CMS Overview

Release 3.0

Notice to Users

2WIRE PROVIDES NO WARRANTY WITH REGARD TO THIS MANUAL, THE SOFTWARE, OR OTHER INFORMATION CONTAINED HEREIN AND HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE WITH REGARD TO THIS MANUAL, THE SOFTWARE, OR SUCH OTHER INFORMATION, IN NO EVENT SHALL 2WIRE, INC. BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, OR SPECIAL DAMAGES, WHETHER BASED ON TORT, CONTRACT, OR OTHERWISE, ARISING OUT OF OR IN CONNECTION WITH THIS MANUAL, THE SOFTWARE, OR OTHER INFORMATION CONTAINED HEREIN OR THE USE THEREOF.

2Wire, Inc. reserves the right to make any modification to this manual or the information contained herein at any time without notice. The software described herein is governed by the terms of a separate user license agreement.

Updates and additions to software may require an additional charge. Subscriptions to online service providers may require a fee and credit card information. Financial services may require prior arrangements with participating financial institutions.

8132009

5100-000758-000

Contents

About this Guide

The *CMS Overview* provides an introduction to the 2Wire Component Management System (CMS). It includes details about product functionality and concepts.

The following information is included:

- Introducing CMS. Provides an overview of CMS and how it fits into the service provider's infrastructure.
- Working with Devices. Describes how devices are managed by CMS.
- Managing Devices with Organizations. Describes how devices are configured in CMS, using organizations, policies, and a policy hierarchy.
- Glossary. Provides a list of terms frequently used in association with CMS.

Audience

This guide is intended for anyone who wants to familiarize themselves with basic CMS functionality. It does not provide details for implementing any CMS features.

Style Conventions

The following style conventions are used in this guide:

Note Notes contain incidental information about the subject. In this guide, they are used to provide additional information about the product and to call attention to exceptions.

Typographical Conventions

Convention	Used For
Blue Text	Cross references
Bold	Interface elements that are clicked or selected
Italic	Emphasis, book titles, variables, list terms
`Monospace`	Command syntax and code
`Monospace Italic`	Variables within command syntax and code

Related Documents

In addition to this guide, the CMS documentation library includes:

- *CMS API Reference*. Lists details about the CMS Application Programmer Interface (API) and its web services, which enable CMS to integrate with external Business Support Systems (BSS) and Operations Support Systems (OSS).
- *CMS Installation Guide*. Provides instructions for installing and configuring the out-of-box implementation of CMS.
- *CMS Management Console Help*. Provides detailed instructions for working with the CMS Management Console web application.
- *CMS Release Notes*. Specifies system requirements, known issues, and resolved issues for the current release.

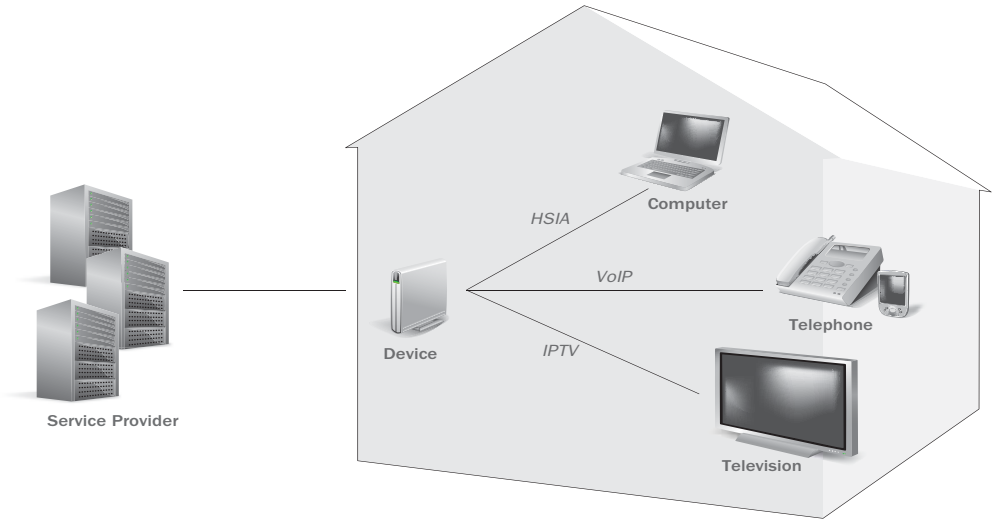
CHAPTER 1

Introducing CMS

The 2Wire Component Management System (CMS) enables telecommunications service providers to manage devices that connect a subscriber's network to the service provider's network. These devices, as well as the computers, telephones, televisions, and other equipment that may be connected to them, are used in conjunction with services such as:

- High-Speed Internet Access (HSIA)
- Voice over Internet Protocol (VoIP) telephone service
- Internet Protocol Television (IPTV)

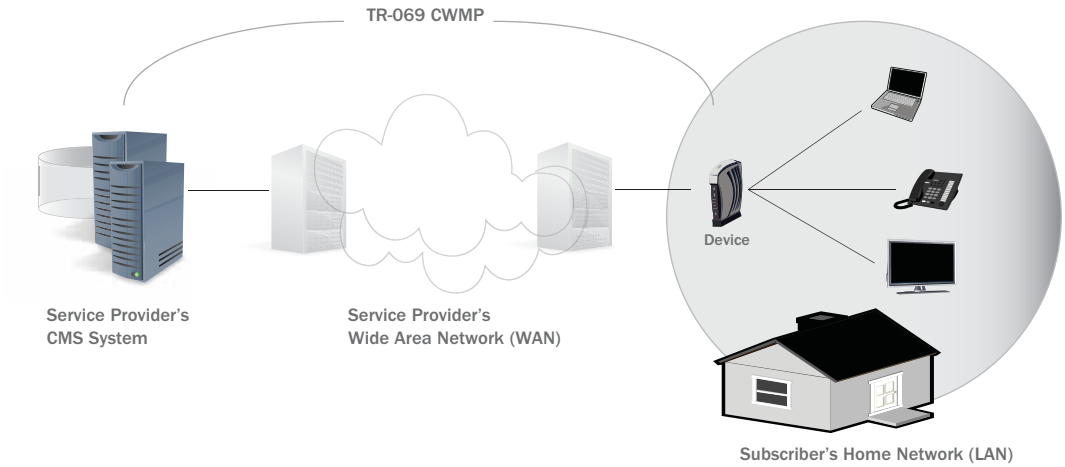
Using CMS, service providers support these services by managing devices from 2Wire as well as other vendors.



CMS enables the service provider to configure the device, ensure that device firmware is always up-to-date, and resolve subscriber issues.

Communicating with Devices using CWMP

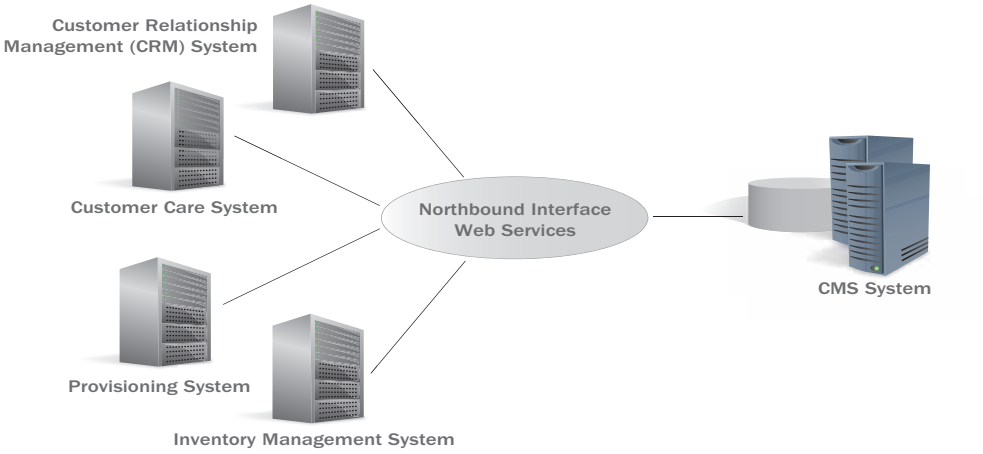
Devices connect the subscriber's local area network (LAN) to the service provider's wide area network (WAN). CMS communicates with devices remotely using CPE WAN Management Protocol (CWMP), the industry-standard protocol defined in TR-069 for remote device management.



As devices operate, they send CWMP messages regarding their status. CMS monitors these incoming CWMP messages and performs actions based on them and other events. These sets of actions initiated by CMS are called workflows. In CMS, users can configure which workflows are run in response to which events. For more information about events and workflows, see Responding to Events with Workflows on page 11.

Communicating with OSS and BSS Applications

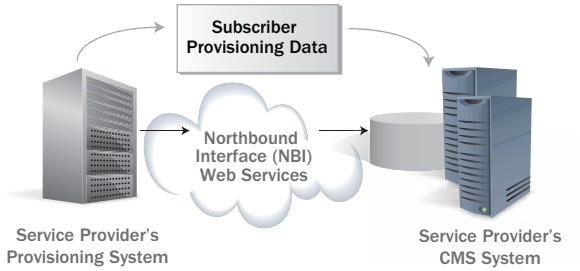
Using web services associated with the CMS Northbound Interface (NBI), CMS can be integrated into the service provider's existing IT environments to interact with Operational Support System (OSS) and Business Support System (BSS) applications. After they are integrated, the OSS and BSS systems can call CMS to perform tasks that are part of larger business operations, such as provisioning services. In addition, service providers can gather data to evaluate their deployments using Customer Relationship Management (CRM), customer care, provisioning, and inventory management systems.



For example, a device must be associated with a subscriber before CMS can provision services on the device. This is accomplished with the help of the service provider's provisioning system, in a scenario such as the following:

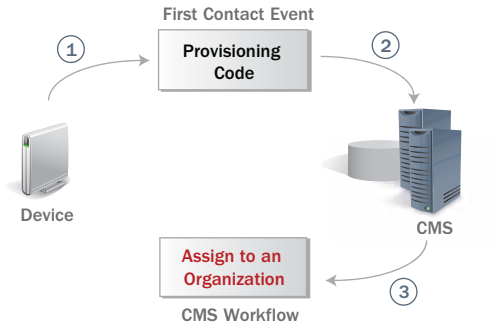
Service Provider Adds Subscriber and Pre-Provisions Services

When a subscriber purchases a new service, the service provider's provisioning system adds information about the subscriber to CMS and pre-provisions services using NBI web services.



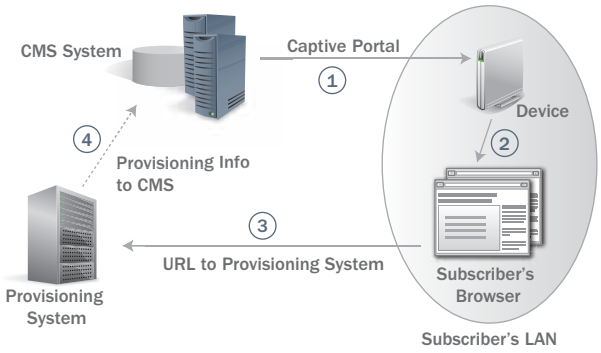
Device Communicates Its Provisioning Code to CMS

When the subscriber connects a device to the service provider's network, the device communicates its provisioning code to CMS. CMS associates the device to the organization that uses that provisioning code.



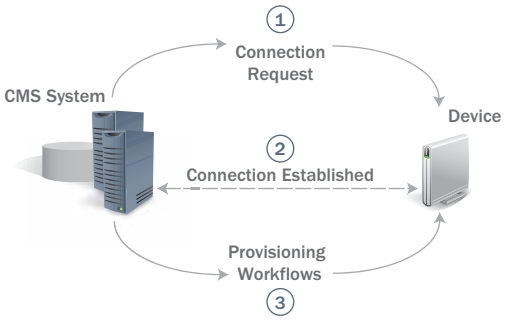
Provisioning System Associates Device and Subscriber

CMS configures captive portal on the device. The subscriber's browser is directed to a registration URL that interacts with the provisioning system. After the subscriber registers the device and new service, the provisioning system matches the device with the subscriber and passes that information to CMS. The device is removed from the captive portal after registration is complete.



CMS Runs Provisioning Workflows

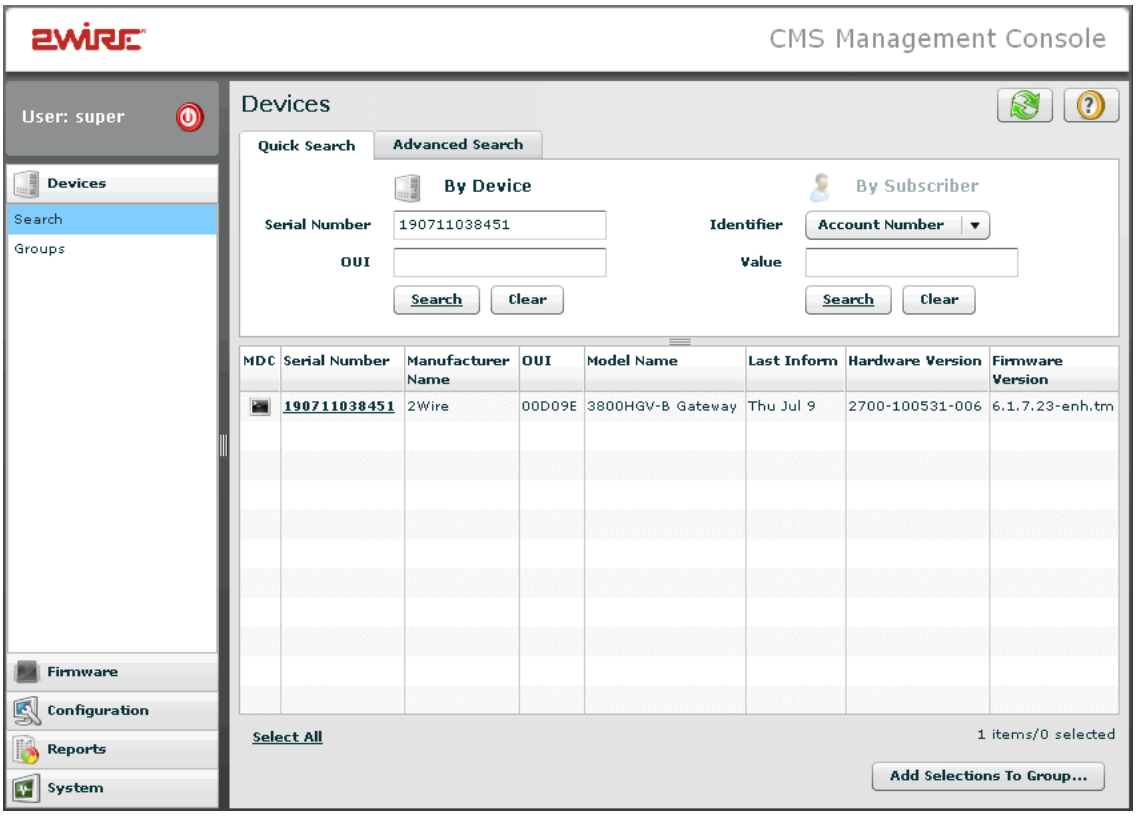
CMS sends a connection request to the device. Upon contact, CMS runs the provisioning workflows associated with the services purchased by the subscriber.



After the device and services are provisioned, CMS can configure and manage the device according to the organization's policy hierarchy.

Working with the CMS Management Console

The CMS Management Console, which is a web application secured with Secure Sockets Layer (SSL), enables users to manage devices and perform administrative tasks related to CMS. Users access the CMS Management Console with a user name and password and can perform any tasks permitted by their security roles.



Using the CMS Management Console, CMS users can perform tasks such as the following:

- Search for devices
- Create groups of devices for easy management
- Create organizations and policy hierarchies that define device configuration
- Troubleshoot device problems
- Schedule firmware upgrades
- View reports

For more information, see *CMS Management Console Help*, which is available within the CMS Management Console web application. The CMS Management Console is available from the following address:

https://*hostname*:*internal-port*

Contact your CMS administrator for the host name and port information and for a user name and password.

CHAPTER 2

Working with Devices

A device is the hardware that connects the subscriber's local area network (LAN) to the service provider's wide area network (WAN), such as a residential gateway (RG) or TR-069 VoIP phones. Devices can be configured and managed by CMS.

Some devices have dependent devices that work in conjunction with the main device. For example, an intelligent Network Interface Device (iNID) is an RG installed outside a subscriber's home. It works with one or more remote bridges inside the home to provide services. These remote bridges are considered dependent devices and are accessed in the CMS Management Console through their iNID counterpart.

Organizing Devices with Groups

A group is a collection of devices bound together for scheduled firmware upgrades and bulk data collection. Refer to Keeping Device Firmware Upgraded on page 6 and Collecting Bulk Data on page 7.

Group membership is based on one of the following:

- *A search expression*. A search expression defines device characteristics and the conditions under which a device is a match for the group. Members of the group can change over time, based on the search expression associated with the group.

  For example, firmware version 2.3.4 has been released for devices with a hardware version of 135.357.579. Devices with a firmware version of 2.3.2 and 2.3.3 need to be upgraded to this new version. A group can be created to include only devices that meet this criteria using the following expression:

  ```
  HardwareVersion==135.357.579 AND
  (FirmwareVersion==2.3.2 OR FirmwareVersion==2.3.3)
  ```

  As new devices that meet this criteria are added to CMS, the number of devices in this group will increase. If a firmware upgrade is scheduled for this group, the number of devices will decrease as each device is upgraded and no longer meets the expression criteria.
- *A list of specific devices*. Members of a group of specific devices are set and do not change unless the group is modified manually. This is useful if a search expression is not specific enough or if the membership of the group must stay the same.

Keeping Device Firmware Upgraded

Device firmware is stored on a firmware server, typically associated with a Content Distribution Network (CDN). CMS users configure which firmware versions are associated with which devices.

CMS triggers firmware upgrades automatically according to the configuration set for the organization level associated with the device. (Refer to Managing Devices with Organizations on page 9.) When a subscriber purchases a device, the firmware on the device may be outdated. Each organization has a list of firmware upgrades that ensures that the devices in the organization have updated firmware versions installed.

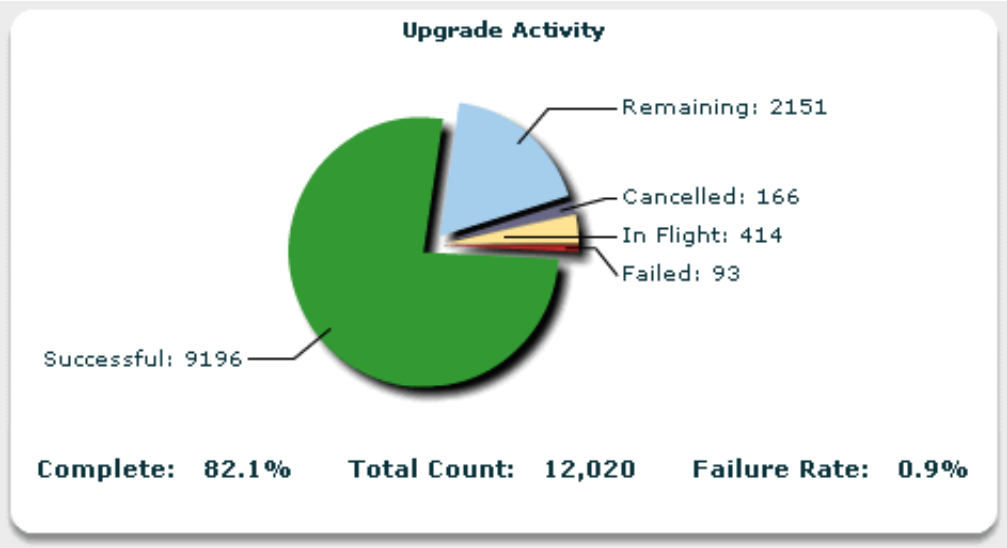
In addition, upgrades can be scheduled for a specific group. When a new firmware version becomes available, the service provider may be required to upgrade an enormous number of devices. CMS provides support for a scheduled upgrade that occurs during a defined maintenance window either once or at regular intervals. Updating millions of devices to a new firmware version may require several weeks of upgrades, which can be accomplished through a single, recurring scheduled upgrade entry.

For example, firmware version 2.3.4 has been released for devices with a hardware version of 135.357.579. Devices with a firmware version of 2.3.2 and 2.3.3 need to be upgraded to this new version.

The CMS administrator ensures that the firmware is saved on the firmware server or the associated CDN, imports the firmware manifest into CMS, and schedules the upgrade. This upgrade entry associates a group of devices to be upgraded, the new firmware version information, the percentage of upgrades that can fail before the upgrade is cancelled automatically, and the window of time when the upgrade can be installed. The window for this upgrade is from 12:00 A.M. to 4:00 A.M., Monday through Friday.

As the upgrade progresses, the CMS administrator monitors the progress in the CMS Management Console, which displays information such as the following:

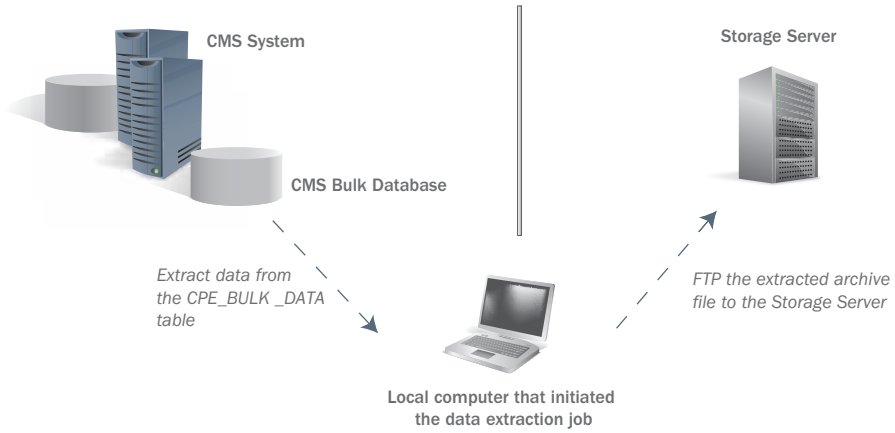
- The number of successful, remaining, cancelled, in flight, and failed upgrades.
- The percentage complete.
- The total number of devices affected.
- The failure rate.



Collecting Bulk Data

Bulk data collection enables service providers to regularly collect and store large numbers of device parameters, such as TR-069 and TR-98 parameters. CMS retrieves these parameters from the devices in the specified group during periodic informs at defined collection intervals. CMS then stores this data in a database that is configured during CMS installation.

Service providers can report on the data in the bulk database directly using their own reporting solution. Alternately the data can be extracted from CMS and transferred to a data warehouse, where it can be consumed by Operational Support System (OSS) and Business Support System (BSS) systems.



Resolving Device Issues

Technical support users can log on to the CMS Management Console to view device details, run diagnostics, reboot devices, upgrade device firmware versions, and perform other operations to resolve subscriber issues.

For example, firmware version 2.3.4 has been delivered to the service provider, and is scheduled to be deployed to the relevant devices during the next scheduled maintenance window. A subscriber calls technical support with a problem that is known to be fixed in the new firmware release. In the CMS Management Console, the Support user searches for the subscriber and upgrades the subscriber's device, since firmware version 2.3.4 is known to fix the subscriber's problem. After the upgrade, the device is rebooted and the problem is resolved.

CHAPTER 3

Managing Devices with Organizations

When a device first makes contact with the service provider, it communicates a provisioning code to CMS. This code is associated with an organization that defines how the device is configured and managed by CMS.

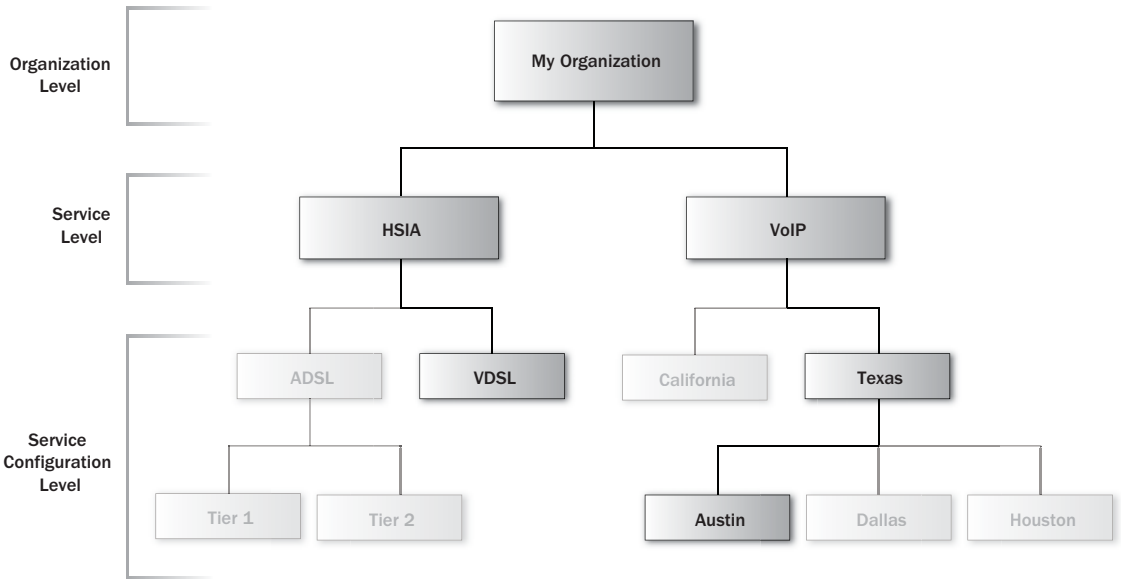
An organization has a policy hierarchy that enables users to specify the rules that govern how services are managed. A policy hierarchy has three levels: the global organization level, the service level, and the service configuration level. The nodes at each level of the policy hierarchy have policies that define how devices are managed, but how devices are selected for policy application at each level varies.

- At the organization level, membership is determined by provisioning code. If a device has a provisioning code that matches the organization, the policies for the organization are evaluated for the device.
- At the service level, membership is determined by the services that have been purchased by the subscriber. If a device is associated with a service, the policies for the service are evaluated for the device. When a device is provisioned for multiple services, CMS takes the order of the services into account when applying policy.
- At the service configuration level, membership is determined by simple comparison expressions that refine which devices have which policy applied. These expressions compare the properties that CMS knows about a device (such as IP address or OUI), as well as custom properties configured by 2Wire Professional Services.

  The configuration level allows sub-levels to further refine a service. At each service configuration level, only a single property is allowed and all expressions in a given level must be unique.

For example, for an HSIA service, Asymmetric Digital Subscriber Line (ADSL) and Very High Bitrate Digital Subscriber Line (VDSL) need to be managed differently. Default HSIA policy is specified by configuration in the service level. Beneath the HSIA policy, in the service configuration level, two different policy configurations are provided: one for VDSL and one for ADSL. Each device with HSIA service matches either ADSL or VDSL.

Likewise, VoIP service is managed differently for each state and for each city within a state. Beneath the VOIP policy in the service level, policy configurations are added to the service configuration level - one for each state. Beneath each of these, a service configuration sub-level is created for each city within the specific state. Each device with VoIP service matches a single city and state combination.



The policy for each level of the hierarchy can have any of the following components, although none are required:

- A profile that defines the CWMP parameters to be observed or set.
- Workflows that are run in response to defined events.
- A captive portal configuration that defines the conditions under which subscribers have restricted network access.
- A firmware base URL that defines where firmware is stored on the firmware server.

In general, more specific policies override more general policies. Policies set at service configuration level of the hierarchy override policies set in the service or organization levels. In addition, the nodes in the service level are given priority in the policy hierarchy, and the policies of those with higher priority override the policies of nodes with lower priority.

To view the policy for a device, view its details in the CMS Management Console. This effective policy is a combination of the policies for the organization level, each service associated with the device, and all the nodes at the service configuration level that match the device.

Configuring Parameters with Profiles

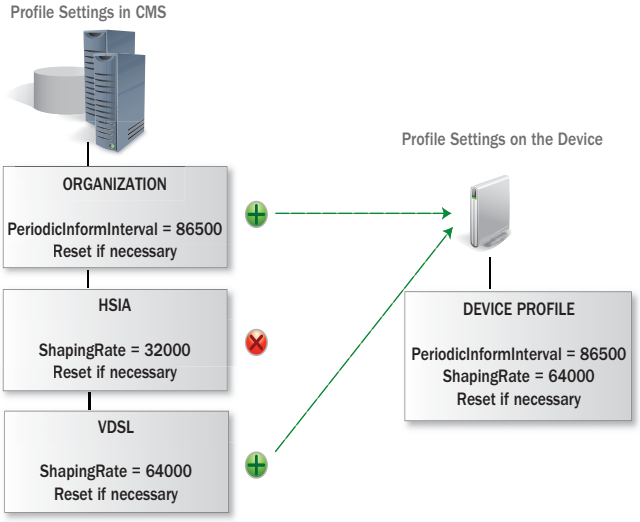
A profile is a list of CWMP device parameters and the rules about how they should be configured on a device. During each device inform, CMS checks to ensure that the parameters in a profile are set or observed according to the rules defined in the profile. Each parameter has a device classifier that defines the types of devices to which the profile applies as well as:

- An observation rule that defines whether CMS should watch this parameter for changes.
- A definition rule that defines whether CMS should set a value for this parameter.
- A value that will be set according to the definition rule.

Profiles can be configured at all levels of the policy hierarchy. Profiles set at the service configuration level override those set at the service level, which override those set at the organization level.

For example, the HSIA service node has a VDSL service configuration node below it in the policy hierarchy.

- The organization node's profile is configured to set InternetGatewayDevice.ManagementServer.PeriodicInformInterval to 86500. If the device's value is not 86500, the profile dictates that CMS should reset the parameter.
- The HSIA node's profile is configured to ensure that the InternetGatewayDevice.QueueManagement.Queue.2.ShapingRate parameter is set to 32000. If the device's value is not 32000, the profile dictates that CMS should reset the parameter.
- The VDSL node's profile is configured to set the ShapingRate parameter to 64000.
- Therefore, CMS will set the PeriodicInformInterval to 86500 and the ShapingRate parameter to 64000 for a device that matches both the HSIA and VDSL nodes.



Responding to Events with Workflows

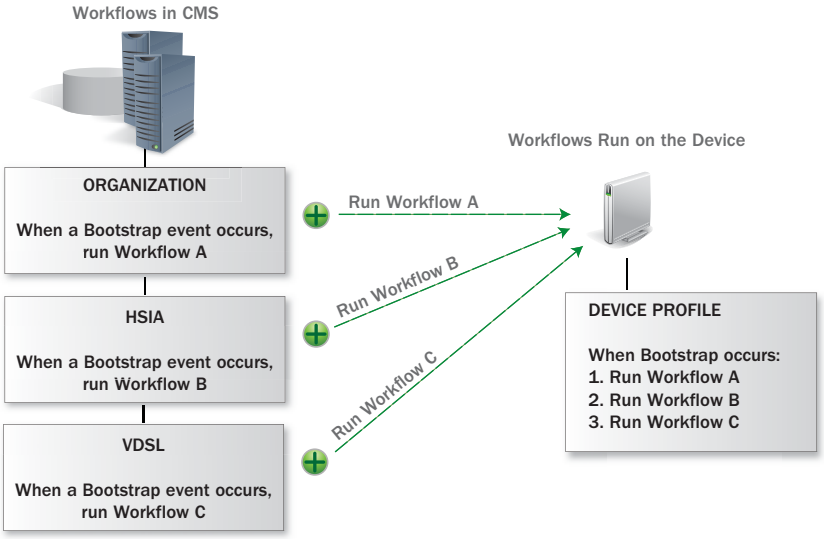
CMS is notified of events, such as CWMP messages, that occur on the devices that it manages. CMS can be configured to respond to these events with workflows, which are sets of CWMP commands.

CMS automatically performs much of the work associated with the default workflows. 2Wire Professional Services can create custom workflows to perform additional tasks. For example, the Periodic Inform event is paired with a custom workflow that monitors the number of remote bridges associated with each iNID. When information about a new remote bridge is retrieved, the workflow adds the information to CMS. While this example describes a task that CMS already performs regularly, it illustrates how workflows can be used to perform tasks in response to particular events.

Event and workflow pairs can be configured at all levels of the policy hierarchy. CMS runs all workflows associated with a device's effective policy, starting with the workflows at the organization level.

For example:

- The organization node's policy dictates that Workflow A should be run in response to a Bootstrap event, when the device is installed and booted for the first time.
- The HSIA node's policy dictates that the Workflow B should be run in response to the Bootstrap event.
- The VDSL node's policy dictates that the Workflow C should be run in response to the Bootstrap event.
- In response to the Bootstrap event, CMS will run the Workflow A, Workflow B, and Workflow C, in that order.



‘

Restricting Subscriber Access with Captive Portal Configuration

The captive portal is a mechanism to restrict subscriber access to the network for a variety of purposes, such as:

- *Entitlement and activation*. Access is restricted until the subscriber registers and accepts the terms of service.
- *Delinquent user*. Access is restricted until the subscriber updates the information associated with the account.
- *Suspended user*. Access is restricted because the subscriber has violated the service provider's use policies.

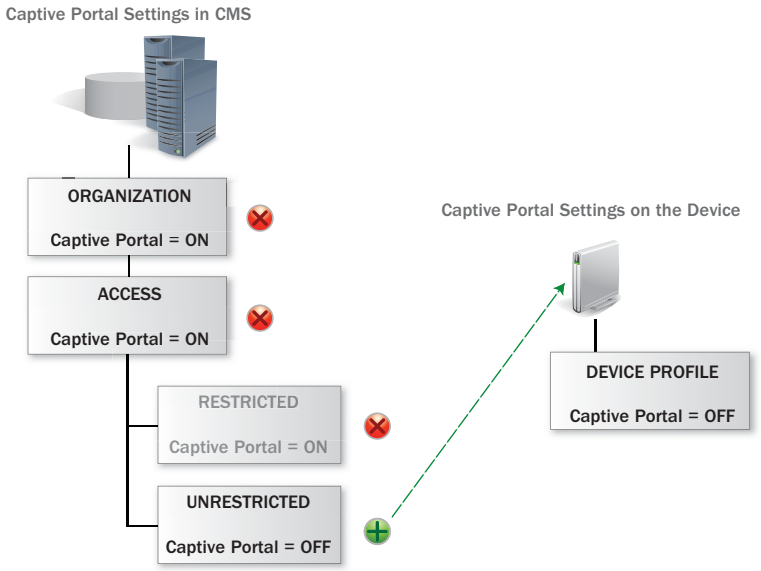
The following captive portal states are available:

- *On*. Enables captive portal. When captive portal is enabled, HTTP traffic is redirected to the URL defined and only IP addresses in the white list are accessible.
- *Off*. Disables captive portal.
- *Inherit*. Defers to captive portal settings at the next higher level in the policy hierarchy.

Captive portal information can be configured at all levels of the policy hierarchy. Configuration defines the URL where HTTP traffic is redirected and the white list of IP addresses that a device can access when the captive portal restricts subscriber access to the network. Captive portal configuration set at the service configuration level overrides settings at the service level, which override settings at the organization level.

For example, adding an Access service-level node to the policy hierarchy keeps captive portal configuration confined to one service that can be prioritized above the other services. This service node has two nodes at the service configuration level: Restricted and Unrestricted.

- Captive portal configuration is enabled at the organization, Access service, and Restricted service configuration nodes.
- Captive portal is turned off for the Unrestricted service configuration node.
- For a device that matches the organization, Access service, and Unrestricted service configuration nodes, captive portal is turned off.

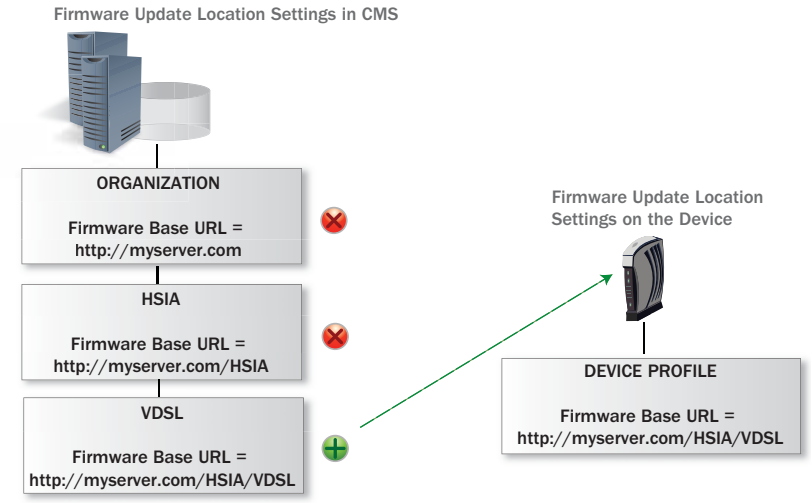


Defining the Location of Firmware Updates

The firmware base URL defines a portion of the location where the firmware specific to the organization or service resides on the firmware server. The base URL can be set at all levels of the policy hierarchy. The URL configured at the service configuration level overrides the URL at the service level, which overrides the URL set at the organization level. A device only pulls firmware updates from the location defined by its effective policy, which includes this base URL plus the location set in the firmware entry.

For example:

- The firmware base URL for the organization node is http://myserver.com.
- The URL for HSIA node is http://myserver.com/HSIA.
- The URL for VDSL node is http://myserver.com/HSIA/VDSL.
- CMS will pull firmware for a device that matches both HSIA and VDSL from http://myserver.com/HSIA/VDSL.



APPENDIX A

Glossary

activation

The act of initiating services on a device. Activation is the last step in provisioning a service and is sometimes used as a synonym for provisioning.

bulk data collection

A CMS feature that enables the collection and storage of a large number of device parameters during periodic informs at defined collection intervals.

Business Support Systems (BSS)

The tools that a telecommunications service provider uses to run its customer-related business operations, such as customer relationship management systems and billing systems.

captive portal

A mechanism to restrict subscriber access to the network. For example, access is restricted until the subscriber registers and accepts the terms of service as well as when the subscriber has violated the service provider's use policies. In the captive portal, the subscriber's browser is redirected to a specific URL and the subscriber is given directions for how to resolve the issue.

CMS Management Console

The web application used by the service provider to interact with devices and manage groups, organizations, services, bulk data collection, and CMS users.

CPE WAN Management Protocol (CWMP)

The industry-standard protocol that facilitates communication between a device and CMS and enables secure auto-configuration and other management functions. CWMP is described in the Broadband Forum's TR-069 specification.

device

The hardware that connects the subscriber's local area network (LAN) to the service provider's wide area network (WAN). A device can be managed by CMS through TR-069. Devices are sometimes referred to as CPE.

device classifier

A means of labeling a device based on functionality that the device supports or a characteristic of the device, such as `TR98.Diagnostics.IPPing` for devices that support ping or `2Wire.device` for 2Wire devices. Device classifiers define the devices that are affected by CMS functionality. For example:

- For profiles, device classifiers define the types of devices on which a parameter should be observed or set.
- For event and workflow pairs, device classifiers define the types of devices on which events should be observed.
- For services, device classifiers define the types of devices to which a service applies.

group

A set of devices defined by listing specific devices or entering a search expression, which enables group membership to change over time. Groups are used to schedule firmware upgrades and for bulk data collection.

intelligent Network Interface Device (iNID)

A residential gateway (RG) that is installed outside the subscriber's home, making it easily accessible to service technicians. An iNID and one or more remote bridges, which are installed in a subscriber's home, provide high-powered wireless and wired internet access. Like other RGs, an iNID can be managed by CMS.

Operations Support Systems (OSS)

The tools that a telecommunications service provider uses to maintain network inventory, provision service, configure network components, and manage faults, fulfillment management, and order provisioning.

organization

An organizational unit that partitions one or more devices so that those devices can be configured and managed as a unit. An organization has associated services and policies. A device can belong to only one organization.

policy

The automation of one or more management activities. Policies include the configuration of profiles, event and workflow pairs, the captive portal, and a firmware base URL. Policies are associated with the nodes at each level of the policy hierarchy.

policy hierarchy

An arrangement of an organization that includes individual policy nodes at a global organization level, a service level, and a service configuration level. Each node in the hierarchy has an associated policy that defines how devices are managed and configured.

profile

A list of CWMP device parameters and the rules about how they should be observed and configured on a device. A profile is part of a policy and can be set at each level of the policy hierarchy.

provisioning

The act of providing and configuring the hardware and firmware required to establish services to subscribers. During the provisioning process, the device becomes part of the service provider's network, which removes the burden of maintenance and management from the subscriber.

remote bridge

A wireless access point installed inside a subscriber's home that works in conjunction with an iNID to provide services to the subscriber. A remote bridge is a dependent device that can be configured in CMS through its associated iNID.

residential gateway (RG)

A broadband modem that connects a subscriber's local area network (LAN) to a service provider's wide area network (WAN). RGs often include integrated services, such as internet connection sharing (wireless or wired), firewall, or digital phone interface. An RG can be managed by CMS.

service

A logical set of functionality made available to a subscriber, such as high speed internet access (HSIA), Voice over Internet Protocol (VoIP), and Internet Protocol Television (IPTV). Services are fulfilled by devices and require configuration.

subscriber

A customer who has a subscription to access one or more services. A subscriber is connected to the service provider through a device.

TR-069

Broadband Forum Technical Report 069: CPE WAN Management Protocol. TR-069 defines the application layer protocol for remote management of devices.

workflow

A set of CWMP commands to be carried out between CMS and a device either in reaction to an event such as a CWMP message or in order to diagnose or resolve an issue. Workflows are part of a policy and they can be set at each level of the policy hierarchy.