 In the **Action** column, click **Delete** for the device that you want to delete.
- 2 In the confirmation dialog, click **OK**.

**Note.** This option is available only for devices that are offline.

## Viewing device status

Device status provides information about the CPE gateway device for this 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 pane, click [view](#).

**STATUS**

Status

First Inform: 563 days 2 hours ago  
 Last Inform: 11 seconds ago  
 Inform Interval: 23 hours  
 Connection Request URL: http://64.30.100.228:30005/  
 Device Up Time: 19 days 5 hours

**WAN Interface 1**

ID: WAN: IP  
 Interface Type: Ethernet  
 Connection Type: Routed  
 Statistics:

	Transmit	Receive
Packets	19060796	23098533
Bytes	167932713	2147483647
Drops	0	0
Errors	0	0

## Status

The Status section of the Status pane shows basic information about the device, including the time since the first inform (check in), 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 pane 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 pane displays information about the amount of data (blocks) transmitted upstream and downstream. It also displays statistics about line errors. This information is available for devices that support it.

## WAN Interface statistics

The WAN Interface section of the Status pane displays information about the subscriber's WAN connection. Information includes the WAN ID, interface type, connection type, and statistics about the amount of data transmitted and received and how many errors occurred and how many packets were dropped. This information is only available for devices that support it



# Working with Services

---

[Managing wireless settings](#) 35

---

[Managing port forwarding](#) 38

---

[Managing content filtering](#) 40

---

[Managing time blocking](#) 45

---

Each account may have one or more services enabled. Some services apply to the entire home network, others can be applied to specific devices. This chapter explains how to do the following tasks:

- Manage wireless networking
- Manage port forwarding
- Manage content filtering
- Manage time blocking

Services appear on the left side of the Customer Support tab.

---

**Note.** You may see additional services, or services may appear in a different order, depending on how your system administrators have configured ClearVision. For more on adding services or changing the order in which services are listed, see [Managing services](#) on page 84.

---

To view services, click Services. To view a specific service, click [view](#).

## Managing wireless settings

Wireless service enables the subscriber to connect LAN devices to the CPE device wirelessly. Any device capable of wireless networking, such as computers, video streaming devices, web cameras, or Wi-Fi-capable phones and tablets, can connect to the subscriber device.

To display the Wireless Settings pane, click [view](#).

## About wireless settings

To enable wireless service, you need to specify several parameters.



**Channel.** Typically, the channel is set to Auto to enable the device to select a channel. However, if there are many devices using the same channel in close proximity, performance may be enhanced by selecting a specific channel. Channels are numbered 1 through 11.

---

**Note.** If the subscriber has multiple wireless services, they must all be set to the same channel.

---

**Enabled.** This check box turns the CPE device's wireless capabilities on or off.

**SSID.** This is the ID displayed by the CPE device and is typically a word, code, or short phrase. Compatible devices can choose from available SSIDs to connect. You can set the SSID. Subscribers can also set the SSID for their devices from their Control Panel.

**Broadcast SSID.** You can set whether the SSID is broadcast to available devices or whether users need to know the SSID to connect.

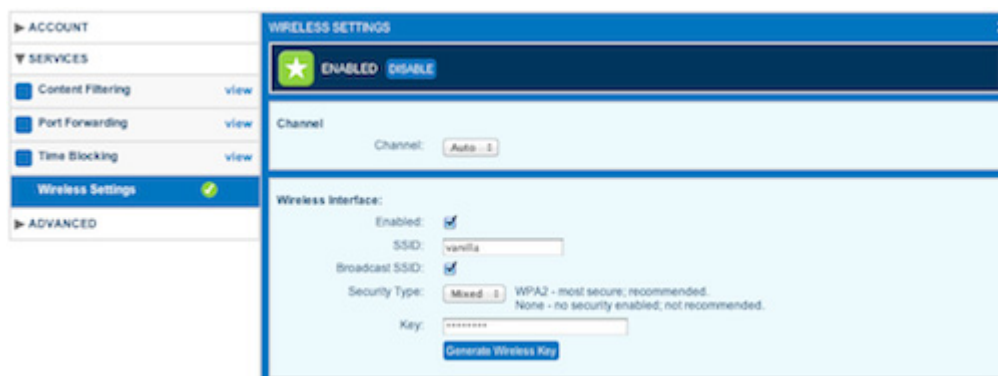
**Restore Factory SSID.** Click this button to restore the SSID to the original value from the first time the device checked in with the system. This button appears only for devices that support this capability.

**Security type.** You can use the following security types.

Type	Definition
None	No password is needed to connect a LAN device to the network. Anyone can connect. This is the least secure setting for a local network.
WAP	Wi-Fi Protected Access. This standard provides more security than WEP. It is backward-compatible with WEP.
WAP2	Wi-Fi Protected Access 2. This standard provides the highest level of security available for local networks. It uses AES encryption.
Mixed	The security type allows devices using WEP, WAP, and WAP2 to connect.
WEP	Wireless Equivalent Privacy. WEP is a protocol that uses stream cipher RC4 encryption standard for confidentiality protection and CRC-32 for integrity assurance. This is the least secure encryption method.



**Key.** The password or phrase used to establish secure communications. You can specify a key, or ClearVision can generate one for you. Subscribers need to know the key to connect LAN devices to the wireless access point. All security types except None require a key.



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

## Enabling and disabling wireless service

### To enable wireless service

- 1 In the Wireless pane, click Enable. This enables the wireless function on the device.
- 2 Select the Enabled check box. This enables the wireless service from the provider.
- 3 Specify the SSID and any SSID options. The SSID may be 1 to 32 characters long and cannot contain the following characters: ' " & < > or \.
- 4 From the Security Type menu, choose a security type.
- 5 In the Key field, do one of the following:
  - Specify a security key. Depending on the security type selected, passwords must meet the following requirements:
    - WEP: 5 or 13 characters long.
    - WPA/WPA2: 8 to 30 characters long. Cannot contain ' " & < > or \.
  - Click Generate Wireless Key to generate a key.
- 6 Click Save.



To disable wireless service

- 1 In the Wireless pane, click Disable.
- 2 Click Save.

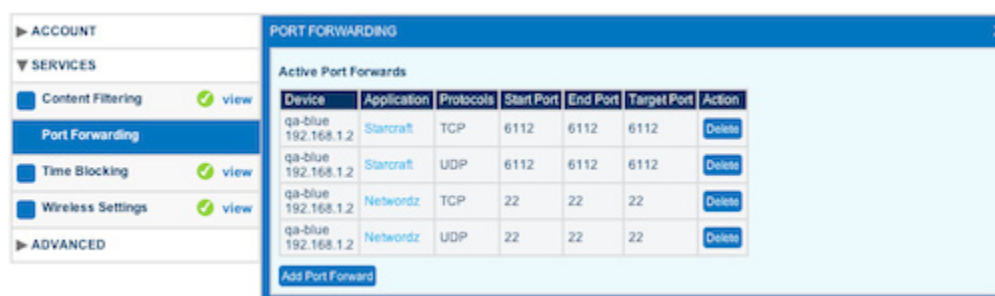
## Managing port forwarding

Port forwarding enables you to specify specific 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 is unable to use an application, you may need to determine which ports need to be open.

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

To display the Port Forwarding pane, click [view](#).



## Enabling and disabling port forwarding

You can quickly enable or disable port forwarding.

To enable port forwarding

- 1 In the Port Forwarding pane, click Enable.
- 2 Click Save.

To disable port forwarding

- 1 In the Port Forwarding pane, click Disable.
- 2 Click Save.



## Managing port forwards

To add a port forward, you need to 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 need to 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 and ClearVision will locate the necessary port information.

To add a port forward

- 1 In the Port Forwards pane, click Add Port Forward.

**Add Port Forwards**

Validation Error

☒ Select Device: WebCam

☐ Enter IP Address:

☐ Enter Custom:

Application	Protocols	Start Port	End Port	Target Port
	<input type="checkbox"/> TCP <input type="checkbox"/> UDP			

☒ Choose from List:

Find an Application:

webcam

- GeoVision TwinDVR with Webcam
- GeoVision Webcam
- Webcam32
- WebcamXP
- Yahoo Messenger Super Webcam
- Yahoo Super Webcam

cancel OK

- 2 In the Add Port Forwards dialog box 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.



- 3 Specify the port by doing one of the following:
  - Choose Enter Custom. Enter the Application name, select one of more protocols (TCP/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. Type 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, click on the application name. The port numbers are displayed.
- 4 Click OK to dismiss the dialog, then Save to save your changes.

To delete a port forward

- 1 In the Port Forwards pane, locate the port forward you want to delete.
- 2 Click Delete.
- 3 Click Save to save your changes.

## Managing content filtering

Content filtering enables subscribers to block inappropriate web content. You can set content filters at four levels or specify no content filtering. Subscribers can also create lists of specific sites to allow or block. Filter settings can be applied to the entire network or to specific devices. Subscribers can change these settings using their Control Panel.

**Note.** Filter level names and categories can be configured using a special configuration file. Configuration options can also 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 pane, click [view](#).

**CONTENT FILTERING**

★ **ENABLED** [DISABLE](#)

**Default Settings**

Filter Level: [Young Teens](#)

Allow List: [Enabled](#)

Block List: [Enabled](#)

[Edit Default Lists](#)

**Settings By Device**

Device	Use Default	Filter Level	Allow List	Block List
qa-blue	<input checked="" type="checkbox"/>	Young Teens	Enabled	Enabled
Alices Phone	<input checked="" type="checkbox"/>	Young Teens	Enabled	Enabled
Alices iPad	<input type="checkbox"/>	<a href="#">Mature Teens</a>	<a href="#">Disabled</a>	<a href="#">Disabled</a>



## About content filtering levels

Content filtering uses a third-party service that categorizes web sites into specific categories. Here are the default category filters:

**Kids (6 and under).** The Kids category filter is different from the other filter groups in that it allows access only to certain sites rather than blocking some categories of sites and allowing all others. The Kids filter 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).** The Young Children filter 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).** The Young Teens filter 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).** The Mature Teens filter 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 web sites constantly appear 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. Depending on what type of filtering features are enabled, such as Allow Lists, Block Lists, content filtering, or time blocking, the result may change. It is important to understand the interactions among these features to be able to troubleshoot specific site access issues.

---

**Note.** It is important to recognize that 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, access to items on the Block List is blocked if a Block List is active, 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 more information about restricting access by time, see [Managing time blocking](#) on page 45.)
- 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, etc.) 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.** ClearVision 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). In these cases, a subscriber may not be able to reach a specific site.

---

### Examples

Here are some examples showing how content filtering works.

---

#### Example 1. Allow List applied. Category filter set to Kids.

*The user requests access to nickelodeon.com.*

The device checks the Allow List, which does contain nickelodeon.com. Access is allowed. Because nickelodeon.com is on the Allow List, it doesn't need to check with the content rating service.

---



---

#### Example 2. Allow List applied. Category filter is not applied.

*The user requests access to nickelodeon.com.*

The device checks the Allow List, which does not contain nickelodeon.com. 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 wildchat.com.*

The device first checks the Block List, which does not include wildchat.com. Then it checks time-blocking to see if access is allowed at this time. Then 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 wildchat.com.*



---

The device first checks the Block List, which does not include wildchat.com. Then it checks time-blocking to see if access is allowed at this time. The device then checks the Allow List, which contains wildchat.com. Access is allowed.

---

**Example 5. Allow List applied. Category filter set to Young Teens. Time-blocking applied.**

*The user requests access to wildchat.com.*

The device first checks the Block List, which does not include wildchat.com. The device then checks the time-blocking settings, which show that the device is not available for use at the current time. Access is blocked.

---

## Enabling and disabling content filtering

You can quickly enable or disable content filtering for a subscriber.

To enable content filtering service

- 1 In the Content Filtering pane, click Enable.
- 2 Click Save.

To disable content filtering service

- 1 In the Content Filtering pane, click Disable.
- 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 and 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 web site domains, such as google.com, that the subscriber's device will allow or block access to. Allow and block lists override the filter-level setting. For example, if the filter allows access to bigbeer.com, but you place it on a block list, the site will be blocked.

To set default content filtering settings

- 1 In the Default Settings section of the Content Filtering pane, choose a default filtering level from the Filter Level menu.
- 2 From the Allow List menu, choose Enabled to enable the list or Disabled to disable the list.



- 3 From the Block List menu, choose Enabled to enable the list or Disabled to disable the list.
- 4 Click Save.

#### To edit default allow and block list

- 1 In the Default Settings section of the Content Filtering pane, click Edit Default Lists.  
ClearVision displays the allow/block list editor.
- 2 Enter the domain names for allowed and blocked web sites. Enter only one domain name per row.
- 3 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 may 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 Block or Allow List for each device. Individual devices use the Block and Allow Lists set up in Default Settings. You cannot create separate lists for each device.

#### To set content filtering for specific devices

- 1 In the Settings by Device section of the Content Filtering pane, choose a filter level for each device.
- 2 Enable or disable the Allow List for each device
- 3 Enable or disable the Block List for each device.
- 4 Click Save.

#### To reset content filtering for a specific device so it uses the network default

In the Settings by Device section of the Content Filtering pane, check the Use Default check box for that device.

## Managing time blocking

Time blocking enables subscribers to restrict local network access. You can restrict access by setting specific hours when service is not available. You 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 using their Control Panel.



To display the Time Blocking pane, click [view](#).

**TIME BLOCKING**

★ **ENABLED** [DISABLE](#)

**Default Settings:**

Time Zone:

**Night Blocking**

Weekday [Sun-Thu]:  :  to

Weekend [Fri-Sat]:

**Bonus Time**

Remaining: 1 1/2 hours

**Settings By Device**

Device	MAC Address	Time Limits		Night Blocking		Remaining
		Weekday (Mon-Fri)	Weekend (Sat-Sun)	Weekday (Sun-Thu)	Weekend (Fri-Sat)	
qa-blue	b8:70:54:66:44:b8	n/a	n/a	Default	Default	Default
Alices Phone	5c:59:48:1b:c7:f1	n/a	n/a	Default	Default	Default
Alices iPad	d8:30:62:90:d5:59	7 hours / day	Unlimited	10:00 pm to 6:00 am	Not Blocked	1 1/2 hours

## Enabling and disabling time blocking

You can quickly enable or disable time blocking.

To enable time blocking

- 1 In the Time Blocking pane, click **Enable**.
- 2 Click **Save**.

To disable time blocking

- 1 In the Time Blocking pane, click **Disable**.
- 2 Click **Save**.

## Managing default time-blocking settings

Default settings apply to the entire home network. The default settings also specify the local time zone.

**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

- 1 In the Default Settings section of the Time Blocking pane, choose a time zone from the Time Zone menu.
- 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.
- 3 Click Save.

## Manage 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 computer that is night blocked is removed from the network for a week, night blocking will take effect again when the computer is returned 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

- 1 In the Settings by Device section of the Time Blocking pane, click a device name.
- 2 In the Edit Time Blocking dialog, clear the User Default check box.
- 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.
- 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.
- 5 (Optional) Add bonus time.



## 6 Click OK, then click Save.

**Edit Time Blocking** [X]

Device: Alices Phone Use Default ☐

**Time Limits per day**

Weekday [Mon-Fri]: 12 hours

Weekend [Sat-Sun]: Unlimited

**Night Blocking**

Weekday [Sun-Thu]: Blocked : 10:00 pm to 6:00 am

Weekend [Fri-Sat]: Not Blocked

**Set Bonus Time**

Length of Bonus Time: 1/2 hour

None 23 1/2 hours

Cancel OK

## 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

- 1 In the Add Bonus Time section, choose the amount of time to add.
- 2 Click Save.

**Bonus Time**

Remaining: 1 1/2 hours

None

None 23 1/2 hours







# Performing Advanced Tasks

---

---

Working with event logs 51

---

Using the parameter browser 53

---

Managing device synchronization 55

---

Working with scripts 56

---

Upgrading firmware 58

---

Replacing a device 59

---

Setting up local GUI access 60

---

When working with accounts, you may need to investigate the customer network, send information to the customer's device, or update device firmware. This chapter describes the following tasks:

- View and manage event logs
- Browse parameters
- Synchronize devices
- Run scripts
- Upgrade 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 installation of ClearVision is set up and your user level (CSR or Admin).

---



## Working with event logs

Event logs record information about TR-069 communications between the device and the ACS. You can view event logs at different levels of detail and you can print event logs. You can also configure the amount and type of information collected by the log.

To view the Event Logs pane, click [view](#).

**Recent Sessions**

Connected At	Duration	Events
Mon Apr 23rd 2012 17:30:26	12.1s	2 PERIODIC
Mon Apr 23rd 2012 17:28:53	12.1s	2 PERIODIC
Mon Apr 23rd 2012 17:26:37	12.1s	2 PERIODIC
Mon Apr 23rd 2012 17:24:24	12.0s	2 PERIODIC
Mon Apr 23rd 2012 17:23:59	12.4s	2 PERIODIC
Mon Apr 23rd 2012 17:22:29	11.8s	2 PERIODIC
Mon Apr 23rd 2012 17:06:12	21.2s	2 PERIODIC
Mon Apr 23rd 2012 16:51:15	18.8s	2 PERIODIC
Mon Apr 23rd 2012 16:11:13	12.3s	2 PERIODIC
Mon Apr 23rd 2012 15:11:45	12.4s	2 PERIODIC

View 10 per page  
Page 1 of 4  
Showing 1-10/33 items.

**Configure Logging Detail**  
Change the logging level for this device: **Network**

**Device Logging Help**  
This page shows the details of all TR-069 communication sessions between the current device and the server. These activity logs are kept for a maximum of 10 days. You can set a device to track one of four levels of sessions:  
**No Logging** - You can set a device so that it does not track and log any information.  
**Info** - This level logs when the device connects to the server and any events that are triggered.  
**Debug** - This level logs scripts that are executed and their parameters, and includes calls made by these scripts to the device. It also shows the session information.  
**Network** - This level tracks a complete record of all network traffic sent and received; in addition to session information and debugging information.

**Session Log**

Hardware Version	SR300NE	Show Trace Detail	<input type="checkbox"/>
Software Version	2.3.1.8_4.02L.03.wp1.d21j2	Show SOAP Detail	<input type="checkbox"/>
Session ID	492197E4CFE4B2B68B5351717AF34FA3.demo24		
Time	Type	Event Detail	
+0.025s	SOAP XML	2622 bytes received from device	
+0.067s	Fire Event	CONNECTION_REQUEST	

The Event Logs pane displays a list of recent sessions by date and time and a menu for configuring the logging detail level. It also shows information about event logging levels.

To refresh the event log list

To ensure that the Recent Sessions list displays the most recent sessions, click .



## About event logs

Event logs record when data is sent to or received from a device, error messages, and the results of scripts or scheduled events. You can control the level and type of detail displayed in the log.

Logs are kept for a maximum of 10 days.

### To view a session log

On the Event Log pane, click a log file.

The logged information appears in the Session Log.

Use the icons in the upper right corner of the session log to:



Print the log.



Expand the log to fill the pane.



Collapse the log display.



Close the log file.

Depending on the event logging level, you may be able to view display trace and Simple Object Access Protocol (SOAP) detail in the log. Use the check boxes in the upper right corner of the session log to turn on trace or SOAP detail.

**Trace detail** provides very detailed information about any events captured by the log. You can view the parameter and properties used as well as detailed information about script execution.

**SOAP detail** displays the XML communications with the device for each event in the log.



## About event logging levels

ClearVision enables you to set a level for capturing events to the log. The level applies to the device. If a device is functioning well, you may want to turn off logging to reduce traffic or to avoid using up disk space. Conversely, if a customer reports an issue, you may 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.** The system records when the device connects to the server and information about any events that occurred, such as an inform, upgrade, or other event.

**Debug.** The system records session information and information about any scripts that are executed. It records parameters used in scripts and the calls made by the scripts to the device.

**Network.** The system saves a complete record of all network traffic sent and received in addition to session and debug information.

### To set event logging level

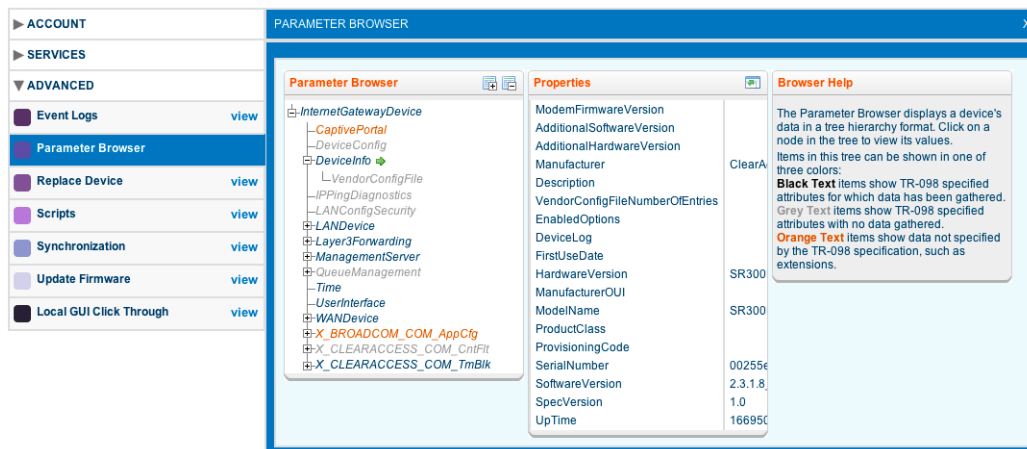
- 1 Display the Event Logs pane for an account.
- 2 In the Configure Logging Detail section, choose a logging level for the device.

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

## Using the parameter browser

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

To view the Parameter Browser pane, click [view](#).





The parameter browser uses color to show types of information.

**Black text** items show TR-098-specified attributes for which data has been gathered.

**Grey text** items show TR-098-specified attributes for which no data has been gathered.

**Orange text** items show data not specified by the TR-098 specifications.

To view device parameters

- 1 Display the Parameter Browser for an account.
- 2 Use the plus and minus icons to display more of the parameter hierarchy until you see the parameter you want to investigate.
- 3 Click the parameter.

The parameter's properties appear in the Properties section of the Parameter Browser pane. Click the Expand icon to expand the Properties view.

Use the icons on the Parameter Browser pane to customize the display:



Expand the parameter hierarchy.



Collapse the parameter hierarchy.



Expand the Properties section to fill the pane.



Collapse the Properties section.



Close the Parameter Browser.



## Managing device synchronization

The Synchronize pane enables you to view parameters that can be synchronized between the device and the server. You can see which applications need to be initialized or synchronized and you can select items to sync.

To view the Synchronize pane, click [view](#).

▶ ACCOUNT

▶ SERVICES

▼ ADVANCED

Event Logs

view

Parameter Browser

view

Replace Device

view

Scripts

view

Synchronization

Update Firmware

view

Local GUI Click Through

view

SYNCHRONIZATION

Application	Code	Ownership	Pending Sync	Needs Initialization	State	Last Sync
Access Control	AccessControl	SERVER	<input type="checkbox"/>		OK	503 days 22 hours ago
Captive Portal	CAPO	SERVER	<input type="checkbox"/>		OK	503 days 21 hours ago
Content Filtering	CF	SERVER	<input type="checkbox"/>		OK	N/A
Click Through	ClickThrough	SERVER	<input type="checkbox"/>		OK	429 days 1 hour ago
Control Panel	ControlPanel	SERVER	<input checked="" type="checkbox"/>		OK	503 days 22 hours ago
DeviceIdentification	DeviceIdentification	SERVER	<input checked="" type="checkbox"/>		OK	N/A
Device Info	DeviceInfo	DEVICE	<input checked="" type="checkbox"/>		OK	14 seconds ago
Device Statistics	DeviceStats	DEVICE	<input type="checkbox"/>		OK	14 seconds ago
Entone STB	EntoneSTB	SERVER	<input type="checkbox"/>		OK	N/A
Factory Reset Device	FactoryResetDevice	SERVER	<input type="checkbox"/>		OK	N/A
Firewall	Firewall	SERVER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	OK	18 hours 34 minutes ago
Firmware Management	FirmwareManagement	SERVER	<input type="checkbox"/>		OK	N/A

## Understanding synchronization status

The Synchronize pane displays a list of applications that ClearVision supports. It also contains information about the ownership of the application data, whether or not changes are pending or the application needs initializing, the state of the application, and the last sync.

For each application, it shows who “owns” the data for the application. The owner is considered the master data holder for the application. For example, the ACS server owns the data for whether a service, such as Wireless, is enabled. However, the device owns the information for the LAN devices attached to the device. When a synchronization occurs, data from the master is delivered to the ACS or device, as appropriate.

The Pending Sync check boxes show applications awaiting a sync. If application data has changed, the Pending Sync check box is selected for that application.

The Needs Initialization check boxes appear for applications that need initial setup. For example, if you enable the Port Forward application for a device, the Needs Initialization check box is selected.

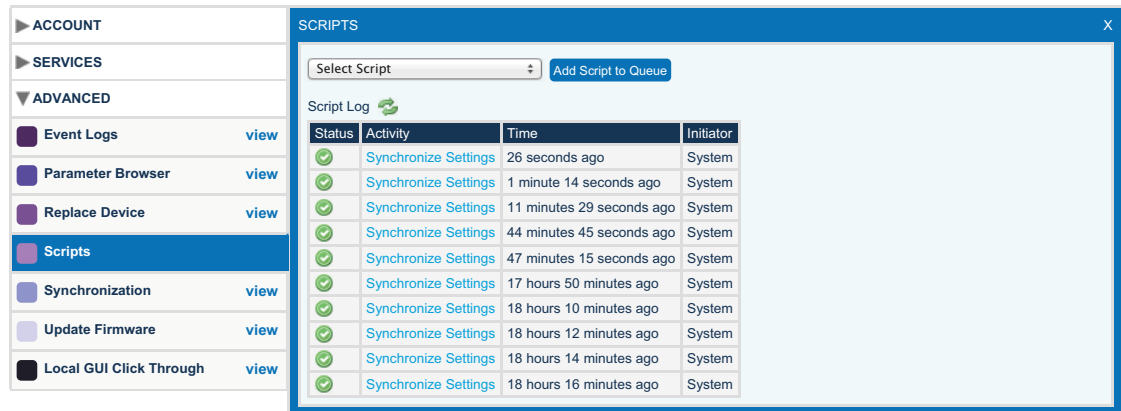
You can select a check box to force a sync or initialization for an application. Clear the check box to avoid a sync.



## Working with scripts

The Scripts pane enables you to add predefined scripts to a queue. Scripts placed in a queue run against the device the next time it checks in. For more information about defining scripts, see *Managing scripts* on page 90.

To view the Scripts pane, click **view**.



## About scripts

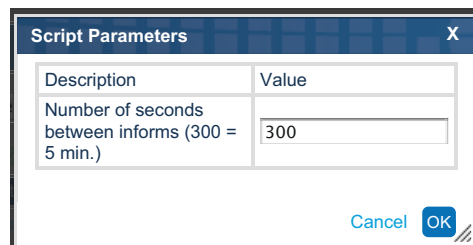
Scripts define actions to be taken for a device. ClearVision supplies some scripts, and system administrators can write additional scripts. The scripts can address any parameters in the data model. For example, there is an included script to set the inform interval.

When you work with scripts in the context of an account, you select a script from a menu. You may need to specify some 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 pane.

To add a script to the queue

- 1 In the Scripts pane, choose a script from the Select Script menu.
- 2 Click Add Script to Queue.
- 3 If requested, specify script parameters.

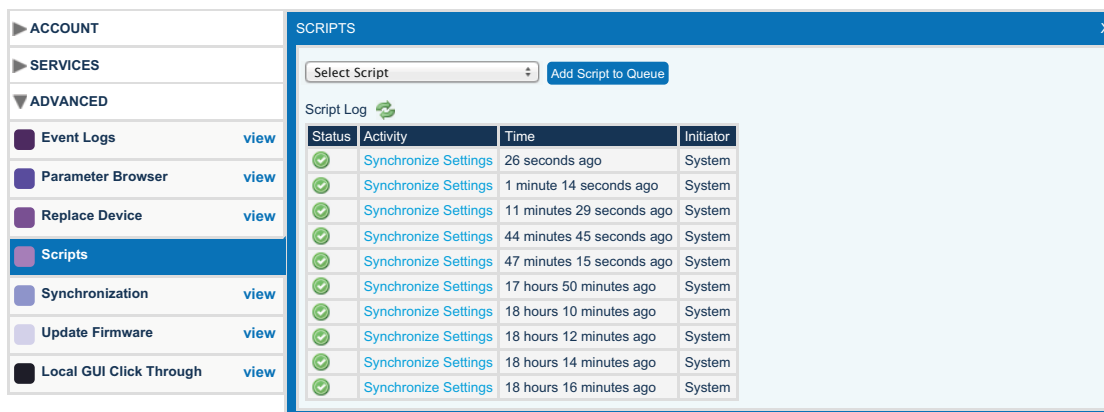


- 4 Click OK.



- 5 If desired, add more scripts to the queue.
- 6 Click Save to save your changes.

The Script Log displays the pending scripts.



To view script results

In the Scripts pane, click a script Activity.

Activities that are complete are displayed in blue text. The status field is blank.

The Script Log Detail shows the results of the action.

Script Log Detail			X
Tue Apr 24th 2012 11:39:55	WARNING	[Driver]: Using base driver for ManagementServerStatus application, as no explicit driver found against device 'ClearAccess', 'SR300NE', '2.3'	
Tue Apr 24th 2012 11:39:55	WARNING	Unable to sync app FirmwareManagementStatus include in sync is false	
Tue Apr 24th 2012 11:39:55	WARNING	Excluding FirmwareManagementStatus from sync.	
Tue Apr 24th 2012 11:39:55	INFO	syncing module :: DeviceInfo	
Tue Apr 24th 2012 11:39:57	INFO	syncing module :: WANDevices	
Tue Apr 24th 2012 11:39:57	INFO	syncing module :: Hosts	
Tue Apr 24th 2012 11:40:05	INFO	syncing module :: DeviceStats	
Tue Apr 24th 2012 11:40:05	INFO	syncing module :: TBStatus	
Tue Apr 24th 2012 11:40:05	INFO	syncing module :: WANInterfaces	
Tue Apr 24th 2012 11:40:05	INFO	syncing module :: ManagementServerStatus	

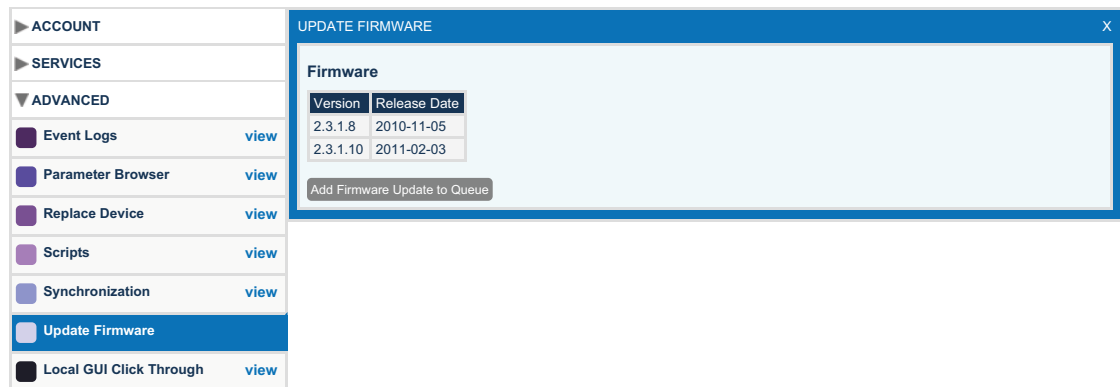


## Upgrading firmware

The Firmware Upgrade pane enables you to 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 Firmware Upgrade pane lists any installed firmware upgrades that are available for the specified device model. If no upgrades are available, none is listed.

To view the Firmware Upgrade pane, click [view](#).



To queue a firmware upgrade

- 1 On the Firmware Upgrade pane, select a firmware version.
- 2 Click Add Firmware Update to Queue.
- 3 Click Save.

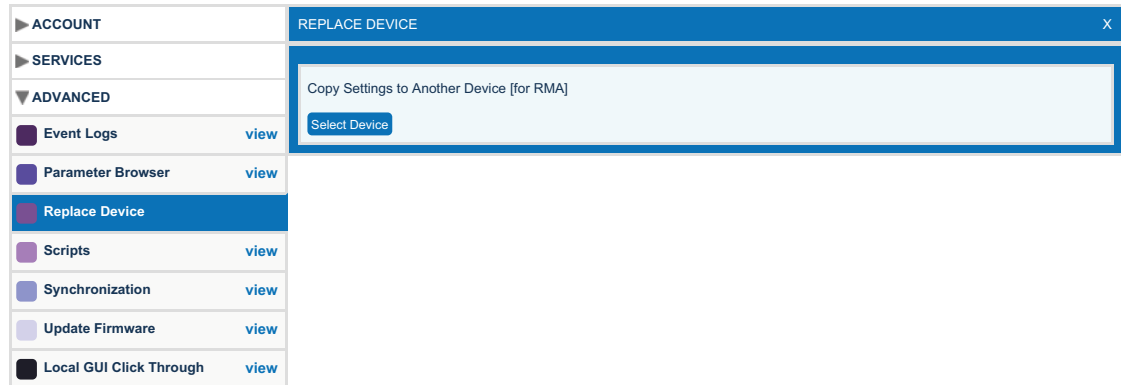


## Replacing a device

If a device malfunctions, you may need to replace it. The Replace Device pane enables you to copy settings from the currently displayed device to another device.

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

To display the Replace Device pane, click [view](#).



To copy device settings to another device

- 1 On the Replace Device pane, click Select Device.
- 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 search for an 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 search for and locate a CPE device.

**Note.** Depending on how your installation of ClearVision is set up, you may not see the Activation Server Device tab.

- 3 Click the device you want to copy settings to.
- 4 Verify that the selected device is the correct one.
- 5 Click Copy Settings.



After you copy the settings, the page will reload the information about the device that has just received the settings. This enables you to make further configuration changes to the new device.

**REPLACE DEVICE**

NEW DEVICE | EXISTING DEVICE | ACTIVATION SERVER DEVICE

Find Device:

OUI	Serial Number	Provisioning Code	Manufacturer	Model	Device Label
001018	001018801A62	--	ClearAccess	WRG3380	
001018	00101880215E	--	ClearAccess	WRG3380	
001801	001505F747E9	--	Actiontec	3A - GT724-WG	DSL Gateway
001A2B	001A2B22771F	--	ClearAccess	EG10W-IPTV - 96348GW-11	
0022CE	0022CE9786E1	--	Cisco	DPC3825_1.0 - DOCSIS 3.0	
00255E	00255E45FB8F	--		--	
00255E	00255EA9367A	--	ClearAccess	SR300N	
00255E	00255EAEB150	--	ClearAccess	SR100G	
00255E	00255ECD6089	--	ClearAccess	SR100	
00255E	00255EDA5D3B	--	ClearAccess	SR300N	

View 10 per page Page 1 of 5 Showing 1-10/44 items.

**Selected Device:**

Device Manufacturer: ClearAccess  
Device Serial Number: 00101880215E

Copy Settings

## Setting up local GUI access

The Local GUI Click Through pane enables you create a link to the user interface for a device. This enables a CSR to access local statistics maintained by the CPE device, or to configure device-specific settings that are not available through the ClearVision interface.

To view the Local GUI Click Through pane, click [view](#).

**LOCAL GUI CLICK THROUGH**

Device Click Through

Enable Local GUI Access ☒

Enabling Access

Steps:

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

To set up local GUI access

- 1 On the Local GUI Click Through pane, select the Enable Local GUI Access check box.
- 2 Click Save.



- 3 After the device has updated, return to the Local GUI Click Through pane to use a link to the device user interface.

---

**Note.** The link remains active for about 15 minutes. After that, access must be re-enabled before using it again.

---



# Reports

---

---

About reporting 62

---

Running existing reports 63

---

Creating custom reports 66

---

Running aggregate reports 71

---

Using Reports to understand your network 72

---

## About reporting

ClearVision 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, 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.



## About included reports

ClearVision Reporting comes with five built-in reports. The built-in 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.

Here are the reports included with ClearVision Reporting:

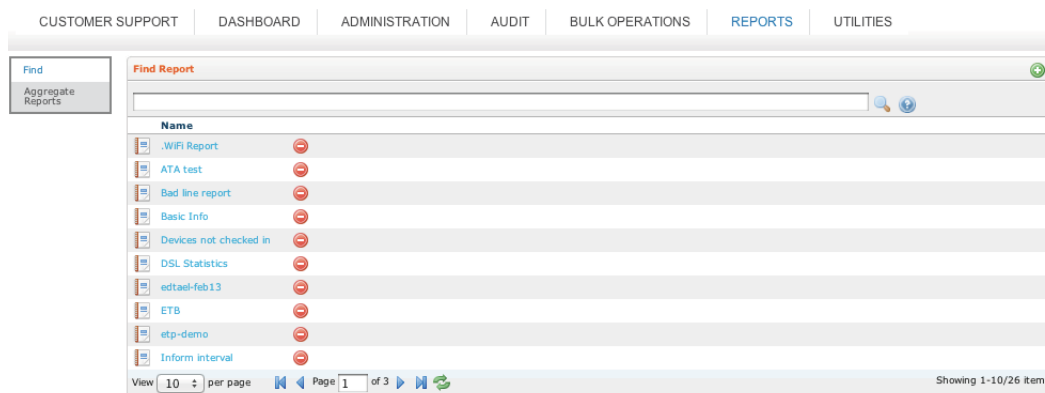
- Device Count by Firmware Version
- Device Count by Manufacturer and Model
- Device Count by Label
- Subscriber Count by Label
- Device Count by WAN Interface

## About 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.

## Running existing reports

You can easily locate and run reports from the Reports tab.





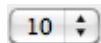
The Reports tab displays a list of previously defined custom reports. You can use the following controls on this tab:



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.

To find a report






















1 Type all or part of the report name.

2 Click .

To run an existing report




Click the report name.

ClearVision displays the report results.

.WiFi Report								  	
Subscriber Name	Subscriber State	Email Address	WiFi Number of Devices	WiFi Standard	LAN Device Count	WiFi Security Type	Subscriber Label		
Saul Barnett	DE	Saul_Barnett_52280@hotmail.com	7	a	11	None			
Tina Dietz	AL	Tina_Dietz_68780@gmail.com	6	a	10	None			
Loren Cook	TN	Loren_Cook_45203@me.com	7	a	10	None			
Sam Hill	NV	Sam_Hill_99311@yahoo.com	6	a	7	None			
Vikki Phillips	NM	Vikki_Phillips_72813@gmail.com	6	a	12	None			
Jewel Claire	WY	Jewel_Claire_98762@gmail.com	9	a	11	None	 		
Noah Perez	OK	Noah_Perez_53299@gmail.com	6	a	10	None			
Herbert Maloney	MP	Herbert_Maloney_47504@gmail.com	6	a	10	None			
Kelvin Maloney	MT	Kelvin_Maloney_55711@me.com	6	a	9	None			
Kathie White	TX	Kathie_White_57555@me.com	6	b	8	None			
View <input type="text" value="10"/> per page   Page <input type="text" value="1"/> of 4   								Showing 1-10/31 items.	
Apply labels to 31 : <input type="text" value="Labels"/>								 Save as CSV  New Bulk Operation	



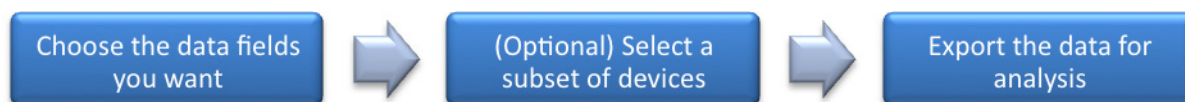
You can do the following with the report results:

- To 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.
- To save the report results as a comma-separated values (csv) file, click Save as CSV.
- To 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](#).
- To print the report, click .
- To edit the report definition, click .
- To close the report and return to the Find Report pane, click .



## Creating custom reports

When you create a custom report, you decide which data fields you want to use, optionally select a subset of devices to report on, and export the data for analysis.



As you build your report, ClearVision shows you the potential Report Results.

**Edit Report**

Report name: Content Filtering Enabled

Available Columns

Search this list:

- Click Through Application Sta
- Content Filtering Dynamic In
- Content Filtering Enabled
- Content Filtering In Use
- Content Filtering Static In Use
- Control Panel Application Mes
- Control Panel Application Stat
- Control Panel Provisioning ID
- Country
- Default Connection Service

Include These Columns

- Subscriber Name
- Manufacturer & Model
- Device Labels
- Serial Number

Sorting

Manufacturer & Model A..Z

Filter Criteria

Subscriber Associated is true

and

Content Filtering Enabled is true

☐ Advanced Syntax

---

**Report Results**

Subscriber Name	Manufacturer & Model	Device Labels	Serial Number
Brooks Macielinski	Cisco A0000A - SIM	<span>Blue</span> <span>Red</span>	TNBSACURRT2352
Darryl Wright	Cisco A0000A - SIM	<span>Green</span>	FSYXPIDQNF4836
Mildred Pate	Cisco A0000A - SIM	<span>Red</span>	EALWXXVRIIS2972
Xavier Tichenor	Cisco A0000A - SIM	<span>Green</span>	IPLLNWGAAT5070
Vito Davis	Cisco A0000A - SIM	<span>Yellow</span>	PEAZQXKJAY9193
Treva Cook	Cisco A0000A - SIM	<span>Blue</span>	TSFLNWUPWP3902
Percy Dupre	Cisco A0000A - SIM	<span>Green</span>	BWBKTYESOY2813
Lily Cruz	Cisco A0000A - SIM	<span>Red</span>	FWFTYAUGFU1163
Mable Kelly	Cisco A0000A - SIM	<span>Blue</span> <span>Red</span> <span>Yellow</span>	ENSMJWHPLE5991
Clare Rodriguez	Cisco A0000A - SIM	<span>Green</span>	RMTEDJLHKK9790


View  per page Page  of 124 Showing 1-10/1237 items.

Apply labels to 1237:



---

**To create a custom report**

- 1** On the Reports tab, click .
- 2** In the Report Name field, enter a name for your report.
- 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 .

---

- 4** (Optional) Choose 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 you want to sort.
- 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 order you want to filter.
- 6** Do one of the following:
  - Click Save to save the report and stay in the Edit Report pane.
  - Click Save and Return to View to save the report and view the results on the Devices and Subscribers pane.

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



## 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, two options appear:

- **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.

To change 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. The parameters may be a simple true or false, or you may be able to specify a relationship (more than, less than, equal to) or set up a list of values.





For example, if you wanted 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

If you need to change a parameter after applying it, click Edit. Mouse 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. 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.

The screenshot shows a 'Filter Criteria' window. On the left, a vertical blue bar contains the word 'and'. To its right, there are two 'or' operators. The first 'or' groups two criteria: 'Subscriber Associated is true' and 'Content Filtering Enabled is true'. The second 'or' groups two criteria: 'Manufacturer & Model matches AG10W-NA2' and 'Manufacturer & Model matches AG10-NA1'.

## Working with Advanced Syntax

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

The screenshot shows an 'Advanced Syntax' window. It contains a text area with the following query statement: `subscription with (hasSubscriberAssociation: true and contentFilteringEnabled: true) show fullName as "Subscriber Name" manufacturerModel as "Manufacturer & Model" deviceLabel as "Device Labels" serialNumber as "Serial Number" sort manufacturerModel asc`. There is a small icon in the bottom right corner of the text area.

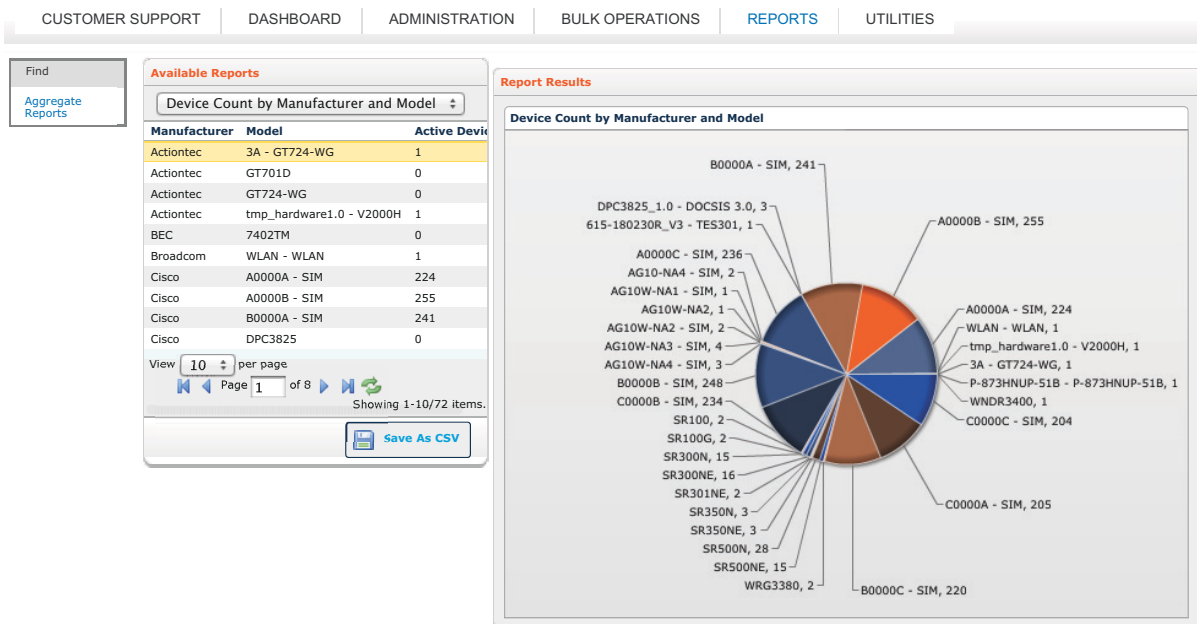
To view advanced syntax

Click .



## Running aggregate reports

Aggregate reports are included with ClearVision. These reports give you insight into the total subscriber/device base.



Included aggregate reports include:

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

To run an aggregate report

- 1 On the Reports tab, click Aggregate Reports.
- 2 From the Available Reports menu, choose a report.
- 3 Do one of the following:
  - View the results on your screen.
  - To export the results, click Save as CSV.



## Using Reports to understand your network

Reports can be used to export data that is maintained in ClearVision. This data can be used to study a wide variety of conditions. Some common uses are:

- Identifying potential problem access lines as indicated by SNR, attenuation, retrain, and data rate. This can help reduce churn.
- Identifying CPEs with open Wi-Fi security and excessive Wi-Fi devices. Having this information will reduce calls to your CSRs and result in cost savings.
- 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- vs. lower- end managed devices. It may also help indicate product longevity, based on a first- inform time analysis.

Examples of other trend reports would include:

- Number of managed devices by Manufacturer, Model, and Firmware version
- Distribution of Wired vs. Wireless networks
- Use of DSL vs. Ethernet
- Studying device trends in the home, which is helpful for understanding device trends and up-sell potential.

Examples of in-home managed device trends would include:

- Number of LAN devices per subscriber
- Number of Wi-Fi vs. Ethernet devices per subscriber
- Percentage of subscribers using Wi-Fi security (and, if so, 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 having 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 would include:**
  - **Downstream/upstream link speed**
  - **Attenuation**
  - **Noise margin**
  - **Retrain frequency and uptime**
  - **Average broadband speed**
- **Investigating subscriber breakdown by device associated, advanced services enabled vs. used, label, location, and first contact date.**



---

# Administrator Tasks



# Administration Overview

---

---

[Managing labels 76](#)

---

[Managing users 78](#)

---

[Managing device types 80](#)

---

[Managing firmware versions 82](#)

---

[Managing services 84](#)

---

[Managing scripts 90](#)

---

[Managing events 93](#)

---

[Managing announcements 95](#)

---

**You use the Administration tab to control and manage the ClearVision software.**

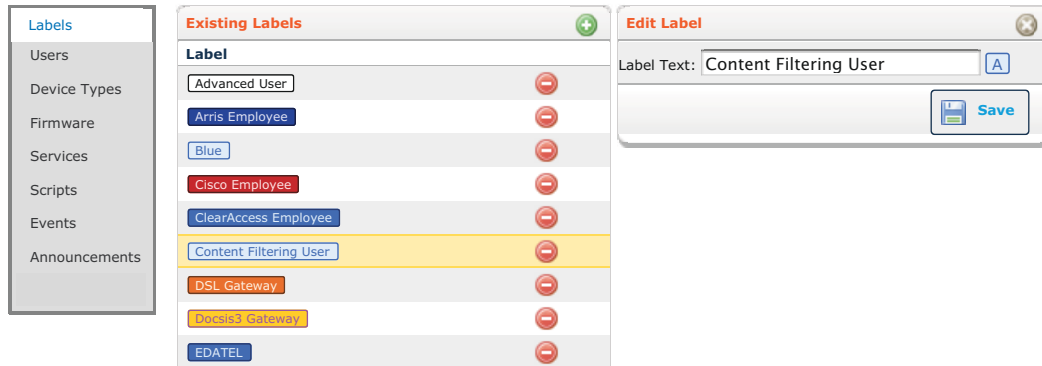
**System admins can:**

- **Create global system labels**
- **Add new user accounts to ClearVision and manage existing accounts**
- **Set roles for each new user to ClearVision**
- **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**



## Managing labels

Use the Labels pane to review, edit, and create new labels to apply throughout ClearVision. You can apply labels to devices, subscribers, firmware, users, and scripts.



**Existing Labels.** This list 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 modify existing labels.



Click to close the editor and discard your changes.



Click to delete a label from the system.






Click to save your changes.



## Using the Label Editor

To add a new label to the system


- 1 On the Administration tab, select Labels.
- 2 Click  . The system displays the Label Editor.
- 3 Enter the label name in the Label Text field.
- 4 Click  . A color palette window appears with various colors that you can use to distinguish your label.
- 5 Select a color to apply from the color palette.
- 6 Click  Save .

---


**Note.** Labels can include upper and lowercase letters, numbers, underlines, and spaces only. Labels cannot exceed 32 characters in length.

---

To edit a label

- 1 On the Administration tab, select Labels.
- 2 Click on a label to edit from the Existing Labels List.
- 3 Make your changes to the fields. You can change a label's name or color scheme.
- 4 Click  Save .

To delete a label

- 1 Locate the label to delete from the Label list.
- 2 Click  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.



## Managing users

Use the Users pane to manage users in ClearVision. This page includes a secondary search field that allows you to quickly search for user information. It appears just under the User List heading.

The screenshot displays the 'User List' and 'User Edit' panels in the ClearVision interface. The 'User List' panel includes a search bar and a table of users. The 'User Edit' panel allows for modifying user details. The 'User Actions' panel at the bottom provides options for managing user labels.

Login	Name	Email	Labels
cisco1	CSR - Cisco1	cisco1@cisco.com	Cisco Employee
cisco2	CSR - Cisco2	cisco2@cisco.com	Cisco Employee
connyf	Conny Franz	connyf@inteno.se	
csr-carol	Carol CSR	carol@clearaccess.com	
csr-login	csr login	csr@clearaccess.com	
CSR1	CSR1	csr1@clearaccess.com	
daxtman	Dan Axtman	daxtman@cradlepoint.com	
demo	ClearAccess demo	demo@clearaccess.com	
demo2	DEMO 2	demo2@clearaccess.com	
desposito	Dan Esposito	dan.esposito@tdstelecom.com	

View 10 per page Page 4 of 7 Showing 31-40/62 items.

**User Edit**

Login: CSR1

Enabled: ☒

Full Name: CSR1

Email: csr1@clearaccess.com

Password:

Confirm:

Roles: Administrator, CSR

Domains: Service Provider 1, Service Provider 2, Service Provider 3

**User Actions**

Labels:

Currently, ClearVision includes two different roles that you can apply to a user account. These are:

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

The user list displays a search result list of users in ClearVision. Here are things you can do with the user list:

Click to add a new user to ClearVision.

Click to refresh the User list.

**Search field and .** Use the search field to search for a user name.

**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 modify user information. Enable the account by putting a check mark in the Enabled check box. Disable the account by removing the check mark in the Enabled check box

**User Actions.** Assign or remove labels from the user.





 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 to save your changes.

## Using the User Editor

To add a new user


- 1 On the Administration tab, click Users.
- 2 Click .
- 3 Enter the user's login name in the Login field.
- 4 Select the Enabled box to activate the account and allow the user to log in. Disable the account by clearing the Enabled check box
- 5 Enter the user's full name in the Full Name field.
- 6 Enter the user's email in the Email field.
- 7 Enter the user's password in the Password field.
- 8 Enter the user's password again in the Confirm field.
- 9 Select a role for your user from the Roles list.
- 10 (Optional) Select one of 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.
- 11 Click .

To edit user information

- 1 Search for the user.
- 2 Click a user name in the Users List to display the User Editor.
- 3 Edit any of the fields for that user.
- 4 Click .



### To delete a user

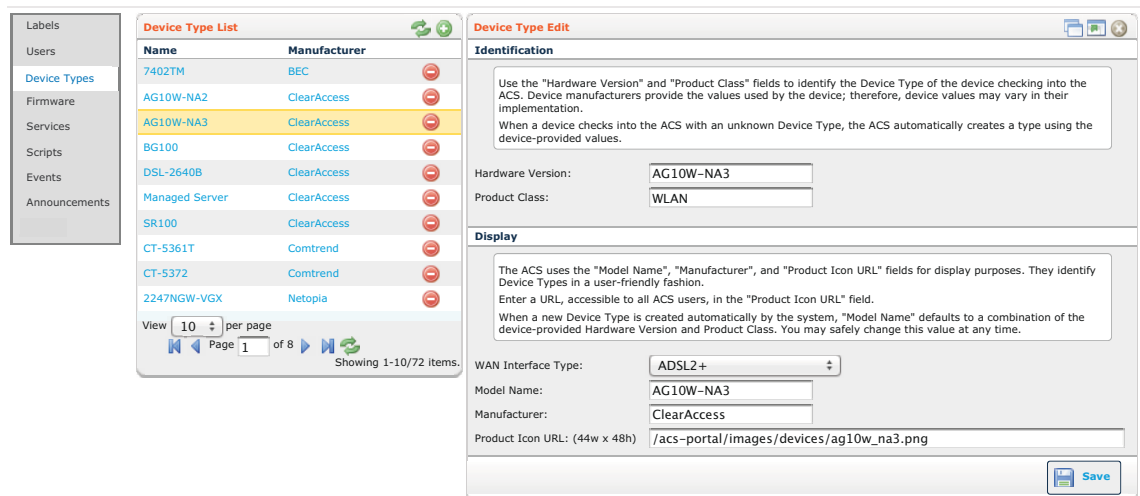
- 1 Locate the user to delete from the User List.
- 2 Click  in the user's row to remove the user from the system. The system refreshes the page, listing the remaining users.

## Managing device types











Use this page to manage device type profiles in your system. A device type maps to a hardware model. Each model has its own unique signature. ClearVision 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 hardware version and/or hardware class that the device has built in. The system will try and pull in as much information from the device into the profile as it can.

When you connect a new device to ClearVision, 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 type.



The screenshot shows the 'Device Type List' and 'Device Type Edit' interface. The 'Device Type List' on the left displays a table of device types with columns for Name, Manufacturer, and a delete icon. The 'Device Type Edit' on the right shows the 'Identification' section with fields for Hardware Version and Product Class, and the 'Display' section with fields for WAN Interface Type, Model Name, Manufacturer, and Product Icon URL.

Name	Manufacturer	
7402TM	BEC	
AG10W-NA2	ClearAccess	
AG10W-NA3	ClearAccess	
BG100	ClearAccess	
DSL-2640B	ClearAccess	
Managed Server	ClearAccess	
SR100	ClearAccess	
CT-5361T	Comtrend	
CT-5372	Comtrend	
2247NGW-VGX	Netopia	

View 10 per page Page 1 of 8 Showing 1-10/72 items.

**Device Type Edit**

**Identification**

Use the "Hardware Version" and "Product Class" fields to identify the Device Type of the device checking into the ACS. Device manufacturers provide the values used by the device; therefore, device values may vary in their implementation.

When a device checks into the ACS with an unknown Device Type, the ACS automatically creates a type using the device-provided values.

Hardware Version:

Product Class:

**Display**

The ACS uses the "Model Name", "Manufacturer", and "Product Icon URL" fields for display purposes. They identify Device Types in a user-friendly fashion.

Enter a URL, accessible to all ACS users, in the "Product Icon URL" field.

When a new Device Type is created automatically by the system, "Model Name" defaults to a combination of the device-provided Hardware Version and Product Class. You may safely change this value at any time.

WAN Interface Type:

Model Name:

Manufacturer:

Product Icon URL: (44w x 48h)

**Device Type List.** This list displays all the available device types in the system. Click on a device name from the list to open the Device Type Editor.



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.** Use the Device Type Editor to create or edit device types.

 Click to clone and create a new device type based off the current settings. Only appears when editing a pre-existing device type.



 Click to expand the Device Types Editor window 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 to save changes to the device type.

## Using the Device Type Editor

To add a device type to the system


- 1 On the Administration tab, select Device Types.
- 2 Click .
- 3 Enter the device name in the Hardware Version field.
- 4 Enter the device product class in the Product Class field.
- 5 From the WAN Interface Type menu, select the WAN interface type.
- 6 Enter the model name in the Model Name field.
- 7 Enter the manufacturer name in the Manufacturer field.
- 8 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.
- 9 Click .

To edit a device type

- 1 On the Administration tab, select Device Types.
- 2 Select the device name from the Device Types list. The system displays the Device Types Editor window.
- 3 Manually edit the fields.
- 4 Click .

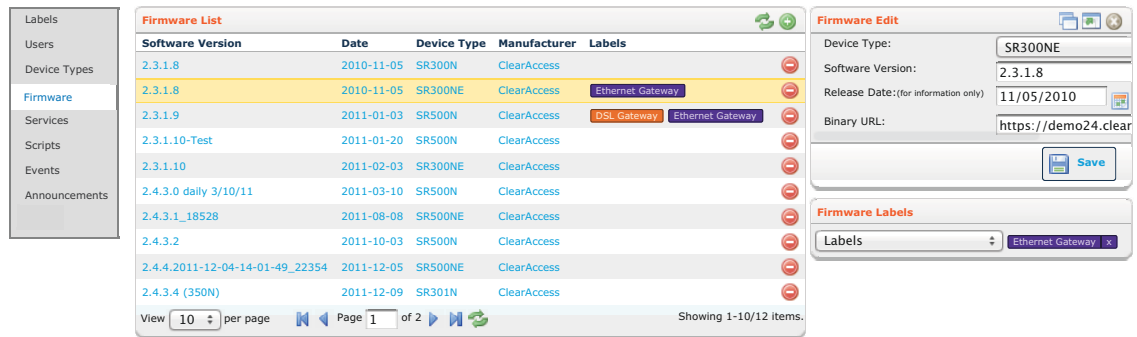


### To delete a device type

- 1 Locate the device type to delete from the Device Types List.
- 2 Click  to remove a device type from the system. The system refreshes the page, listing the remaining device types.

## Managing firmware versions

Use this page to manage firmware versions for the CPE. This page collects various firmware for device types and tracks upgrade paths so that you can make sure that each upgrade is compatible with the previous firmware. If a subscriber's current system has errors, you may want to update or downgrade the firmware that is running on their device.



Software Version	Date	Device Type	Manufacturer	Labels
2.3.1.8	2010-11-05	SR300N	ClearAccess	
2.3.1.8	2010-11-05	SR300NE	ClearAccess	Ethernet Gateway
2.3.1.9	2011-01-03	SR500N	ClearAccess	DSL Gateway Ethernet Gateway
2.3.1.10-Test	2011-01-20	SR500N	ClearAccess	
2.3.1.10	2011-02-03	SR300NE	ClearAccess	
2.4.3.0 daily 3/10/11	2011-03-10	SR500N	ClearAccess	
2.4.3.1_18528	2011-08-08	SR500NE	ClearAccess	
2.4.3.2	2011-10-03	SR500N	ClearAccess	
2.4.4.2011-12-04-14-01-49_22354	2011-12-05	SR500NE	ClearAccess	
2.4.3.4 (350N)	2011-12-09	SR301N	ClearAccess	

View 10 per page Page 1 of 2 Showing 1-10/12 items.

**Firmware Edit**

Device Type: SR300NE

Software Version: 2.3.1.8

Release Date:(for information only) 11/05/2010

Binary URL: https://demo24.clear

Save

**Firmware Labels**

Labels: Ethernet Gateway

**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.

**Firmware Editor.** Use the Firmware Editor to create new or edit firmware releases.

 Click to create a new firmware release based off the current settings.

 Click to expand the Firmware Editor window 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 to save the changes to the firmware.



## Using the Firmware Editor

To add a firmware version to the system

- 1 On the Administration tab, select Firmware.
- 2 Click . The system displays the Firmware Editor window.
- 3 Select the model of device to associate the firmware version to in the Device Type drop-down menu.
- 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 ClearVision. The URL must be accessible to the device.

---

- 7 Click .

To edit a firmware version

- 1 On the Administration tab, select 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 to quickly create new update releases that contain similar information for the previous firmware.

To clone a firmware version

- 1 Click  to create a new firmware version based on current settings.
- 2 Modify and adjust the information in the Firmware Editor.

- 3 Click .



## Managing services

Use the Services pane to manage services offered by your company. You can create new services and edit them directly in this page.

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

The screenshot shows two side-by-side panels. The left panel, titled 'Services', has a sidebar with navigation links: Labels, Users, Device Types, Firmware, Services (selected), Scripts, Events, and Announcements. The main area of the Services panel is a table with columns 'Service' and 'Active'. It lists 17 services with their active status. The right panel, titled 'User Interface Groups', has a table with columns 'Code', 'Name', 'Order', and 'Realm'. It lists 8 groups, including 'cpLocal', 'wireless', 'cpService', 'cpAdvanced', 'Test', 'account', 'service', and 'advanced'. At the bottom of the right panel is an 'Add Group' button and a 'Save' button.

Service	Active
Announcements	false
Bandwidth Monitor	true
Broadband Speed Test	false
Captive Portal	true
Content Filtering	true
Device	true
Energy Management	true
Event Logs	true
Firewall	true
Internet Time Blocking	true
IPTV	false
Local GUI Click Through	true
Local Network	true
Marketing opt-in	false
Parameter Browser	true

Code	Name	Order	Realm
cpLocal	Local Network	1	Control Panel
wireless	My Wireless Network	2	Control Panel
cpService	Parental Controls	3	Control Panel
cpAdvanced	Advanced	4	Control Panel
Test	Test	5	Control Panel
account	Account	1	Portal
service	Services	2	Portal
advanced	Advanced	3	Portal

**Services.** The Services list displays a list of all services in the system.



Click to refresh the Service List. Forces a refresh of all services.



Click to add a new service.



Click to delete a service. (Only available for custom services.)



Click 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.




## Managing user interface groups

User interface groups let you control how services are grouped together on the ClearVision Customer Support tab and on the subscriber's Control Panel. Once you've created the groups that make sense for your users, you then assign new and existing services to those groups.

### To add a user interface group


- 1 On the Administration tab, select the Services pane. The system displays the User Interface Groups pane.
- 2 On the User Interface Groups pane, click .
- 3 In the Code field, enter a unique identifier for this group.
- 4 In the Name field, enter the name of the group.
- 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.
- 6 From the Realm menu, choose where this group appears:
  - Portal: This group will appear on the ClearVision Administrator tab in the Services list
  - Control Panel: This group will appear on the screen used by subscribers to manage their services.
- 7 Click .

### To edit a user interface group

- 1 On the Administration tab, select Services.
- 2 Locate the service on the User Interface Group pane.
- 3 Modify any field.
- 4 Click .

### To delete a user interface group

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

- 1 In the User Interface Groups pane, locate the group you want to delete.
- 2 Click  to delete your custom group from the system. The system refreshes the page, listing the remaining groups.



## Using the Service Editor

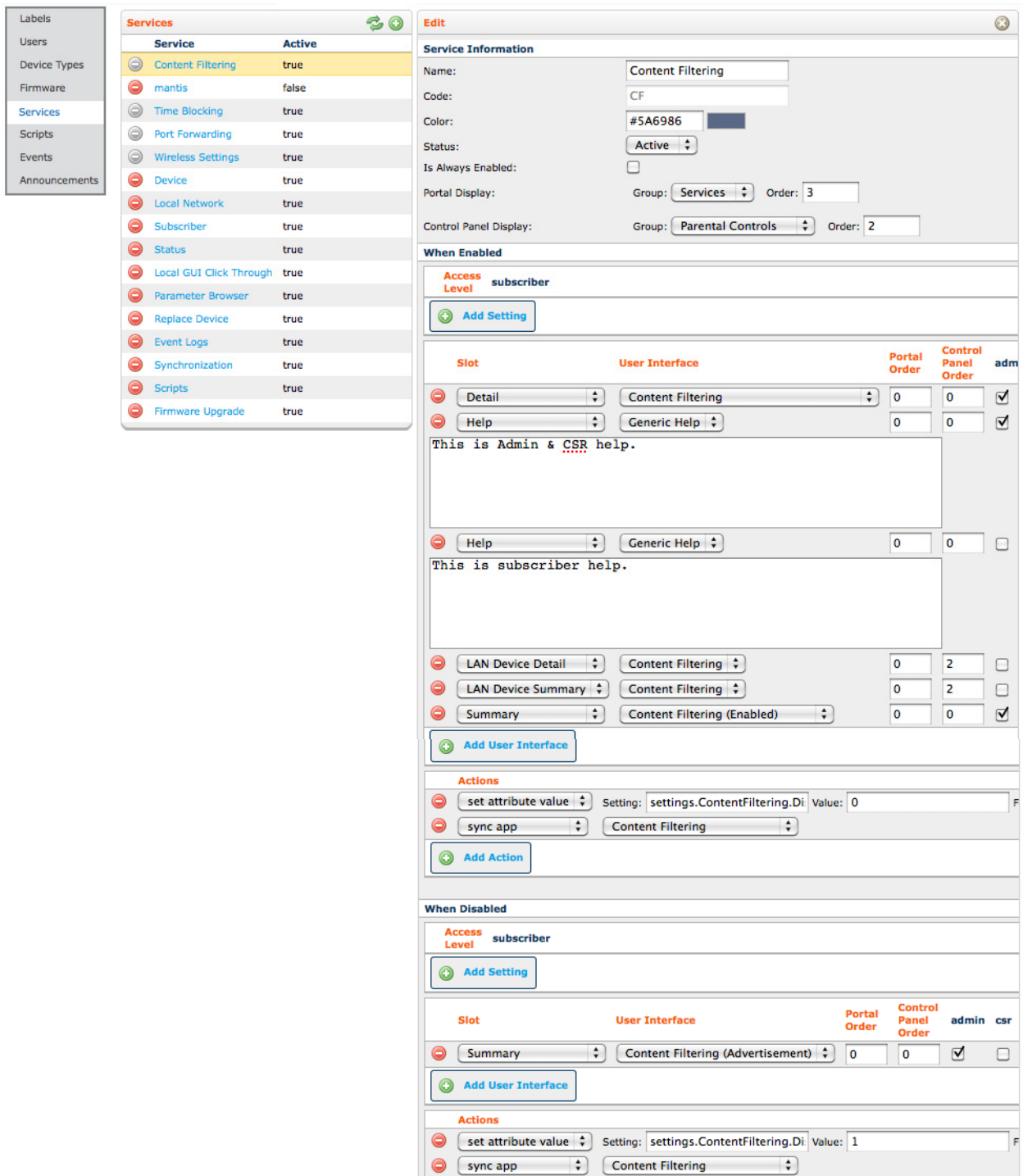
To add a new service

### Step 1: Add Service Information

- 1 On the Administration tab, select the Services pane.



- 2 Click . The system displays the Service Editor window.




The screenshot shows the Service Editor window with the 'Content Filtering' service selected. The left sidebar lists various system components, with 'Services' highlighted. The main window is divided into several sections:

- Services List:** A table showing the status of various services. 'Content Filtering' is highlighted in yellow and set to 'true'.
- Service Information:** Fields for Name (Content Filtering), Code (CF), Color (#5A6986), Status (Active), Is Always Enabled (unchecked), Portal Display (Group: Services, Order: 3), and Control Panel Display (Group: Parental Controls, Order: 2).
- When Enabled:**
  - Access Level:** subscriber
  - Add Setting:** Button to add settings.
  - User Interface:** A table with columns: Slot, User Interface, Portal Order, Control Panel Order, and admin. It lists settings for Detail, Help, LAN Device Detail, LAN Device Summary, and Summary.
  - Actions:** A table with columns: Action, Setting, and Value. It lists 'set attribute value' and 'sync app'.
- When Disabled:**
  - Access Level:** subscriber
  - Add Setting:** Button to add settings.
  - User Interface:** A table with columns: Slot, User Interface, Portal Order, Control Panel Order, and admin. It lists a setting for Summary.
  - Actions:** A table with columns: Action, Setting, and Value. It lists 'set attribute value' and 'sync app'.

- 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.
- 4 In the Code field, enter a unique identifier for this service.



- 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. This color appears next to the service name on the Customer Support tab.
- 6 From the Status menu, choose Active or Inactive. Active services appear on the Customer Support tab; inactive ones do not.
- 7 Do one of the following:
  - Select the Is Always Enabled check box for services that are always enabled.
  - Clear 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.

---

- 8 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.

## Step 2: Configure When Enabled properties

- 1 **Configure Access Level.** Access levels control whether subscribers are able to modify settings for this service.
  - a In the Access Level section, click Add Setting.
  - b Enter the element of the data model that describes the setting (for example, settings.enabled.timeblocking).
  - c From the menu, choose None to deny access or Modify to allow access.
  - d Repeat steps a through c for each access level you want to add.
- 2 **Configure 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 pane 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 on the left navigation of the subscriber's Control Panel.
  - **Help** lets you display helpful information in the subscriber's Control Panel.
  - **Status** is 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 hover 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.
- 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 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. Select the Force check box to change the value regardless of prior setting; clear the Force check box to leave an existing value unchanged.
    - **remove attribute** removes a setting from the data model. Enter the data model element.

### Step 3: Configure When Disabled properties

Add settings, user interfaces, and actions as described in Step 2.




---

**Step 4: Save your changes**

Click  .

To edit a service

- 1 On the Administration tab, select Services.
- 2 Locate the service from the Services List. The system displays the Service Editor window.
- 3 Modify any field.
- 4 Click  .

## Managing scripts

---

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

---

Scripts are implemented using a customized JavaScript-based environment which 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 pane 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 in to the system, scripts are executed on the device in the order in which they were put into the queue.

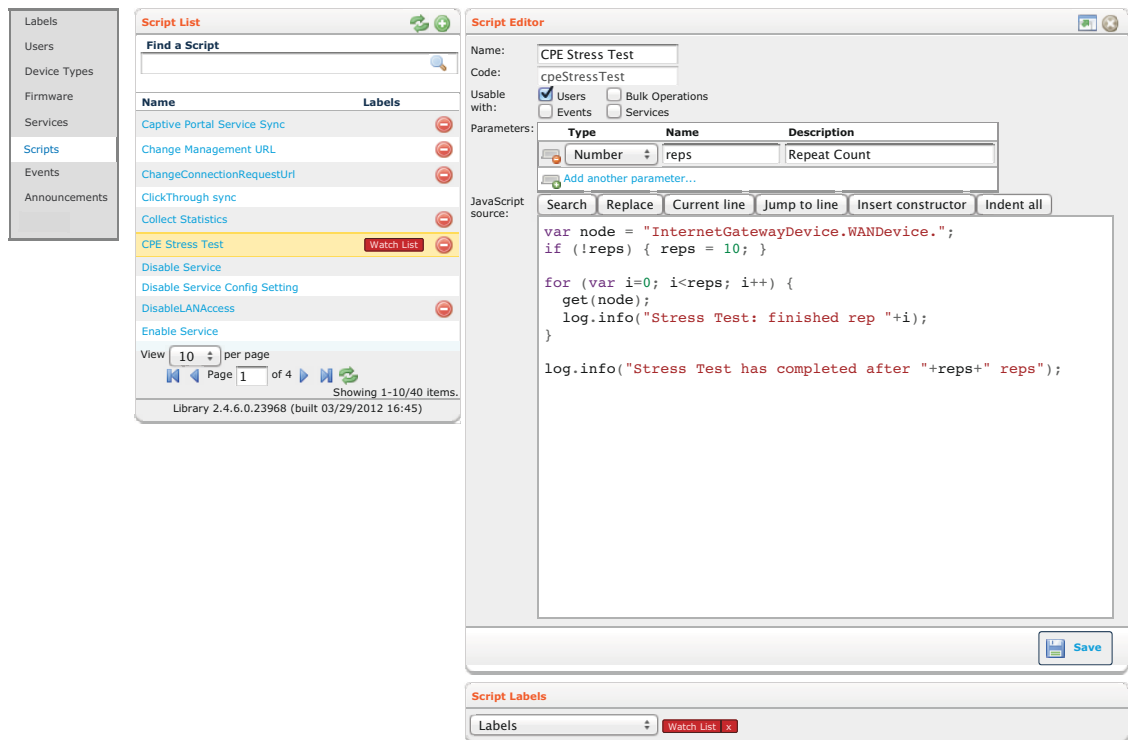
ClearVision contains two types of scripts: bundled and custom.

- **Bundled scripts.** These scripts are bundled with ClearVision.
- **Custom scripts.** These are scripts 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 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.**



**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.



 Click to refresh the Script List.

 Click to add a new script.

Click on 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.

 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 label(s) to the script currently selected.

 Click to save your changes.




## Using the Script Editor

To add a new script

- 1 On the Administration tab, select Scripts.
- 2 Click . The system displays the Script Editor window.
- 3 In the Name field, enter the name of the script.
- 4 In the Code field, enter a unique identifier for this script.
- 5 Select where you want the script to execute. You can select more than one location.
  - Users. Script executes on user accounts.
  - Events. Script executes upon specific events.
  - Bulk Operations. Script executes during bulk operations.
  - Services. Script executes on services.
- 6 Click Add New Parameter and specify its type, name, and description. Click Add Another Parameter to add additional parameters.
- 7 In the JavaScript Source text box, enter the code for the script.
- 8 Select a script label, if appropriate to the action.
- 9 Click .


To edit a script

You can edit any script in the system.

- 1 On the Administration tab, select Scripts.
- 2 In the Script List, click the name of the script to edit. The system displays the Script Editor window.
- 3 Make changes to any of the fields.
- 4 Click .

To delete a script

Only custom scripts can be deleted from the system.

- 1 In the Script List, locate the script you want to delete.
- 2 Click  to delete your custom script from the system. The system refreshes the page, listing the remaining scripts.



## Managing events

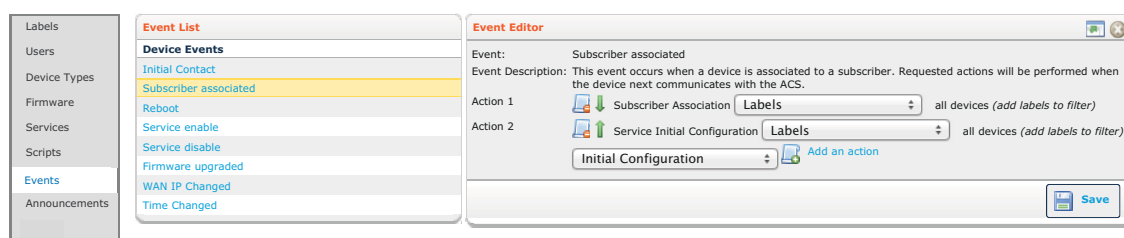
An event is a pre-defined occurrence on a CPE that triggers scripts at specified moments. They represent various points within the device's lifecycle. You cannot add new events to the list but you can add new scripts to be run at each event point. An event can have multiple scripts. However, each script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

ClearVision defines the following types of events:

- **Initial Contact.** This event occurs when the server sees the CPE appear on its network for the first time.
- **Subscriber Associated.** This event occurs when a device is associated to a subscriber. It also occurs when a future device informs for the first time.
- **Reboot.** This event occurs when the CPE reboots due to a power outage or specific request. It also typically occurs with Initial Contact.
- **Service Enable.** This event occurs after a service is enabled on a device.
- **Service Disable.** This event occurs after a service is disabled on a device.
- **Firmware Upgraded.** This event occurs when firmware is upgraded.
- **Inform.** This event occurs every time the CPE contacts the server, after any previously scheduled actions have run. Because this happens so frequently, it's 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.



Use the Events pane 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.



**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 ones.


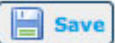
 Click to expand the Event Editor window to full size. When in full-size mode, click  to restore the window to its original size.

 Click to cancel the event and discard your changes.



 Click to save your changes.

## Using the Event Editor

### To add a new Event Action

- 1 On the Administration tab, select Events.
- 2 Select an event from the Events List. The system opens up the Event Editor window.
- 3 Select an action from the Action drop-down menu.
- 4 Click  to add the action to the event. Some actions may require user input to complete and will display the appropriate fields.
- 5 Click .



### To edit an Event Action

- 1 On the Administration tab, select Events.
- 2 In the Event List, click the name of the event.
- 3 In the Event Editor, click the name of the action.
- 4 Edit the properties for the action, if any.
- 5 Use the  and  icons to rearrange the order in which the actions execute.



- 6 Click  .

To delete an Event Action

- 1 On the Administration tab, select Events.
- 2 In the Event List, click the name of an event.
- 3 Click  next to the action you want to delete from the event.
- 4 Click  .

## 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 installation of ClearVision is set up. Announcements can be configured as a standalone service, or an announcements panel can be added to another service.

---

ClearVision supports the following types of announcements:



Information announcements



Warning announcements





Alert announcements



## Using the Announcements Editor

You use the Announcements editor to create your announcements.

### To add a new announcement

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

### To edit an announcement

- 1 On the Administration tab, select Announcements.
- 2 Edit announcements as desired.
- 3 Click  .

### To delete an announcement

- 1 On the Administration tab, select Announcements.
- 2 Locate the announcement to delete and click Delete.



## Chapter 9

# Reviewing Audit Logs

Audit logs give you a view into exactly what is happening on your system. The audit log records every transaction and event. Click the Audit tab to access your audit logs.

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

Two filters help you find the information you want:

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

Portal users are Admin or CSRs, who can make changes to device or subscriber records and to other portal users' accounts.

Subscribers are customers who can make changes to their devices through the Control Panel. The audit log will show 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.

**Audit**

**Search Audit Logs**  
Please select a start and end date for your search, you may further refine the results by using the filters below.

From: 04/19/2012 To: 04/24/2012

**Filter Transactions:**

Changed By: Portal User (amerriwether)

Applied To: Device (00255E6E05EE)

**Search**

**Results**

Summary: 27 transactions returned. [expand all](#) - [collapse all](#)

**Date:** Tue Apr 24th 2012 15:53:42  
**Transaction:** amerriwether(user) changed 16 fields on device(00255E6E05EE)  
[Changes +](#)

**Date:** Tue Apr 24th 2012 15:53:40  
**Transaction:** amerriwether(user) changed 2 fields on device(00255E6E05EE)  
[Changes -](#)

applications.CF.dto.Settings.ContentFiltering.Hosts.1.Server	was: <b>mature_teens</b> now: <b>young_teens</b>
applications.CF.dto.Settings.ContentFiltering.Default.Server	was: <b>young_teens</b> now: <b>mature_teens</b>

**Date:** Tue Apr 24th 2012 15:53:01  
**Transaction:** amerriwether(user) changed 1 fields on device(00255E6E05EE)  
[Changes +](#)

**Date:** Tue Apr 24th 2012 15:52:46  
**Transaction:** amerriwether(user) changed 9 fields on device(00255E6E05EE)  
[Changes +](#)

To view the audit log

- 1 Click the Audit tab.
- 2 In the Audit dialog, specify a range of dates to display information for.



- 3 The default is the past five days.
- 4 (Optional) From the Changed By menu, choose Portal User, Subscriber, or System. Enter the username of a portal user or a subscriber code. Leave blank for System.
- 5 (Optional) From the Applied To menu, choose Bulk Operation, Device, Portal User, or Subscriber. Enter a device serial number, a portal username, or a subscriber code. Leave blank for Bulk Operation.
- 6 Click Query.

ClearVision displays the audit results. 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.

You can also view the results through a web service, which displays a comma-separated (.csv) file of results.

To view .csv-formatted results

- 1 In the Results pane, click .
- 2 Click **webservice**.



# Managing bulk operations

---

---

[Creating bulk operations 100](#)

---

[Examples for bulk operations 100](#)

---

[Best practices for working with bulk operations 106](#)

---

[Understanding bulk operation options 108](#)

---

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.

---

**Note.** Certain bulk operation actions may be limited when using third-party CPEs. Please contact Cisco Customer Support if you have any 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 in to the auto configuration server (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.

Here are some things you can do with bulk operations:

- Stage complicated WAN changes
- Silently accomplish firmware updates
- Enable and disable services
- Cause browser redirection for CPEs having 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.



## Creating bulk operations

In general terms, the steps to create a bulk operation are:



The examples in the following section describe how to create bulk operations.

## Examples for bulk operations

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

### Scenario: Update Firmware on All SR100G CPEs

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

For this example, let's 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 8, 2010, and you want it to run during your maintenance window, which is Mon-Fri from 12:01 AM to 5:59 AM.


- 1 In ClearVision, select the Bulk Operations tab.

The system displays a list of existing bulk operations.


Find

Create

Bulk Operations						
Name	Beginning Date	Occurs	Status	Delete		
Update SR100G firmware to 2.3.1.8	11/10/2010	Once	Completed			
john	02/16/2011	Now	Cancelled			
Service through bulk op	06/01/2011	Now	Completed			
test content filter enable	06/20/2011	Now	Completed			
Resync STUN	09/20/2011	Now	Completed			

- 2 Click  to add a new bulk operation.
- 3 In the Name field, enter a descriptive name for the operation.
- 4 Do one of the following:
  - To contact devices without waiting for an inform, select the Solicit Devices check box.
  - To wait for an inform to run the operation, clear the Solicit Devices check box.



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

Find
Create

### Create Bulk Operation

**Bulk Operation**

**Name:** Upgrade SR500NE firmware to 2.4.3.5

**Solicit Devices:** ☒ (contact 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

Name	Value
The name of the firmware image to upload	2.4.3.5 (2012-01-09)

**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**

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
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

**May 2012**

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	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	5	6	7	8	9

**June 2012**

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	31	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
1	2	3	4	5	6	7

**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**

Search this list: enter keywords

- Captive Portal Active Configuration
- 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
- Control Panel Application Message

**Filter Criteria**

and Drag a column from Available Columns here to refine results.

☐ Advanced Syntax

- 6 From the Action menu, select 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.



- 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 here, you see an expandable area that shows you exactly which devices will be affected by this bulk operation, if the bulk operation is run at this time.

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

- 8 From the Run menu, chose Once.
- 9 Set the following scheduling parameters.
  - Beginning date: 4/28/2012
  - Day of week: Mon, Tues, Wed, Thu, Fri
  - Run from: 12:01 AM
  - Run to: 5:59 AM

- 10 Click Create.

The bulk operation is listed on the Find pane along with the operation's scheduled beginning date, frequency, and status.

Find

Create

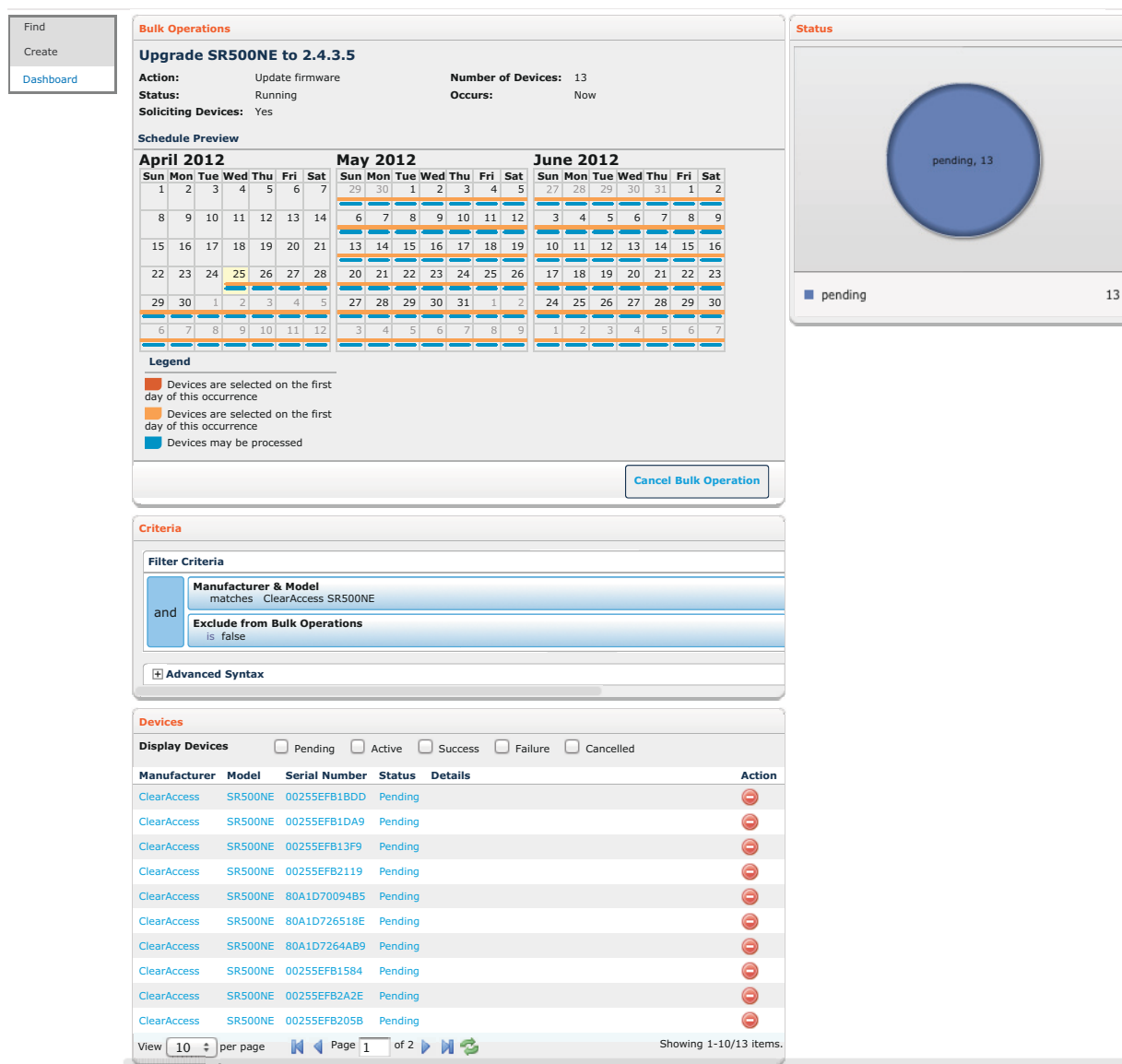
Bulk Operations

Name	Beginning Date	Occurs	Status	Delete
Update SR100G firmware to 2.3.1.8	11/10/2010	Once	Completed	<div></div>
john	02/16/2011	Now	Cancelled	<div></div>
Service through bulk op	06/01/2011	Now	Completed	<div></div>
test content filter enable	06/20/2011	Now	Completed	<div></div>
Resync STUN	09/20/2011	Now	Completed	<div></div>
Upgrade SR500NE firmware to 2.4.3.5	04/28/2012	Once	Scheduled	<div></div>



## Viewing bulk operation progress

Once the update starts, you can click the name to see a dashboard view of the operation's progress.



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 selecting 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 having each status.
- A pie chart shown the failure results along with error codes.



## Scenario: Enable Content Filtering on all CPEs

When you deploy a new service, you may want to enable it on all CPEs as a promotional event. This scenario 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.

- 1 On the Bulk Operations tab, select the Create pane.
- 2 In the Bulk Operation section, do the following:
  - Enter a name for the operation.
  - From the Action menu, choose Enable Service.
  - From the Parameters menu, choose Content Filtering.

- 3 From the Run menu, choose Once and set the following scheduling parameters.
  - Beginning date: 4/30/2012
  - Select all days of the week.
  - Select All Day.



- 4 Specify your zip code filter to limit the promotion to a subset of Atlanta zip codes.
  - 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**.

The screenshot shows a web interface for configuring filters. On the left, the 'Available Columns' section has a search bar with the text 'enter keywords' and a list of columns: Manufacturer & Model, Model, Notifications Application Message, Notifications Application State, OUI, Port Forward Application Message, Port Forward Application State, Port Forward Description, Postal Code, PPP Application Message, and PPP Application State. On the right, the 'Filter Criteria' section shows a filter rule: 'Postal Code is between 30300 and 30399'. Below this, there is a dashed box with the text 'Drag a column from Available Columns here to refine results.'.

- 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 which you should fully understand before you use it. It is possible to adversely affect your subscribers' services if you do not understand the actions you schedule.

---

### 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 will interfere 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 pane, and clearing 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 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 appropriate maintenance time window. Between 2:00 a.m. and 5:00 a.m. is a suggested time window.
- Remember 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 expect 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 expect to go through the bulk update process in 23 days.

### Troubleshooting failed bulk operations

Bulk Operations rarely fail on all CPEs, if you have set the operation set up correctly. However, there can be "failed actions" on a particular CPE. In this case, ClearVision does not attempt to re-run the action against that CPE.



If the operation is scheduled to run multiple times, the CPE may “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 will 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 goes off and grabs N CPEs from the result set (the list of CPEs that are part of the bulk operation) to solicit. It then goes off and solicits the CPEs, and the spacing between those solicits is `bulkOp.minimumTimeBetweenSolicitsMS`.

Every `bulkOp.timeBetweenSolicitingSchedulerSecs` seconds, the engine looks to see if there are any 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 amount of CPE sessions that are active. For example, if `tr069.maxConcurrentSessions` is set to 100, and `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:** Validate 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 may need to perform interim updates prior to updating them to the current version. Please contact Cisco Customer Support if you have questions.
- **Firmware definitions:** View the firmware definition on the Firmware pane 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 ClearVision to select the pool of CPEs to be acted on.

**CPE Selection.** The CPEs you want this operation to run on.



## About 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.

ClearVision 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 pane 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. If you would like to create a custom service, please contact Cisco Advanced Services.

## About schedule options

Bulk operations can be scheduled to run Now, Once, Weekly, or Monthly.

If you choose...	The ACS creates a list of CPEs that meet your criteria...	And the action runs on the list of CPEs...
Now	When you click Create	When you click Create
Once	On the Beginning Date	On the first scheduled weekday after the Beginning Date
Weekly	First time. On the Beginning Date Each subsequent time. On the same weekday every week For example, if the Beginning Date is Tuesday, February 2nd, a new list of CPEs is chosen each Tuesday after that date.	On the first scheduled weekday after the Beginning Date and every scheduled day thereafter
Monthly	First time. On the Beginning Date 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.	On the first scheduled weekday after the Beginning Date and every scheduled day thereafter



---

## About 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 scenarios.**
- **If you have ClearAccess 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 pane.**



# Using Utilities

---

---

[Utilities overview 111](#)

---

[Importing subscriptions 112](#)

---

[Using the RESTful service tool 113](#)

---

## Utilities overview

Utilities provide administrators with the following tools to troubleshoot their system:

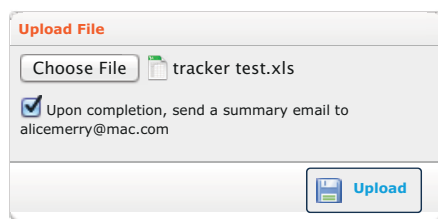
- **Import Subscriptions.** This tool allows you to batch upload your subscriber data.
- **RESTful tool.** A diagnostic tool. See “RESTful Service Tool Page Overview” on page 96.



## Importing subscriptions

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 Comma Separated Value (CSV) and must conform to the format described in *Appendix B, Subscription Import File Format*.



**Choose file.** Click this button to open a dialog window that allows you to find the CSV file to upload.

**File path.** This text shows the file to be uploaded.

**Check the box to send a summary email when import is completed.**

**Upload button.** Click this button to upload a CSV file. It will process and load subscriber information in to the database.

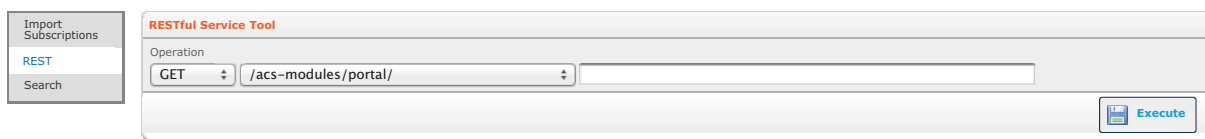
### To import multiple subscriptions

- 1 On the Utilities tab, select Import Subscriptions.
- 2 Click Choose File. A system dialog box appears.
- 3 Choose a CSV file to upload.
- 4 Click Upload button. ClearVision imports your data, displays a progress bar, and informs you of success.



## Using the RESTful service tool

The RESTful service tool enables you to run actions against URLs and to directly call the integration API.



The screenshot shows a web interface for the RESTful Service Tool. On the left is a sidebar with three buttons: 'Import Subscriptions', 'REST' (highlighted in blue), and 'Search'. The main area has a title bar 'RESTful Service Tool'. Below it, the 'Operation' section contains a dropdown menu with 'GET' selected, followed by a text input field containing '/acs-modules/portal/'. To the right of the text field is an empty input field. At the bottom right of the main area is a blue button with a play icon and the text 'Execute'.

**RESTful Service Tool.** This tool enables admins to enter URLs and call the integration API directly.

**Operation.** Select an HTTP verb from the drop-down menu, and enter a URL in the text box.

**Execute.** Click to run that operation on the desired URL.



---

## References



# Glossary

---

## A

### ACS

Automated configuration service. Software like ClearVision.

### Administrator role

A user role in that gives users full access to all features and functions in the system. Referred to in the manual as admin.

### Attribute

A unit of data associated to a device or subscriber.

## C

### CPE

Customer premise equipment. Also known as a gateway.

### Customer support role

A user role that allows access to the Customer Support tab.

## D

### Device

Any piece of equipment that the system can track.

## E

### Event

A pre-defined occurrence on a CPE that triggers actions to occur at specified moments. Events represent a notable point within the device's lifecycle.

## I

### Inform

The act of a managed device connecting to the system and receiving updates.

## L

### Label

Arbitrary tags which can be added to certain items in the system to enable grouping for easy searching.

## M

### Managed device

A device which possesses the traits necessary to be managed by the system.



---

## **O**

### **OUI**

Refers to manufacturer ID. Also known as the first 6 characters of the MAC address.

## **P**

### **Property**

A property is a single named piece of configuration data.

## **R**

### **Reporting administrator role**

A user role that allows access to the Reports tab.

## **S**

### **Script**

Code written in the JavaScript language which can be executed by the system.

### **Service**

A capability that can be enabled for a device/subscriber account.

### **Subscriber**

An end user who has devices managed by the system.

### **Subscription**

A set of packages to which a device is subscribed.



## Appendix B

# Subscription Import File Format

The file format for importing subscriptions is a ISO-8859-1 encoded CSV file. The first line of the file contains headers with the following meanings.

Column	Appearance	Description
Operation	Optional	+ or -, causing the record to be either updated or removed. Omitting this column will cause the column to be treated as if it were being updated.
SubscriberCode	Required	A unique identifier for the subscriber.
SerialNumber	Required, unless ProvisioningCode	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.
OUI	Required, unless ProvisioningCode	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.
ProvisioningCode	Required, unless SerialNumber/OUI	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 SerialNumber / OUI gains precedence.
Subscriber.(PropertyName )	Optional, multiple	This column header specifies a subscriber property name.
Service.(ServiceName)	Optional, multiple	This column header specifies a service which is already defined in the system. Values for rows under this column can be on or off.
Settings.(PropertyName)	Optional, multiple	This column header specifies a settings property name.
Label.(PropertyName)	Optional, multiple	This column header specifies a label which is already defined in the system. Values for rows under this column can be on or off.
CP.UserName	Optional, but required if there is a CP.Password, CP.OverwriteLogin, or a CP.SendEmail field.	The subscriber's Control Panel user name. If credentials already exist and CP.OverwriteLogin is not set to on, an error message will be displayed and the credentials will not be changed.
CP.Password	Optional, but required if there is a CP.UserName, CP.OverwriteLogin, or a CP.SendEmail field.	The subscriber's Control Panel password. If credentials already exist and CP.OverwriteLogin is not set to on, an error message will be displayed and the credentials will not be changed.



Column	Appearance	Description
CP.OverwriteLogin	Optional, but required if there is a CP.Password, CP.UserName, or a CP.SendEmail field.	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.
CP.SendEmail	Optional	This column header specifies whether or not to send an email to the subscriber containing their Control Panel login credentials. The email address is specified in Subscriber.EmailAddress. Values for rows under this column can be on or off.

## Sample CSV file

```

SerialNumber,DOI,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
0000000f4240,000000,,jada-clark-f4240,JadaOwens,jada.clark.1000000@test.com,mailing,Cleveland,WA,5630
OakWay.,98296,home,311-188-3268,off,off
0000000f4241,000000,,alexander-le-f4241,AlexanderLe,alexander.le.1000001@test.com,mailing,Clayton,ID,8520 Silent
Blvd.,91464,home,909-808-3883,off,off
0000000f4242,000000,,mateo-williams-f4242,Mateo
Williams,mateo.williams.1000002@test.com,mailing,Centerville,TD,2530 Battery
Rd.,92827,home,604-218-5762,on,off
0000000f4243,000000,,isaiah-cox-f4243,IsaiahCox,isaiah.cox.1000003@test.com,mailing,Bellevue,ID,3630 Martin Luther King
Ave.,20082,home,205-420-2107,off,off

```