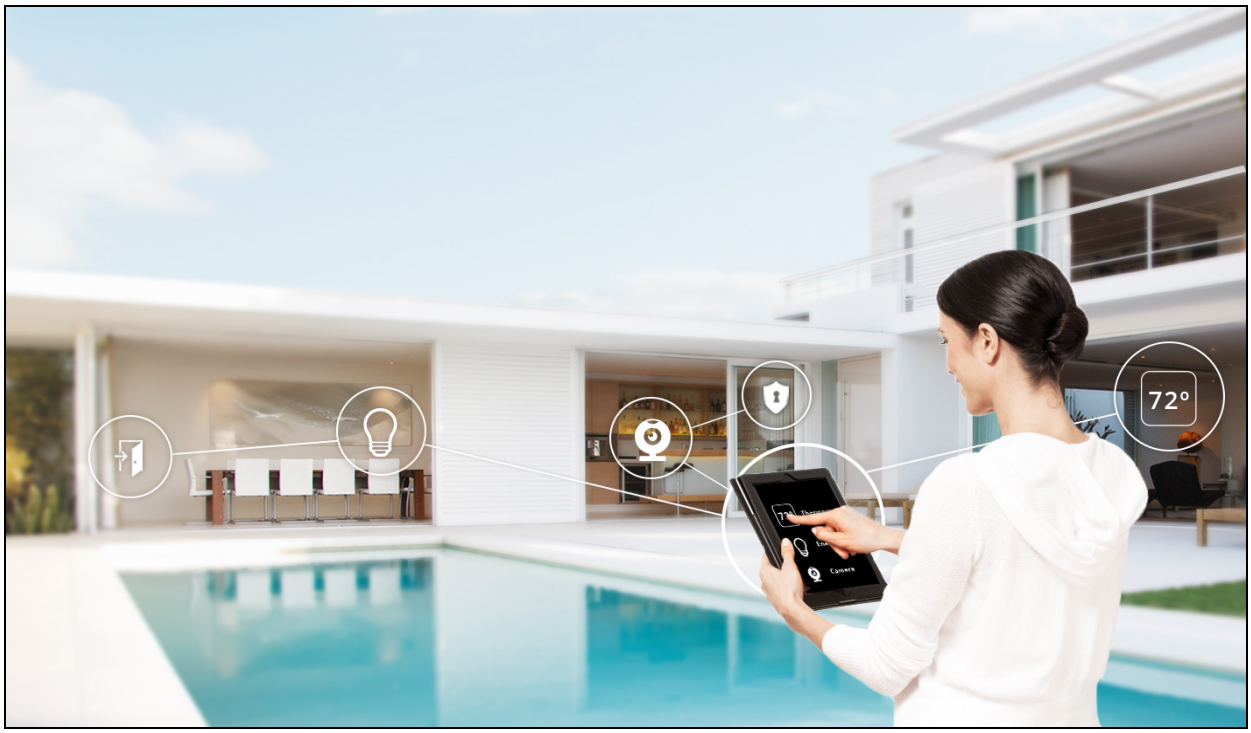
Management Portal Guide

7.3 Quadra



Document Information

Release version: 7.3 Quadra
Document name: Management Portal Guide
Build date: 9/12/2016

Contents

Revision History

Release	Revisions
7.3 Quadra v6	❑ Updated "Command History Report" on page 135 to indicate that events in the report are filtered by date ❑ Clarified that "Wi-Fi clients" do not support the Adjust Wi-Fi Channel feature (see Adjust Wi-Fi Channel on page 170) ❑ Added the note "The file size must be less than 2 MB." for batch importing CPE devices and SIM cards.

7.3 Quadra v5	❑ Added the OAuth Manager advanced role to the roles table under "Advanced Roles" on page 74
	❑ Updated the REST Integration advanced role in the roles table under "Advanced Roles" on page 74
	❑ Added the following tier properties for camera watchdog configuration (see Tier Properties on page 26):
	`cpe.camera.pingIntervalSeconds`
	`cpe.camera.onlineDetectionThreshold`
	`cpe.camera.offlineDetectionThreshold`
	❑ Added the following tier properties for CPE trouble annunciation (see Tier Properties on page 26):
	`cpe.troubles.ackExpireMinutes`
	`cpe.troubles.annunciationIntervalMinutes`
	`cpe.troubles.deferSleepHours`
	`cpe.troubles.minTroubleVolume`
	`cpe.troubles.noAlarmOnCommFailure`
	`cpe.troubles.showTroublesAfterAnnunciation`
	❑ Added the following tier property for the energy management feature (see Tier Properties on page 26):
	`energy.management.url`
	❑ Added new `ZigBee DoS Detection` tier properties for the ZigBee RF Security feature. See cpe.zigbee.defender.<suffix> on page 32
	❑ Clarified an app is updated if it is already installed on a touchscreen when a new or updated app is pushed to current tiers. See Touchscreen App Actions on page 53.

7.3 Quadra v4	❑ Added new `ZigBee Jamming Detection` tier properties for the ZigBee RF Security feature. See "cpe.zigbee.healthCheck.<suffix>" on page 32
	❑ Updated the value range of the following tier properties (see Tier Properties on page 26):
	`connection.broadbandHeartBeatRate`
	`image.upload.dailyLimit`
	`sms.dailyLimit`
	`video.upload.dailyLimit`

Release	Revisions
7.3 Quadra v3	❑ Added new `networkInfo` tier properties for the diagnostics offloading feature. See "cpe.diagnostics.networkInfo.<suffix>" on page 31 ❑ Added a note addressing the case where the touchscreen is tampered while the `device.tamper.enabled` property is modified. See Advanced Properties Report on page 153.
7.3 Quadra v2	❑ Added new `commQueue` tier properties for the diagnostics offloading feature. See "cpe.diagnostics.commQueue.<suffix>" on page 31 ❑ The "Reviewing Reports" section has been updated and renamed Reviewing System Status on page 122. ❑ Many advanced properties have been added to Advanced Properties Report on page 153 .
7.3 Quadra v1	❑ Replaced all instances of "Insight" with "Touchstone" ❑ Added a new tier property, tvr.banner.enabled on page 36, to enable and disable a banner advertising TVR on the touchscreen ❑ Added a new section, Managing Partners on page 42 ❑ Clarified .txt and .csv files are the accepted file formats in Batch-Importing CPE Devices to Inventory on page 60 ❑ Clarified .txt and .csv files are the accepted file formats in Importing SIM Card Data to Inventory (Converge Only) on page 64 ❑ Added a new section, Managing Bundles on page 67 ❑ Added new employee roles: CAT Manager, Bundle Manager and Bundle User, to the roles tables in Management Portal Roles on page 71 ❑ Added requirements for subscriber account usernames and passwords in Modifying Account Information on page 95 ❑ Clarified that the troubleshooting option Adjust Wi-Fi Channel on page 170 is not displayed when the device does not support the feature
7.2 Padre	❑ Updated Dashboard screen on page 12 to include the customer connectivity status report field. ❑ Updated "Account Report" on page 130 to include the Account GUID ❑ Updated "Querying Accounts" on page 91 to describe the customer connectivity status report field. ❑ Added "Refresh customer connectivity status reports" to the admin role in "Management Portal Roles" on page 71.

Release	Revisions
7.1 Oahu	❑ Updated Dashboard screen on page 12 to include the server version number in the footer ❑ Added advanced MP roles, REST Integration and REST MDU to the roles table under "Advanced Roles" on page 74 ❑ Added new TCA tools actions, Reboot Router, Reboot Camera, and Adjust Wi-Fi Channel, to the roles table under "General Roles" on page 71 ❑ Updated the role types allowed to deactivate accounts in the roles table under "General Roles" on page 71 ❑ Added new Troubleshooting sections: ❑ ❑ "Rebooting a Security Router Remotely (Converge only)" on page 157 ❑ "Rebooting a Camera Remotely" on page 158 ❑ "Adjust Wi-Fi Channel" on page 170 ❑ Added a new tier property, "tvr.enabled" on page 36, to enable and disable the Touchscreen Video Recording feature ❑ Added a new section, "Multi-Dwelling Unit Package for Touchstone" on page 26 ❑ Removed "Legal Notices" section. Information is included in the Build Information for each release ❑ Removed "Browser Compatibility" section. For information about supported browsers, see: https://share-icontrol.atlassian.net/wiki/display/CSKB/7.1+Oahu+Core+-+Build+Information+and+System+Requirements
7.0 Nantucket	❑ Corrected privileges in "Management Portal Roles" on page 71 ❑ Rewrote the description "Tier Properties" on page 26 ❑ Added the section "Other Devices Report" on page 149.
6.3 Maui	v2. Added the "Show CS Integration error only check box" description to the Account Search Criteria table on p
6.2 Lanai	❑ Added the section "Device Health Check Request" on page 169. ❑ Updated Roles to add the new advance REST Operator role. See "Management Portal Roles" on page 71. ❑ The Legal Notices section has been updated to add new third-party software. See "Legal Notices" on page 1.

Release	Revisions
6.1 Kodiak	❑ The Peripheral Report now includes information on gateways and routers. See "Peripherals Report" on page 145. ❑ The Cameras Report has added columns related to motion capable cameras. See "Cameras Report" on page 140. ❑ System objects that refer to the Telephony server have been marked "deprecated". ❑ The information in "Importing SIM Card Data to Inventory (Converge Only)" on page 64 has been updated to state "The third value is the CPE ID of the touchscreen associated with the SIM Card."
6.0 Jamaica - 6.1 Kodiak	❑ The section "Managing Device Descriptor Lists" on page 39 has been broadly updated to include information on managing your blacklist files. ❑ In "Understanding Tiers, Tier Properties, and Packages" on page 18, updated the paragraph describing packages to make it more clear that Packages override the Tier Property values of a subscriber's Tier. ❑ Updated "deviceDescriptor.blacklist" on page 32 to make the use of the blacklist URL property more clear. Also added cross-references to the sections that explain Tiers/Packages and DDL/blacklist.
	❑ Added restricted operations list to "Accessing the Subscriber Portal Backdoor" on page 159.
	❑ Added the following note to the "Using the Account Information Details Section" on page 85 in the description of the Touchscreen Passphrase: **Note:** The passphrase changes within 24 hours of being used and every 7 days from the last time the touchscreen was rebooted.
	❑ The table "Account Management Tools Elements" on page 89 does not incorrectly state that suspended accounts can received firmware updates.

5.3 Ibiza SU1	❑ Added door lock reports.
	❑ Expanded device descriptor lists to include `blacklist.xml` files.
	❑ Deleted the following tier properties:
	  ❑ image.maxAllowed
	  ❑ video.maxAllowed

5.2 Ibiza	Deprecated the following tier properties: ❑ image.maxAllowed ❑ video.maxAllowed
5.1 Hawaii SU1	Currently, for touchscreen with Android firmware, you cannot “Add On Activation” any touchscreen apps you inactivated. Contact your Icontrol representative if you need to activate an inactivated app. Apps on QNX TouchScreens have not changed.

1 Introduction

The intended audience for this document includes IT managers and network architects who need to understand the overall Converge and Touchstone architectures within the service provider's server environment and how it can be deployed to communicate properly with subscriber accounts.

This document contains information on:

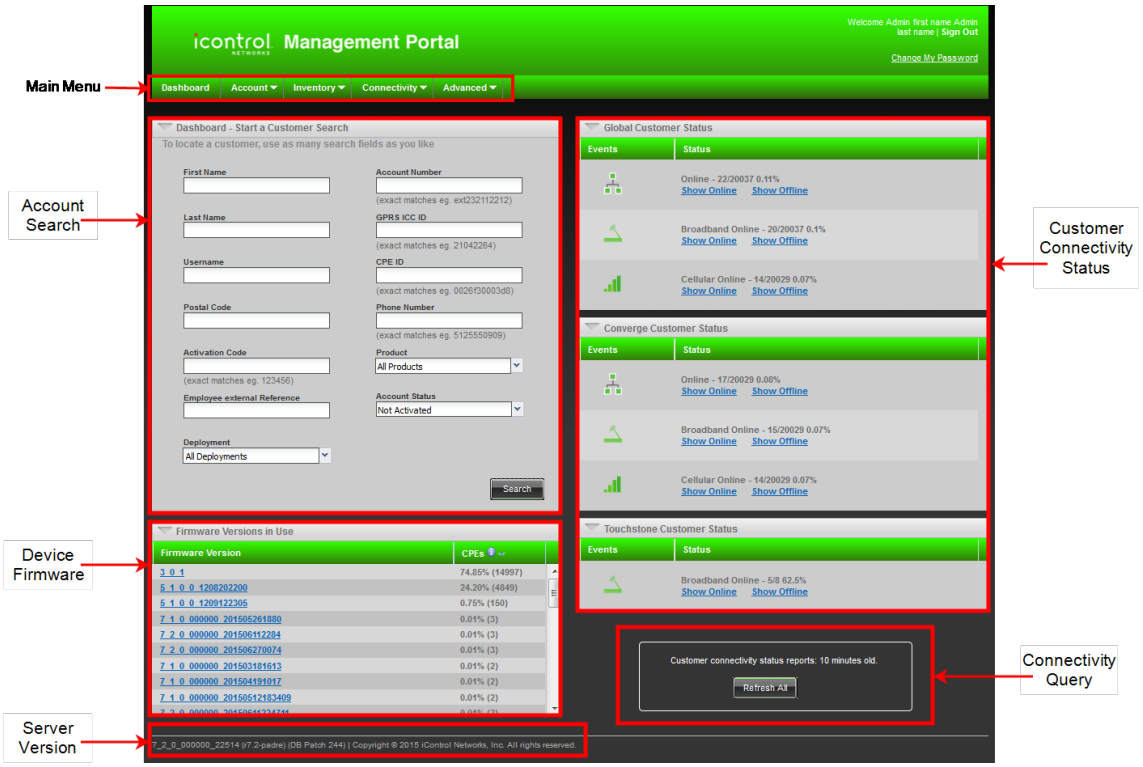
- Setting up the subscriber environment
- Managing employee roles
- Managing customer premise equipment (CPE) inventory
- Creating and managing accounts
- Reports available from the Management Portal

The Management Portal is used by service provider representatives to:

- Support subscribers with account or CPE issues
- Manage environmental properties, such as tiers, packages, device descriptor list, firmware updates, etc.
- Manage CPE inventory
- Run reports

1.1 Understanding the Dashboard

The Dashboard is displayed after logging into the Management Portal. Once logged in, it is also accessed by selecting **Dashboard** from the Menu bar.



- The *Main Menu* can be accessed from any of the Management Portal screens.
- The *Account Search* area provides multiple options to finding an individual customer account. See "Searching for a Customer Account" on page 82 for more information.
- The *Device Firmware* area lists the versions of firmware the Converge touchscreens and Touchstone hubs are running. Click on the headers to sort by firmware version or CPEs. Click on a link to display the list of devices running that firmware version.
- The *Customer Status* area displays the percentage of CPEs that are connected or offline. Global customer reports are the sum of Converge and Touchstone customers. Click on a link to display the list of CPEs in that status.
- An admin user can click on the **Refresh All** button to run the Connectivity Query and refresh the data linked to the Customer Status reports. The age of the current reports is also displayed.
- The server version number is displayed in the footer in every screen.

2 Subscriber Environment

Several properties and settings must be configured prior to adding accounts to the environment. Service providers may choose to keep the default settings Icontrol has provided or modify them. Most topics in this section will be found under the **Advanced** section of the Management Portal's main menu:

- Manage Deployments
- Manage Central Station details (Converge only)
- Manage CPE Firmware
- Manage Tiers & Packages
- Manage Cellular Profiles (Converge only)
- Manage the Device Descriptor List
- Manage Partners
- Manage Touchscreen Apps (Converge only)

2.1 Managing Deployments

Deployments are separate instances of the Icontrol Converge system. Creating deployments is not required to set up the system. From the main menu, select **Advanced > Manage Deployments**. The *Deployment* screen is displayed.

Column	Description
ID	Unique ID number for the deployment; Click to modify the deployment details.
Key	File name of the detail file of the deployment
Display Name	The UI display name of the deployment
Image URL	URL for the banner used by the deployment in the Management Portal and Subscriber Portal

2.1.1 Add a Deployment

From the *Deployment* screen, click **Add**. The *Add New Deployment Information* screen is displayed. Enter the information below and click **Save**.

Column	Description
Key	File name of the detail file of the deployment.
Display Name	The UI display name of the deployment.

Column	Description	
Image URL	URL for the banner used by the deployment in the Management Portal and Subscriber Portal.	
Central Station Settings	Default	Select to use the default Notification email.
	Custom	Select to be able to modify the Notification email.
Notification Email Address	When the central monitoring station sends a notification for any account in the deployment, a notification is sent to this email address as well. Note: Only used for deployments using Email integration with the central monitoring station.	

2.1.2 Modify Deployment Details

From the **Deployments** screen, click the ID of the deployment. The *Edit Deployment* screen is displayed.

- If modifying the Image URL, click **Fetch** to retrieve the new information.
- Clicking **Deactivate**, deactivates all the accounts and inventory associated with the deployment, making them unavailable. The accounts and inventory and deployment details are still maintained in the database.

Once done with editing the details, click **Save** to return to the *Deployment* screen.

2.2 Managing Central Monitoring Station Details (Converge Only)

Central monitoring stations are the centers that receive and qualify alarms at subscriber premises. From the main menu, select **Advanced > Manage Central Station**. The Central Station screen is displayed.

2.2.1 Add a Central Monitoring Station

1. From the *Central Statio*n screen, click **Add**.
2. Enter the details of the central monitoring station

Field	Description
Name	Short name for the central monitoring station.
Phone Number	Contact phone number for the central monitoring station. The phone number must be unique for each central monitoring station.
Receiver ID	Unique ID for the central monitoring station.
Description	Descriptive information to distinguish the central monitoring station from the other stations listed.
Deployment	Deployment that uses the central monitoring station. **Note:** Only displayed for systems that use deployments.

3. Click **Save** to add the central monitoring station and to return to the Central Station screen.

2.2.2 Modify Central Monitoring Station Details

1. From the *Central Station* screen, click the ID of a central monitoring station.

   The *Edit Central Station Receiver* screen is displayed.

2. Modify the desired field(s) and click **Save** to save the changes and return to the Central Station screen.

2.3 Managing Firmware Versions

CPE firmware can be hosted at one or multiple locations. The firmware versions that available for use and the URL for the locations of where to download the firmware are managed via the Management Portal.

View Imported Firmware Versions

From the main menu, select **Advanced > Manage Firmware Version**. The *Firmware Versions* screen is displayed.

Column	Description
Number	Version number of the firmware
Name	Short descriptive name of the firmware version.
URL	Path to web server where the firmware version is hosted (usually the Bundle server).
Product	Converge or Touchstone. The platform of the CPE for which the firmware was designed.
Model	The type of CPE for which the firmware was developed.
Manufacturer	The hardware model of the CPE for which the firmware was developed.
Deployment	The Operator Domain deployment to which the CPE device is assigned; **Note:** This column is only displayed for service providers using deployments.
Active	Whether the firmware is available for download to the CPE.

Click on any of the column headers to sort by that column.

2.3.1 Add a Firmware Version

1. From the *Firmware Versions screen*, click **Add**.

   The Add New Firmware Version Information screen is displayed.

2. In the **Download URL** field, enter the URL to the new version.

3. Click **Get Details**.

   The fields in the screen are updated with the details of the new version.

4. In the **Version Name** field, change the name of the firmware version if desired.

5. Select **Reboot Required**.

6. In the **Deployment** field, select the deployments this firmware version will be available to. To select more than one, hold down the "Ctrl" key.

   Note: This field is only displayed for service providers using deployments

7. Select **Active** to make the firmware available to download from the touchscreen.
8. Enter information in the **Description** field, if desired.
9. Click **Save**.

   The new version is imported to the Management Portal and the Firmware Versions screen is displayed.

Field	Description
Version Name	Short descriptive name of the firmware version.
Firmware Version Number	Version number of the firmware update. **Note:** The value of this field is collected from the selected firmware version. It is not editable.
Download URL	Path to web server (Bundle server) where the firmware version is hosted.
Product Name	Converge or Touchstone **Note:** The value of this field is collected from the selected firmware version. It is not editable.
Hardware Model	Model of the touchscreen or hub **Note:** The value of this field is collected from the selected firmware version. It is not editable.
Hardware Manufacturer	Revision code for the hardware of the CPE. **Note:** The value of this field is collected from the selected firmware version. It is not editable.
Build Date	Date the firmware version was built. **Note:** The value of this field is collected from the selected firmware version. It is not editable.
Build Time	Time of day (based on server time) that the firmware version was built.
Reboot Required check box	Selected if the CPE should be automatically rebooted after the firmware is updated.
Deployment	The deployment to which the firmware is assigned; **Note:** This menu is only displayed for service providers using deployments.
Active check box	For Converge only. Selected if the firmware version is accessible by touchscreens when the Update Firmware button is tapped on the touchscreen.
Description	Additional information regarding the firmware version.
Information	Displays the Rule version and Action version of the current firmware version.

2.3.2 Modify the Details of a Firmware Version

1. From the *Firmware Versions* screen, click the firmware version number.

   The Edit Firmware Version screen is displayed. The following details of a firmware version can be modified:

   - **Version name** - Short descriptive name of the firmware version
   - **Download URL** - The location URL of the firmware version on the web server (Bundle server)
   - **Build Date/Time** - The date/time that the firmware version was created;
     Change this to the current date/time to have devices choose the current version rather than the version that previously had the most recent date.
   - **Reboot Required** - DO NOT UNSELECT
   - **Active** - Selected if the firmware version is accessible by touchscreens when the Update Firmware button is tapped.
   - **Description** - Additional information regarding the firmware version

2. Modify the desired fields.

   Note: If the **Download URL** is being modified, click on **Get Details** before modifying other fields.

3. Click **Save** and return to the *Firmware Versions* screen.

2.3.3 Delete a Firmware Version

1. From the *Firmware Versions* screen, click the firmware version number.

   The Edit Firmware Version screen is displayed.

2. Click **Delete**.

The firmware version information is deleted from the Management Portal, but not the Bundle server.

2.4 Understanding Tiers, Tier Properties, and Packages

Tiers provide service providers the ability to offer different levels of service to their subscribers. A Tier is made up of a set of Tier Properties. Tier Properties represent configurable settings to features available to the subscribers. There are two types of Tier Properties:

- Server: defines functionality performed by the system servers.
- Client: defines functionality performed by the CPE (touchscreen/hub).

Advanced Tier Properties are read-only and cannot be modified using the Management Portal. They can only be modified by running a database script or by direct database access.

By default, the Converge Tiers are: Converge-Base, Gold, Silver, Bronze, and Test, and the default Touchstone Tiers are: Insight-base and Insight-test. Service providers can modify the Tier Properties and values in the default Tiers, but cannot delete them. Service providers can add Tiers and only the additional Tiers can be deleted.

Each Tier can have different Tier Properties and different values for the Tier Properties. If the value of a Tier Property is changed in a Tier, the value for that Tier Property in other Tiers is not affected. For example, the `sms.dailyLimit` property defines the maximum number of SMS messages allowed to be sent to a subscriber account. The property can be set to 10 in the Gold tier, 5 in the Silver tier and 0 in the Bronze tier. This setting will apply to all accounts in the respective tiers.

Each account is required to be assigned to a Tier when the account is created. The account can be moved to another Tier at any time after it is created and the changes take effect immediately, but it can only be assigned to one Tier.

Packages are similar to Tiers in that they are also made up of a set of Tier Properties however, Packages are not designed to be used independently; they are meant to work in conjunction with Tiers. Tier Property values in a Package override the values of the Tier Properties in a Tier. Service providers can use Packages to change Tier Properties for a subset of accounts in one or more Tiers without having to create a new Tier or reassigning accounts to a different Tier. Unlike Tiers, one or more packages can be assigned to an account.

For example, the `sms.dailyLimit` property can be added to a Package and set to 20. The service provider can offer this increase to all of its subscribers, regardless of Tier, and only those subscribers that sign up for the offer are assigned the Package. The subscriber accounts remain in their respective Tiers and all other Tier Properties remain unaffected.

Packages and Tiers have priorities assigned to them (e.g. 1, 5, 6). If two Packages are assigned the same Tier Property, the Tier Property value of the Package with the greater priority number overrides the other. The priority for Tiers is always 1 and Package priorities are never less than 5; so, Packages always override the Tier.

CAUTION: If two different packages with the same priority and different values for the same Tier Property are assigned to the same account, this will lead to unpredictable results.

Converge Only

In addition to different Tier Property values per Tier, the default rules created by the server when a touchscreen is first activated also vary slightly by Tier. This can not be modified by a Tier Property or Package and do not count towards the account quota for SMS and email messages.

Default rules for accounts on Gold or Silver Tiers:

- Send an email and SMS message if the system is in alarm
- Send an email when the system is armed
- Send an email when the system is disarmed

Default rule for accounts on the Bronze tier:

- Send an email and SMS message if the system is in alarm

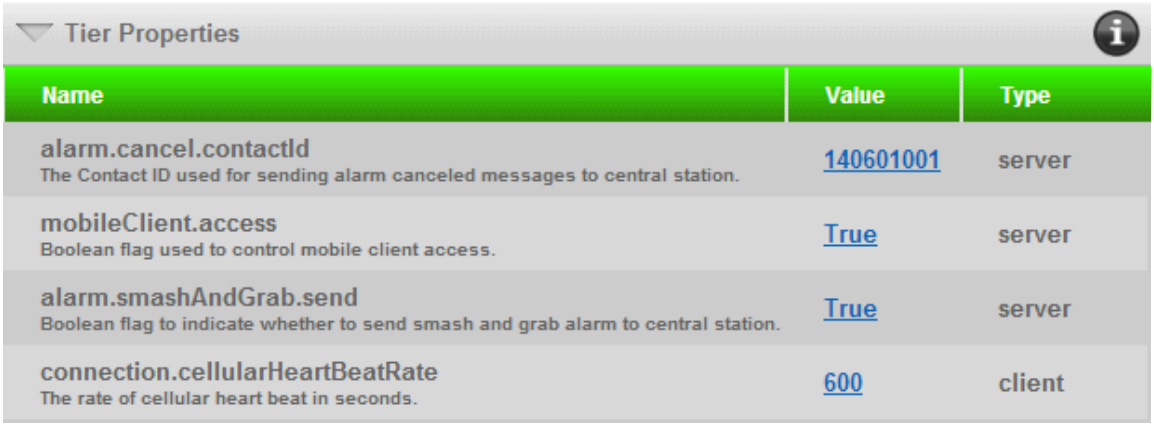
2.4.1 Managing Tiers

To view the Tiers, select **Advanced > Manage Tiers** from the main menu to display the *Manage Tiers* screen. Click **Converge** to view Converge Tiers and click **Touchstone** to view Touchstone Tiers. Click on the **Name** header to sort the tiers by name.

Column	Description
Server Information Section	
Server Version Information	The current Icontrol server installation version
Manage Tiers Section	
Name	Name of the Tier
Description	Short description of the Tier
Priority	The Priority of Tiers is always 1.

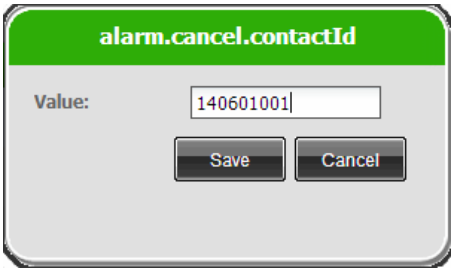
Edit a Tier

1. On the *Manage Tiers* screen, click on the name of a Tier to display the *Edit Tier* screen.
2. Click on the **Name** or **Type** column headers to sort by that column.
3. Click the Information button to toggle the description of the Tier Property.



4. Click the value of a Tier Property to modify its value.

   A dialog is displayed to modify the Tier Property value.

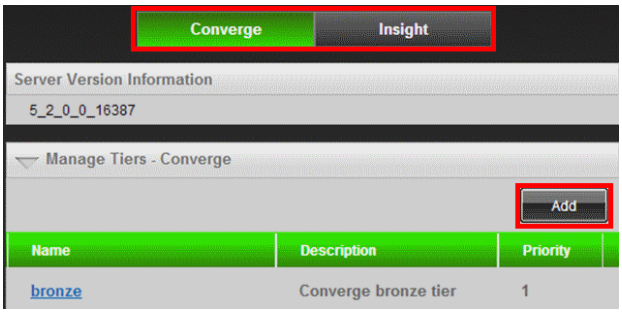


5. Modify the property value and click **Save** to return to the *Edit Tier* screen.

6. Click on another Tier Property to edit or click **Save** in the *Edit Tier* screen to save all edits made to the current Tier. The value to the modified Tier Property is not changed in other Tiers.

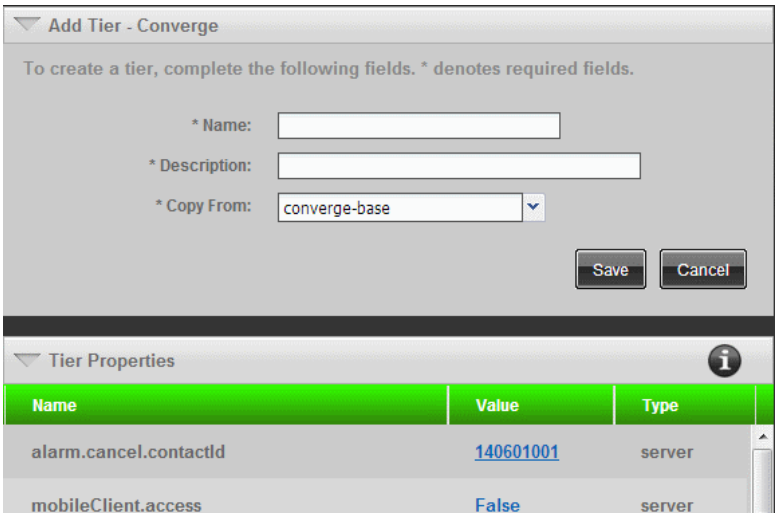
Add a new Tier:

1. On the *Manage Tiers* screen, click **Converge** to add a Tier for Converge accounts or click **Touchstone** to add a Tier for Touchstone accounts.



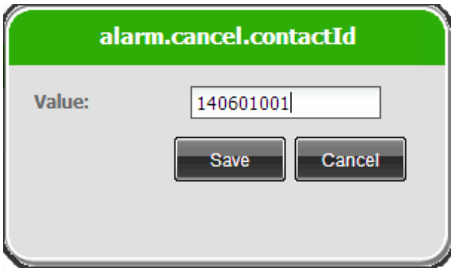
2. Click **Add**.

   The Add Tier screen is displayed.



3. In the **Name** field, enter a descriptive name (no spaces) for this new Tier.
4. In the **Description** field, enter a short, clear description for this new Tier.
5. In the **Copy From** field, select one of the current Tiers whose Tier Property values will be used as a base for this new Tier.
6. Click on the Tier Property values to modify them.

   A dialog is displayed to modify the Tier Property value.



7. Modify the property value and click **Save** to return to the *Add Tier* screen.

   Note: Tier Properties can not be deleted.
8. Repeat these steps the modify the rest of the Tier Property values as needed and click **Save** in the *Add Tier* screen to create the Tier and return to the *Manage Tiers* screen.
9. Click **Cancel** to return to the Manage Tiers screen without creating the new Tier.

Delete a Tier:

A Converge Tier can not be deleted if there are touchscreen apps associated with it. See "Managing Apps (Converge Only)" on page 48 for information about associating Tiers with touchscreen apps. You also cannot delete a Tier if there is an account assigned to it.

1. On the *Manage Tiers* screen, click **Converge** to delete a Tier for Converge accounts or click **Touchstone** to delete a Tier for Touchstone accounts.

2. Click the **Name** of a non-default Tier to delete.

   The Edit Tier screen is displayed.

   Note: If the selected Tier is a default Tier, the **Delete** button is grayed out.

3. Click **Delete** to delete the selected Tier.

   The Tier is deleted and the Manage Tiers screen is displayed.

2.4.2 Managing Packages

To view the Packages, select **Advanced > Manage Packages** from the main menu to display the *Manage Package* screen. Click **Converge** to view Converge Packages and click **Touchstone** to view Touchstone Packages. Click on the **Name** header to sort the packages by name.

Column	Description
Server Information Section	
Server Version Information	The current Icontrol server installation version.
Package Properties	
Name	Name of the Package.
Description	Short description of the Package.
Priority	The priority of the Package in regards to other Packages. **Note:** If two Packages use the same Tier Property with different values and are assigned to the same account, the Tier Property value of the Package with the greater priority value overrides the value that of the other lesser Package. If the priorities are the same, the results are unpredictable.

Edit a Package

1. Click **Converge** to view Converge Packages or click **Touchstone** to view Touchstone Packages.
2. Click the name of a package to modify.

   The Edit Package screen is displayed and is divided into two sections:

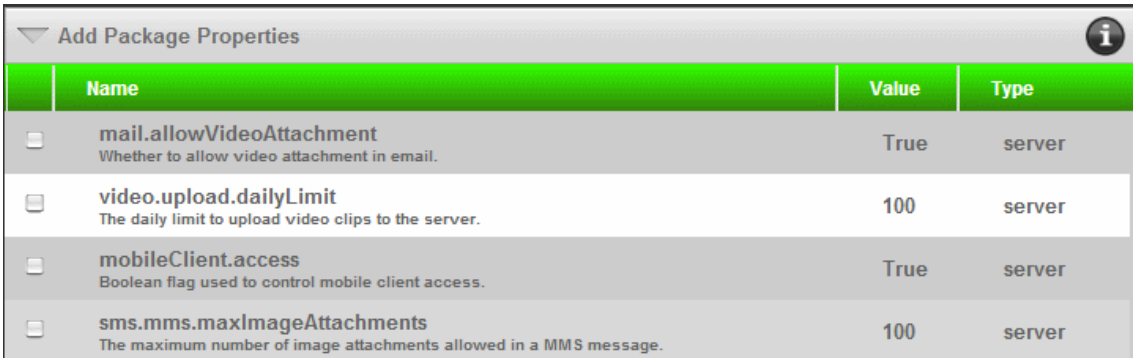
   - Properties
   - Add Package Properties

   Tier Properties that are listed in the Properties section are available to be added to the current Package.

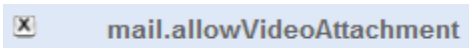
   Select and unselect Tier Properties in the Add Package Properties section to add them to and remove them from the Properties section.

3. Click on the **Name** or **Type** column headers to sort by that column.

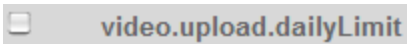
4. Click the Information button to toggle the description of the Package Property.



5. Select a Package Property in the Add Package Properties section to add it to the current Package.



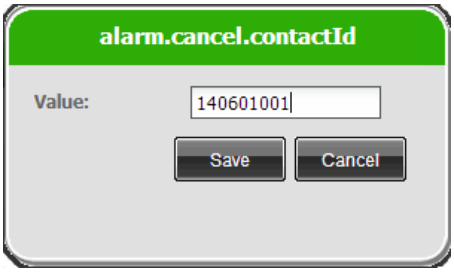
Unselect a Package Property to remove it from the current Package.



The selected Tier Properties are displayed in the Properties section. The unselected Tier Properties are removed from the Properties section.

6. Click the value of a Package Property in the Properties section to modify its value.

A dialog is displayed to modify the Package Property value.

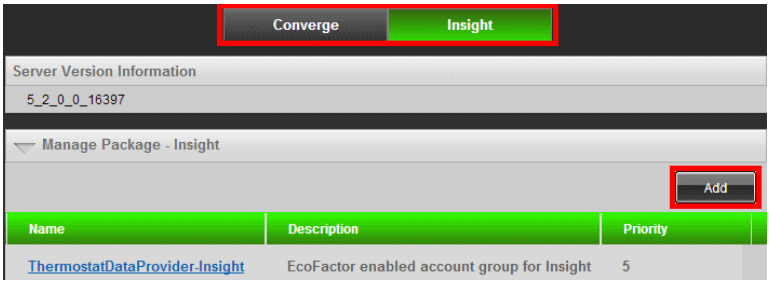


7. Modify the property value and click **Save** to return to the *Edit Package* screen.

The Tier Property has been modified for the current Package. The value to the Tier Property is not changed for other Tiers or Packages.

Add a new Package

1. On the *Manage Package* screen, click **Converge** to add a Package for Converge accounts or click **Touchstone** to add a Package for Touchstone accounts.



2. Click **Add**.

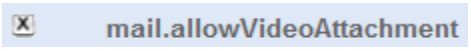
   The Add Package screen is displayed.

3. In the **Name** field, enter a descriptive name (no spaces) for this new Package.

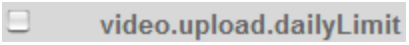
   In the **Description** field, enter a short description for this new Package.

   In the **Priority** field, select a priority for this Package. Packages with greater priority numbers will override Packages with smaller priority numbers if they use the same Tier Properties. Packages always override Tiers.

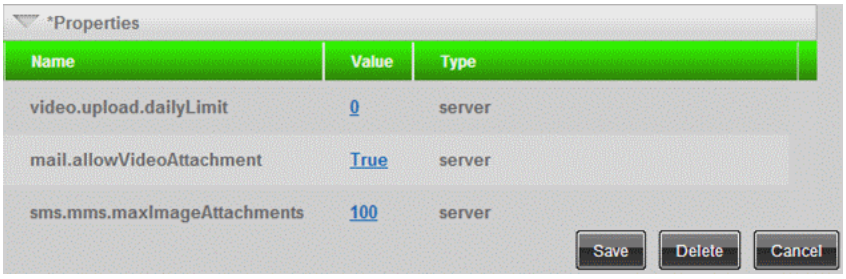
4. Select a Tier Property in the Add Package Properties section to add it to the current Package.



   Unselect a Tier Property to change your mind and remove it from the current Package.

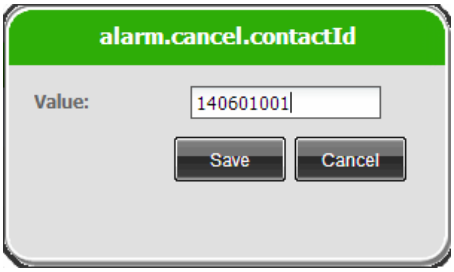


   The selected Tier Properties are displayed in the Properties section. The unselected Tier Properties are removed from the Properties section.



5. Click the value of a Tier Property in the Properties section to modify its value.

A dialog is displayed to modify the Tier Property value.



6. Modify the property value and click **Save** to return to the *Add Package* screen.

   Repeat these steps the modify the rest of the Tier Property values as needed and click **Save** in the *Add Package* screen to create the Package and return to the *Manage Packages* screen. Or click **Cancel** to return to the *Manage Package* screen without creating the new Package.

   After you have saved the Package, click **Cancel** to return to the Manage Packages screen.

Delete a Package

A Package can not be deleted if it has been assigned to an account. See "Using the Account Information Details Section" on page 85 for managing Packages assigned to an account.

1. Click **Converge** to view Converge Packages or click **Touchstone** to view Touchstone Packages.
2. Click the name of a Package to delete.

   The Edit Package screen is displayed.

3. Click **Delete** to delete the Package.

   The Package is deleted and the Manage Packages screen is displayed.

Multi-Dwelling Unit Package for Touchstone

The `MDUPartner-Touchstone` package is only available in environments that have the `mdu.enabled` server property set to `True`. Tier properties can be added and removed as described in "Managing Packages" on page 22 and it can be added to a Touchstone account as described in "Using the Account Information Details Section" on page 85.

Refer to the *System Operations Guide* for more information on the `mdu.enabled` property.

2.4.3 Tier Properties

activation.techapp.enabled

When set to true, the Technician App page appears during activation flow (after activating with the server).

Value Type	Value Range	Platform	Default Value	Tier Type
boolean	True/False	Converge	False	server
		Touchstone	False	

alarm.alarm.smashAndGrab.contactId

The contact ID sent to the central monitoring station when the system detects a possible Smash & Grab scenario. See "Managing Smash & Grab Properties (Converge Only)" on page 37

Value Type	Value Range	Platform	Default Value	Tier Type
string	N/A	Converge	113901001	server

alarm.backupServer.boundaryCase.contactId

The contact ID sent by the Back-up Alarm server if a touchscreen lose contact with the Application cluster after transmitting an alarm but prior to the end of the Alarm Transmission Delay (Abort Window).

Note: This Tier property is viewable in the Advanced Tier Properties table in the Edit Tier screen. This Tier Property is only configurable by database scripts or by direct database access.

Value Type	Value Range	Platform	Default Value	Tier Type
string	N/A	Converge	113001001	server

alarm.cancel.contactId

The contact ID sent to the central monitoring station when the customer enters a valid keypad code but the alarm has already been forwarded to the central station.

Value Type	Value Range	Platform	Default Value	Tier Type
string	N/A	Converge	140601001	server

alarm.smashAndGrab.send

Whether the system monitors for Smash and Grab scenarios. See "Managing Smash & Grab Properties (Converge Only)" on page 37.

Value Type	Value Range	Platform	Default Value	Tier Type
boolean	True/False	Converge	true	server

alarm.smashAndGrab.waitTime

Used when the server receives an alarm event but loses contact with the touchscreen before the alarm is forwarded to the central monitoring station (Transmission Delay). This value is the time (in seconds) to wait before server considers the alarm session to be Smash & Grab. The default is 120 seconds. This value should not be decreased. This helps prevent false Smash & Grab alarms. See "Managing Smash & Grab Properties (Converge Only)" on page 37.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	Zero or any positive integer	Converge	120	server

alarm.skipPolicePanicImmediateAudibleAlarm

If, when the subscriber chooses to send a Police panic alarm, the system issues an immediate audible alarm (when set to false) or the system gives the subscriber the opportunity to send a silent alarm (when set to true).

Value Type	Value Range	Platform	Default Value	Tier Type
boolean	True/False	Converge	true	client

cpe.camera.pingIntervalSeconds

How often (in seconds) the CPE pings a camera to determine whether the camera is online. The default camera ping interval is 15 seconds.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	10 – 300	Converge Touchstone	15	client

cpe.camera.onlineDetectionThreshold

Number of times the CPE must ping a camera successfully to consider the camera online

Value Type	Value Range	Platform	Default Value	Tier Type
integer	1 – 10	Converge Touchstone	1	client

cpe.camera.offlineDetectionThreshold

Number of times the CPE must ping a camera unsuccessfully to consider the camera offline. A trouble is issued when the camera goes offline.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	1 – 10	Converge Touchstone	3	client

cpe.troubles.ackExpireMinutes

Minutes for trouble to be cleared before it reappears on the CPE

Value Type	Value Range	Platform	Default Value	Tier Type
integer	1 - 1440	Converge	720	client

cpe.troubles.annunciationIntervalMinutes

How often (in minutes) the touchscreen emits an audible beep when a system/security/life safety device reports a trouble.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	1 - 1440	Converge	60	client

cpe.troubles.deferSleepHours

If enabled, the touchscreen trouble sounds are muted by default between the hours of 10 PM and 8 AM. Only the audible alert is muted; the trouble is reported to the service provider and on all the user interfaces. The trouble audible alert will be emitted 1 minute after the muting period has ended.

Value Type	Value Range	Platform	Default Value	Tier Type
boolean	True/False	Converge	True	client

cpe.troubles.minTroubleVolume

The minimum touchscreen volume level for trouble audible alerts. By default, the volume for trouble audible alerts is the same as the touchscreen volume. If the property is set to any other level, the trouble audible alert volume does not change if chime, app, or any other volume is changed.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	-1 - 7	Converge	-1	client

cpe.troubles.noAlarmOnCommFailure

Enable whether a sensor communication failure generates an alarm.

Value Type	Value Range	Platform	Default Value	Tier Type
boolean	True/False	Converge	False	client

cpe.troubles.showTroublesAfterAnnunciation

Return to home screen to display trouble header within 30 seconds of trouble annunciation.

Value Type	Value Range	Platform	Default Value	Tier Type
boolean	True/False	Converge	False	client

cellular.levelOfService

The level of service for cellular connection:

- **basic** - The touchscreen sends only core events to the server by cellular when broadband is down. Core events include alarm, trouble, entry delay, heartbeat, and arm/disarm events.
- **basicPlus** - An intermediate level. See *Converge System Architecture Guide* for a list of all possible events.
- **enhanced** - All UDP-related events are sent by the touchscreen when the device is connected to the servers over cellular. See *Converge System Architecture Guide* for a complete list of events that can be sent over UDP.

Value Type	Value Range	Platform	Default Value	Tier Type
enum	❑ basic ❑ basicPlus ❑ enhanced	Converge	enhanced	client

cellular.twoWayVoice.enabled

Whether the Two-Way voice feature is enabled that allows the central monitoring station to contact the customer through the touchscreen.

Value Type	Value Range	Platform	Default Value	Tier Type
boolean	True/False	Converge	true	client

cellular.twoWayVoice.maxCallLength

Maximum amount of time in seconds that a Two-Way voice connection between the central monitoring station and a touchscreen;

Value Type	Value Range	Platform	Default Value	Tier Type
integer	-1 thru 600 Use -1 for “no limit”.	Converge	120	client

connection.bbdownCellularRetryRate

Time (in seconds) that the servers wait to attempt to connect to a touchscreen over cellular if there is no broadband or cellular connection

Value Type	Value Range	Platform	Default Value	Tier Type
integer	0 thru 86400	Converge	1200	server

connection.broadbandHeartBeatRate

Time (in seconds) that the Touchscreen sends out heart beat message over broadband.

Note: This Tier Property is viewable in the Advanced Tier Properties table in the Edit Tier screen. This Tier Property is only configurable by database scripts or by direct database access.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	30 thru 7200	Converge	600	client

connection.broadbandQuickHeartBeatRate

Time (in seconds) that the Touchscreen sends out heart beat message over broadband when a Subscriber is accessing the device remotely, such as using the Subscriber Portal or a mobile device.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	0 thru 86400	Converge	180	client

connection.cellularHeartBeatRate

Time (in seconds) that the touchscreen sends out heart beat message over cellular.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	0 thru 86400	Converge	86400	client

connection.cellularRetryInterval

Time (in seconds) that the touchscreen resends cellular heart beat if the previous heart beat message is not successful.

Make sure that the retry intervals are not multiples of one another so that the server is not flooded with synchronized communications from all CPEs at the same time. Instead, choose values that are not multiples such as the examples below:

Sample recommended values

Tier A: cellular communication retry interval = 281 seconds.

Tier B: cellular communication retry interval = 605 seconds.

Tier C: cellular communication retry interval = 899 seconds.

NOT RECOMMENDED

Tier A: cellular communication retry interval = 300 seconds.

Tier B: cellular communication retry interval = 600 seconds.

Tier C: cellular communication retry interval = 900 seconds.

In the case where the intervals are multiples of each other (such as 300/600/900), at 900 seconds after a network communication disruption, all three tiers would simultaneously submit communications to the server. This could result in behavior that could potentially overload the server.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	0 thru 86400	Converge	1800	client

connection.numOfRetries

Number of times a touchscreen resends the cellular heartbeat message before reporting the cellular channel is disconnected at the touchscreen.

Note: This is constraint not necessary for broadband because it has a TCP connection. If the server does not receive regular heartbeat messages, the TCP connection will be broken and the servers will know that the touchscreen has lost broadband connectivity

Value Type	Value Range	Platform	Default Value	Tier Type
integer	0 thru 10	Converge	4	client

cpe.allowResetToFactory

Indicates whether to allow the CPE to be reset to factory default.

Value Type	Value Range	Platform	Default Value	Tier Type
boolean	True/False	Converge	true	client
		Touchstone	true	

cpe.diagnostics.commQueue.<suffix>

The following tier properties are used to configure collection of `commQueue` diagnostics information for the diagnostics offloading feature. For more information, see: https://share-icontrol.atlassian.net/wiki/display/CSKB/7.3+Quadra+-+Diagnostics+Offloading

- cpe.diagnostics.commQueue.avgResponseThresholdMs
- cpe.diagnostics.commQueue.enabled
- cpe.diagnostics.commQueue.eventQueueDelta

cpe.diagnostics.networkInfo.<suffix>

The following tier properties are used to configure collection of `networkInfo` diagnostics information for the diagnostics offloading feature. For more information, see: https://share-icontrol.atlassian.net/wiki/display/CSKB/7.3+Quadra+-+Diagnostics+Offloading

- cpe.diagnostics.networkInfo.dataCollectionIntervalMinutes
- cpe.diagnostics.networkInfo.enabled

cpe.zigbee.defender.<suffix>

The following tier properties are used to configure the ZigBee Denial of Service detection feature. For more information, see: https://share-icontrol.atlassian.net/wiki/display/CSKB/7.3+Quadra+-+ZigBee+RF+Security

- cpe.zigbee.defender.panIdChangeThreshold
- cpe.zigbee.defender.panIdChangeWindowMillis
- cpe.zigbee.defender.panIdChangeRestoreMillis

cpe.zigbee.healthCheck.<suffix>

The following tier properties are used to configure the ZigBee RF jamming detection feature. For more information, see: https://share-icontrol.atlassian.net/wiki/display/CSKB/7.3+Quadra+-+ZigBee+RF+Security

- cpe.zigbee.healthCheck.intervalMillis
- cpe.zigbee.healthCheck.ccaFailureThreshold
- cpe.zigbee.healthCheck.restoreThreshold
- cpe.zigbee.healthCheck.delayBetweenThresholdRetriesMillis
- cpe.zigbee.healthCheck.ccaThreshold

deviceDescriptor.blacklist

A URL to a blacklist file that lists devices that cannot be used in a Converge or Touchstone environment. This value identifies—Tier-by-Tier, Package-by-Package—which devices listed in the Device Descriptor LIst are not available to subscribers.

Value Type	Value Range	Platform	Default Value	Tier Type
string	Valid URL	Converge	N/A	client
		Touchstone	N/A	

See "Understanding Tiers, Tier Properties, and Packages" on page 18 for a detailed explanation of Tiers and Packages.

See "Managing Device Descriptor Lists" on page 39 for a detailed explanation of the Device Descriptor Lists and the blacklist files and how to manage them.

energy.management.url

Specifies the base host and path of the energy management service that the subscriber user interface uses for the energy management feature. When the `energy-management` package (Converge) or the `energy-management-insight` package (Touchstone) is added to the account, this property also enables presence events on the server used to indicate whether someone (e.g., the homeowner) is present in the home.

Value Type	Value Range	Platform	Default Value	Tier Type
string	Valid URL	Converge	http://toBeReplaced	server
		Touchstone	http://toBeReplaced	

image.upload.dailyLimit

Limit per calendar day for a customer account to upload captured images to the server

Value Type	Value Range	Platform	Default Value	Tier Type
integer	0 thru 5000	Converge	12	server
		Touchstone	12	

mail.allowVideoAttachment

Whether to allow video to be attached to a notification email sent to the customer

Value Type	Value Range	Platform	Default Value	Tier Type
boolean	True/False	Converge	false	server
		Touchstone	false	

mail.maxImageAttachments

Maximum number of images that can be attached to a notification email sent to the customer.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	0 thru 5	Converge	1	server
		Touchstone	1	

mobileClient.access

Whether the customer can monitor and manage their system using a mobile client (iPhone, etc.).

Value Type	Value Range	Platform	Default Value	Tier Type
boolean	True/False	Converge	false	server
		Touchstone	false	

sms.dailyLimit

Maximum number of SMS notifications that can be sent to a customer in a calendar day. If this value is set to 0, then subscribers cannot build rules to send SMS messages. If a subscriber reaches the limit, the system sends one notification per day.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	0 thru 1000	Converge	2	server
		Touchstone	2	

sms.mms.allowVideoAttachment

Whether to allow video to be attached to a notification MMS (Multimedia Messaging Service) message sent to the customer.

Value Type	Value Range	Platform	Default Value	Tier Type
boolean	True/False	Converge	false	server
		Touchstone	false	

sms.mms.maxImageAttachments

Maximum number of images that can be attached to a notification MMS message sent to the customer.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	0 thru 5	Converge	0	server
		Touchstone	0	

subportal.connection.showState

Whether and how to show connectivity on CPE.

- none = No Trouble messages are displayed on the Subscriber Portal or History ever for loss broadband or cellular connectivity,
- total = “Connectivity” Trouble messages are displayed in the Subscriber Portal and logged ONLY when there is no broadband AND no cellular connectivity.
- channel = “Connectivity” Trouble messages are displayed in the Subscriber Portal and logged when there is either no broadband OR no cellular connectivity.

Note: This Tier Property is viewable in the Advanced Tier Properties table in the Edit Tier screen. This Tier Property is only configurable by database scripts or by direct database access.

Value Type	Value Range	Platform	Default Value	Tier Type
enum	none, total, or channel	Converge	total	server
		Touchstone	total	

touchscreen.camera.maxAllowed

Maximum number of cameras a customer is allowed to install.

Note: The maximum number of cameras that can be supported is 6.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	0 thru 100	Converge	1	client
		Touchstone	1	

touchscreen.connection.serverResponseTimeout

Time (in seconds) to wait for an acknowledgement after the CPE sends a message to the servers (e.g. event, alarm, etc.). When this period expires, the CPE resends the message.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	0 thru 120	Converge	30	client
		Touchstone	30	

touchscreen.connection.showState

Whether and how to show connectivity on CPE.

- total = “Connectivity” Trouble messages are displayed in the CPE and logged ONLY when there is no broadband AND no cellular connectivity.
  IMPORTANT: Only total is supported.
- none = No Trouble messages are displayed on the CPE or History ever for loss broadband or cellular connectivity,
- channel = “Connectivity” Trouble messages are displayed in the CPE and logged when there is either no broadband OR no cellular connectivity.

Value Type	Value Range	Platform	Default Value	Tier Type
enum	total, channel, or none	Converge	total	client
		Touchstone	total	

touchscreen.doorLock.maxAllowed

Maximum number of door locks a customer is allowed to install.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	0 thru 100	Converge	4	client
		Touchstone	0	

touchscreen.quickarmcountdown.length

After pressing the Quickarm button, the number of seconds the notification is displayed on the touchscreen before the Exit Delay starts.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	0 thru 10	Converge	10	client

touchscreen.sensor.commFail.alarmDelay

The time, in minutes, since the last time a sensor has checked in that the touchscreen waits before sending a Sensor Communication Failure ALARM message. The Contact ID 147 is sent to the central monitoring station.

Note: This Tier Property is viewable in the Advanced Tier Properties table in the Edit Tier screen. This Tier Property is only configurable by database scripts or by direct database access.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	60 – 1440	Converge	720	client

touchscreen.sensor.commFail.troubleDelay

The time, in minutes, since the last time a sensor has checked in that the CPE waits before sending a Sensor Communication Failure TROUBLE message. The Contact ID 381 is sent to the central monitoring station.

Note: This Tier Property is viewable in the Advanced Tier Properties table in the Edit Tier screen. This Tier Property is only configurable by database scripts or by direct database access.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	56 – 1440	Converge	360	client
		Touchstone	360	

tvr.banner.enabled

Enable or disable the banner and First Time User Experience (FTUE) screen shown on the touchscreen camera app screen to promote TVR to subscribers.

Value Type	Value Range	Platform	Default Value	Tier Type
boolean	True/False	Converge	False	client

tvr.enabled

Enable or disable the Touchscreen Video Recording feature.

Value Type	Value Range	Platform	Default Value	Tier Type
boolean	True/False	Converge	False	client

video.upload.dailyLimit

Video upload daily limit for a customer account.

Value Type	Value Range	Platform	Default Value	Tier Type
integer	0 thru 3000	Converge	1	server
		Touchstone	1	

view.thermostat.event

Indicates whether to send all thermostat events to the server. If set to false, the CPE only sends thermostat state changes.

Note: This Tier Property is viewable in the Advanced Tier Properties table in the Edit Tier screen. This Tier Property is only configurable by database scripts or by direct database access.

Value Type	Value Range	Platform	Default Value	Tier Type
boolean	True/False	Converge	false	server
		Touchstone	false	

2.4.4 Managing Smash & Grab Properties (Converge Only)

The following are the Tier Properties associated with Smash & Grab:

- `alarm.alarm.smashAndGrab.contactId` (default value: 113901001)
- `alarm.smashAndGrab.send` (default value: "true")
- `alarm.smashAndGrab.waitTime` (default value: 120 seconds)

The system servers monitor accounts for Smash & Grab scenarios if the `alarm.smashAndGrab.send` value is true.

There are two Smash & Grab use cases:

- The server receives an Entry Delay alert, but no further alerts. The server IMMEDIATELY sends `alarm.alarm.smashAndGrab.contactId` to the central monitoring station.

  After the Entry Delay alert, the server expects to receive the following:

  - An alarm with a Transmission Delay (instructions not to send the alarm to the central monitoring station until it receives another event instructing it to do so).
  - Then the server expects to receive either:
    - Event telling it to send the alarm
    - Abort/Cancel event; the subscriber has successfully entered the keypad code
- The server receives an alarm event, but loses connectivity with the touchscreen before it has forwarded the alarm to the central monitoring station (Transmission Delay period).

- The server waits for the value of the `alarm.smashAndGrab.waitTime` Tier property (default 120 seconds).
- After that period completes, if it has not received either an Event telling it to send the alarm or an Abort Cancel event, it sends `alarm.alarm.smashAndGrab.contactId` to the central monitoring station.

Note: This logic is needed for CP-01 compliance.

Note: If the server loses all connectivity with the touchscreen AFTER an alarm automatically cancels, (which occurs after four minutes) no smash and grab CID is sent to the server.

2.5 Managing Cellular Profiles (Converge Only)

Service providers may choose to provide a cellular connection as an alternate form of communication for the touchscreen if the subscriber's broadband connection goes down. The Cellular Profile can be assigned to the touchscreen when it is added to the inventory or any time thereafter as long as it is not associated to an account (activated).

2.5.1 Add a Cellular Profile

1. From the main menu, select **Advanced > Manage Cellular Profile**.
2. Click **Add**.
3. Enter values for the Cellular Profile.

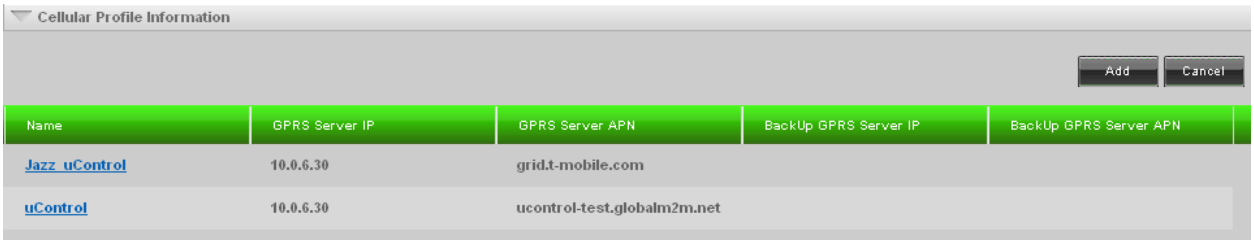
Field	Description
Cellular Profile Name	Name of the cellular profile.
GPRS Server IP	IP address of the cellular server.
GPRS APN	Access Point Name of the cellular server.
Backup GPRS Server IP	IP address of the backup cellular server.
Backup GPRS APN	Access Point Name of the backup cellular server.

4. Click **Save** to return to the *Cellular Profile Information* screen.

2.5.2 Edit a Cellular Profile

1. From the main menu, select **Advanced > Manage Cellular Profile**.

   The Cellular Profile Information page is displayed. Click on any of the column headers to sort by that column.



2. To view the details of a Cellular Profile, click the profile name in the list.
3. Make modifications as necessary on the *Edit Cellular Profile Information* screen and click **Save**.
4. Changes are immediately communicated to the associated touchscreens that are online.

2.5.3 Delete a Cellular Profile

1. From the main menu, select **Advanced > Manage Cellular Profile**.

   The Cellular Profile Information page is displayed. Click on any of the column headers to sort by that column.

2. Click the profile name to be deleted.
3. Click **Delete** on the *Edit Cellular Profile Information* screen.

Note: If touchscreens are still associated with the Cellular Profile, the button will be greyed out. A Cellular Profile can not be deleted if one or more touchscreens are associated with it.

2.6 Managing Device Descriptor Lists

The Device Descriptor List and the Blacklist control the pairing and updating of the firmware for ZigBee devices and cameras. This methodology allows service providers to have greater control over which devices are available to their subscribers. This method ONLY manages ZigBee devices and cameras that can be paired to the CPE. It does not refer to routers or any other type of device that otherwise interfaces with the CPE.

There are two types of lists that manage device pairing and updating:

- Device Descriptor List (also known as, the whitelist or DDL)
  An all inclusive list: This XML file lists all the devices certified for the Converge and Touchstone platforms. The details on this list are defined by Icontrol. Only one DDL per platform is supported. Each platform requires a DDL defined in the Management Portal in order for devices to pair to the subscriber systems. The DDL applies to all accounts, regardless of Tier or Package. This file uses the naming convention: `[platform]DevicesAllowed[version].xml` (where *platform* is *Converge* or *Touchstone*).

  IMPORTANT: This file and all updates are provided by Icontrol and must *never* be edited.

- Blacklist
  An exclusionary list: This XML file lists the devices on the DDL that are not allowed to pair to the Converge and Touchstone platforms. Blacklists are maintained by the service provider. Multiple Blacklists are supported allowing the service provider to customize the available devices by Tier or Package. Each Tier must point to a Blacklist, even it the file contains no items or if it's the same Blacklist for all Tiers. A Package that includes the `deviceDescriptor.blacklist` Tier Property, must point to a Blacklist file.

The CPE downloads the appropriate DDL and/or Blacklist files when:

- The CPE is activated
- The account Tier or Package is modified to point to a different Blacklist

- The subscriber is assigned to a new Tier or Package that points to a different Blacklist
- A new DDL and/or Blacklist is available

Note: If a paired device is removed from a DDL or excluded via a blacklist, the device continues to function with the CPE (even after the CPE is RMA'd) , but the device will not receive firmware updates. If the device is deleted, it cannot be re-paired.

2.6.1 Upload a Device Descriptor List

1. Obtain the URL of the Device Descriptor List(s) . See the "Set up the Device Descriptor List Location" in *Multi-Cluster Server Installation Guide*, "Replace the Device Descriptor List and Device Firmware Files" in *Multi-Cluster Server Upgrade Guide* or the system administrator for more information.
2. From the main menu, select **Advanced > Update Device Descriptor List > Update Converge Device Descriptor List** (for the Converge DDL)

   or **Advanced > Update Device Descriptor List > Update Touchstone Device Descriptor List** (for the Touchstone DDL).

   The Update Device Descriptor List is displayed.

3. Into the **Test Device Descriptor List URL** field, enter the URL to the `DevicesAllowed [version].xml` file.
4. Click **Update TEST DDL** to test the validity of the URL.
5. Click **Promote TEST DDL** to set the new device descriptor file if the test was successful.

2.6.2 View the Contents of the DDL

IMPORTANT: The device descriptor list must not be edited, however the content is viewable for troubleshooting purposes.

1. From the main menu, select **Advanced > Update Device Descriptor List > Update Converge Device Descriptor List** (for the Converge DDL file)

   or **Advanced > Update Device Descriptor List > Update Touchstone Device Descriptor List** (for the Touchstone DDL file).

2. Copy the URL in the *Device Descriptor List* field.
3. Paste the URL into the Address field of your browser.
4. Modify the URL based on your server authentication settings (if necessary).

5. Press **Enter**.

   The DevicesAllowed[version].xml is displayed in your browser.

2.6.3 Create a Blacklist

Icontrol recommends creating a Blacklist even if no devices are being excluded or if some Tiers/Packages will not be excluding devices. A *blank* Blacklist can be used.

For example, a file named `blacklist_blank.xml` with the following contents is a valid Blacklist:

```
<DeviceDescriptorBlackList version="1.0.0">
</DeviceDescriptorBlackList>
```

To exclude a device, only the UUID of the device is needed to be included in the Blacklist to be excluded. The UUID can be obtained from the device or the DDL. The following is an example of the blacklist file contents. All blacklist files must use the following format:

```
<DeviceDescriptorBlackList version="1.0.0">
    <uuid>559C8B8E-E0AB-4F5D-8712-B29B7B79E248</uuid>
    <uuid>806F63F2-236F-4DB7-855A-E6EDDD985DCC</uuid>
    <uuid>8A41C742-BD6D-4139-8E84-8B4C0A08C778</uuid>
    <uuid>2B57DB57-04C1-4A75-BFE1-2AB2E484DDAA</uuid>
</DeviceDescriptorBlackList>
```

IMPORTANT: The `version` parameter is required for the file to be valid. Its value must be in the format: "`[number].[number].[number]`"

When creating more than one Blacklist, Icontrol recommends naming each Blacklist file to indicate the devices that it excludes. For example, `blacklist_thermostats.xml`.

Once the Blackist is created, the URL for the Blackist(s) must be added to the Tier Property `deviceDescriptor.blacklist` in each Tier and/or Package. See Managing Tiers on page 19 and Managing Packages on page 22 for more information.

For CPEs that try to activate to an unrecognized Blacklist:

1. The download of the list of excluded devices to the CPE fails
2. The error is noted in the History of the account.
3. The CPE will pair devices as if it were using a blank blacklist file (no devices are excluded).

2.6.4 Update Blacklist Files

1. As necessary, modify Blacklist file(s).
2. Update the version parameter in the file, i.e. `version="1.0.1"`

3. If the Blacklist is currently in use by a Tier or Package, the file must be renamed. The CPE will not recognize that the Blacklist has been modified unless the file is renamed (i.e. updating the version number) or the URL path has changed.

4. Access and modify the `deviceDescriptor.blacklist` Tier Property for every Tier or Package that points to the URL of new or modified Blacklist. See "Managing Tiers" on page 19 and "Managing Packages" on page 22 for more information.

General Caveats For Modifying a Blacklist File

Do not delete a pre-modified version of a blacklist file until the new version is verified to be valid and correct by validating the Blacklist XML file against the Blacklist.XSD file provided by Icontrol. This validation process will ensure that the XML file is syntactically correct. This process will not ensure that the excluded the devices are the ones intended to be excluded. If a new Blacklist is valid but excludes the wrong devices, no error will be reported.

The following errors will cause a new Blacklist to be judged invalid by a CPE:

- The subscriber's Tier/Package does not find a valid path/filename configured in its `deviceDescriptor.blacklist` Tier property
- The new/updated file has typographical errors

When a CPE discovers that a Blacklist is invalid, the event is noted in the History of the account:

```
System Trouble - err downloading the "black list" file.
```

(see "History Report" on page 125 for information on view the System Status History of an account)

2.7 Managing Partners

Partners are third-parties with cloud services or devices that have gone through Icontrol's Cloud Integration Certification Program to become part of the ecosystem. Once a partner is added via the Management Portal, the cloud device or service appears as a device to the subscriber. A subscriber must already have an active account with the partner prior to attempting to add the cloud service or device to the subscriber's Touchstone or Converge account. The device type determines the controls and monitoring that are available and whether it can be used as an automation trigger, action, or both. The information will be provided by the partner.

To access the **Advanced > Manage Partner** menu, the employee must have "Admin" or "CAT Manager" privileges. See Management Portal Roles on page 71.

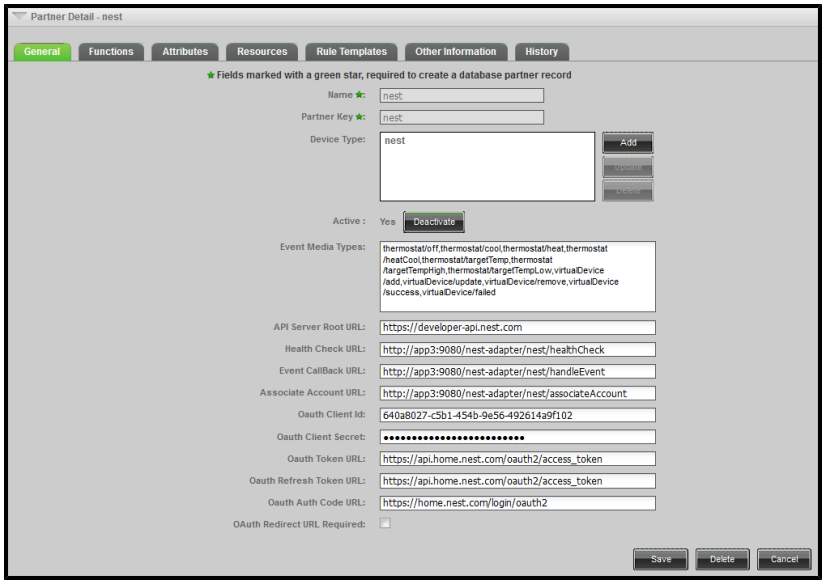
2.7.1 Add a Partner

1. From the main menu, select **Advanced > Manage Partner > Add** to display the "Partner Detail" screen. On the **General** tab, input the following information given from the partner.

   IMPORTANT: Accuweather can not be added as a partner via the Management Portal. See *Cloud Integration Service Installation Guide* for instructions on adding AccuWeather as a partner.

Field	Description
Name	The unique name used to define the partner (alpha-numeric characters only; no spaces or special characters) **IMPORTANT:** The partner name must be the same name that is used in the corresponding card for the partner in the Web and Mobile Apps.
Partner Key	A unique key issued by Icontrol to the partner (alpha-numeric characters only; no spaces or special characters) **IMPORTANT:** The partner key must be the same key that is used in the corresponding card for the partner in the Web and Mobile Apps.
Device Type	Click the **Add** button to display another pop-up and add the devices associated with the partner (duplicate devices are not allowed). **IMPORTANT:** If a partner has multiple devices, each device must have the partner name as a prefix; i.e. for Nest integration, device types can be "nest" for the thermostat and "nest-co" for the carbon monoxide detector.
Active	Allows the service provider to control whether the cloud device or service is available to subscribers without deleting the partner. Default is "No" when a partner is first added.
Event Media Types	The list of event media types that the partner has submitted to Icontrol.
API Server Root URL	The root URL of the partner's server. Icontrol will call this server to access the API provided by the partner.
Health Check URL	The URL to check the availability of the partner's server.
Event CallBack URL	The URL to submit events to the partner's system.
Associate Account URL	The URL used to get a user's partner account and its list of associated devices after OAUTH.
Oauth Client Id	The OAuth client ID issued by the partner.
Oauth Client Secret	The OAuth client secret issued by the partner.
Oauth Token URL	The URL to get the OAuth token from the partner.
Oauth Refresh Token URL	The URL from which to get the OAuth refresh token from the partner.
Oauth Auth Code URL	The URL from which to get the OAuth authorization code. This is typically a login page provided by the partner.
OAuth Redirect URL Required	Check the box if an OAuth redirect URL is required

The following image displays Nest as an example:



2. Click **Save**.

   Note: The partner must be saved with all URLs, Oauth Client ID, and Oauth Client Secret before the other tabs are available.

3. Click on **Functions > Add** to add the device functions, if applicable. Once a function is added, click  to edit or  to delete the function.

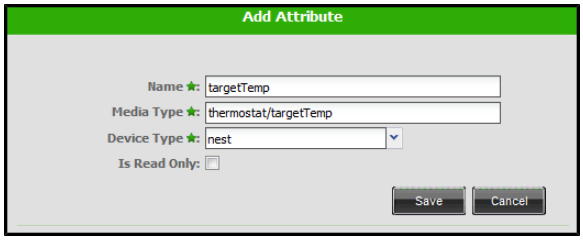
   The following image displays a Nest function as an example:

Field	Description
Name	Name of the cloud object function. For example, for a thermostat, this value could be heat or cool.
Media Type	The media type of the resource. For example, for a thermostat, this value could be thermostat/heat or thermostat/cool.
Description	Description of the function

Field	Description
Device Type	Drop-down menu listing the devices added to the partner in the **General** tab
Argument Name	Unique key
Argument Media Type	The media type of the item
Argument Type	Defines the argument type: integer, double, string, enum, Boolean
Value Constraint	Defines constraints on the value

4. Click on **Attributes > Add** to add the device attributes, if applicable. Once an attribute is added, click  to edit or  to delete the attribute.

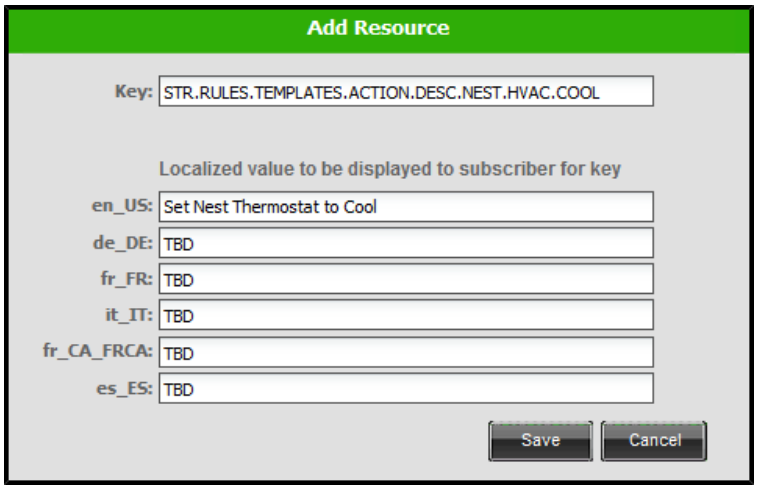
   The following image displays the attribute for the Nest function in the previous step as an example:



Field	Description
Name	The attribute name. Unique key
Media Type	The media type of the attribute.
Device Type	Drop-down menu listing the devices added to the partner in the **General** tab
Is Read Only	A checked box indicates the attribute is read only.

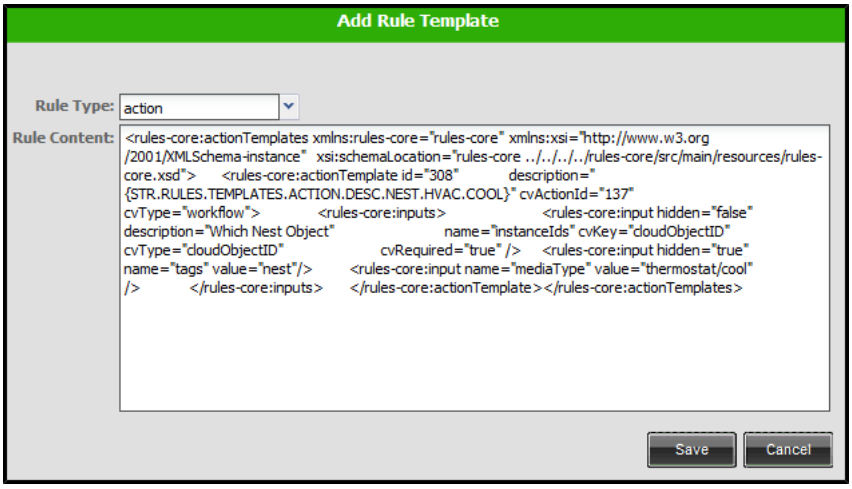
5. Click on **Resources > Add** to add a resource or click on **Change Locale** to change the default language. A resource is needed for each rule template.

   The following image displays the resource for the Nest rule to set the thermostat to cool:



6. Click on **Rule Templates > Add** to add the action and trigger templates for the device or service. These provide the framework for the rules that the subscribers can create. Once a template is added, click  to edit or  to delete the template.

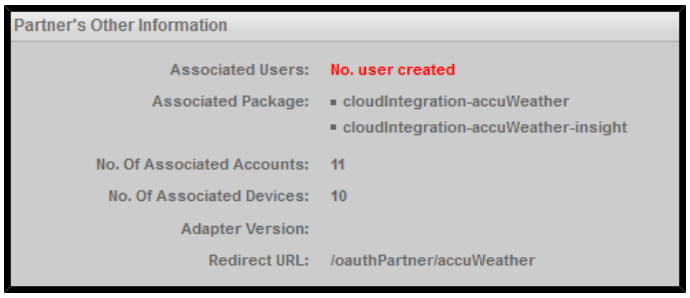
   The following image displays the rule template for the Nest resource in the previous step:



Field	Description
Rule Type	Whether the template is for an action occurring in response to a trigger from a schedule or another device, or for a trigger to cause an action to be executed.
Rule Content	The template of the desired actions of the rule provided by the partner.

7. Click on **Other Information** to view additional details about the partner.

   The following image displays AccuWeather as an example:

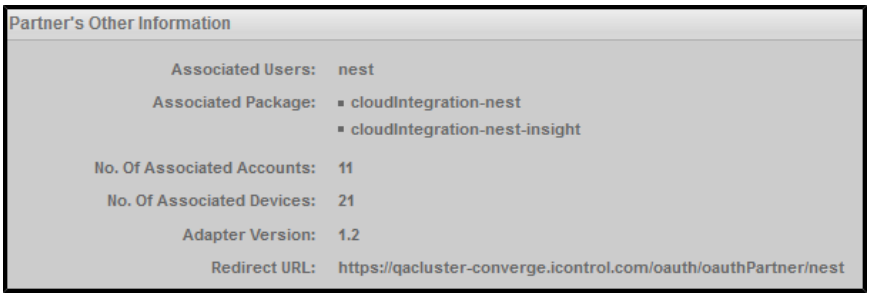


8. Click on **History** to view the activity history of the partner; for example, service offline/online events. The events are listed by day. Click on a date listed, use the Previous or Next links to navigate the dates, or click the calendar icon to select a date.

2.7.2 Enable a Partner

When a partner is first added, the "Active" option on the **Partner Detail > General** screen is set to "No" by default. This setting allows the service provider to control when the cloud device or service is available to subscribers. Before enabling a new partner, a new "Cloud Integration" employee must be created for the partner.

1. From the main menu, select **Advanced > Manage Employee** and click **Add**.
2. Fill in the required fields with the information provided by the partner.
3. Expand **Advanced Roles** and select **Cloud Integration**.
4. From the Cloud Integration drop-down menu, select the partner and click **Save**.
5. Navigate to **Advanced > Manage Partner** and click on the partner link.
6. On the **General** tab, click **Activate** to enable the partner.
7. Navigate to the **Other Information** tab and verify that the employee is listed in "Associated Users". In the image below, the employee is "nest".



2.7.3 View all the Partners

From the main menu, select **Advanced > Manage Partner** to display the list of all the partners. Click on any of the column headers to sort by that column. Click on the link for the partner number to display the details for that partner. Click **Cancel** to return to the list.

2.7.4 Disable a Partner

A partner can be disabled by clicking on the **Deactivate** button on the **General** tab. This allows the service provider to remove access to the partner without deleting the partner. A partner can be deactivated while accounts are still associated with it, but it can not be deleted. When a partner is deactivated:

- The subscribers can not create automations with the partner's cloud device or service
- Existing automations with the partner's cloud device or service (if any) will not run
- The partner can not log in to the Cloud Integration Service to send or receive events
- Clients can not call the partner's API(s)

Setting the partner to "Active" will restore all the functionality and make the cloud device or service available to the partner and subscribers once more.

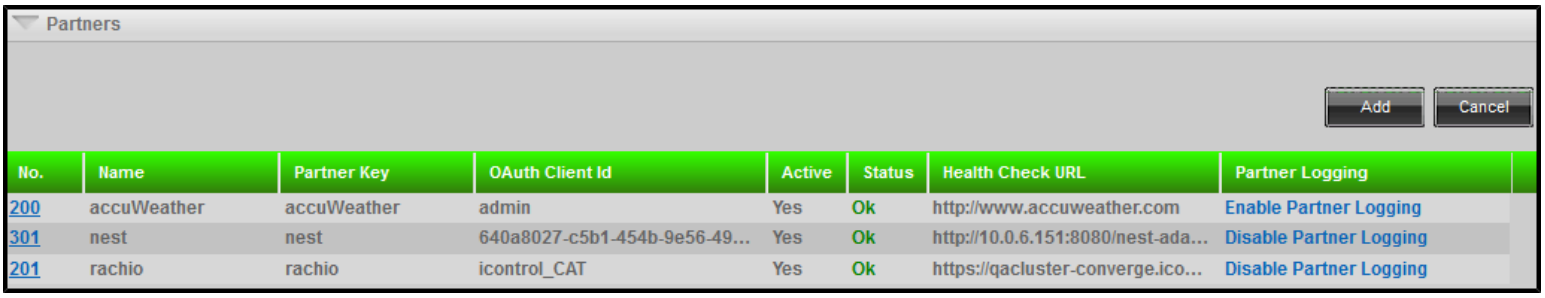
2.7.5 Delete a Partner

From the main menu, navigate to **Advanced > Manage Partner**. Click on any of the column headers to sort by that column. Select the partner and click **Delete**. Deleting a partner removes all information from the database, the Management Portal, and the Web and Mobile Apps. In order for the partner to be deleted, there must not be any accounts associated with it. If there are still accounts associated with it, the partner can be deactivated instead.

IMPORTANT: This action can not be undone. If the partner is deleted, it must be added as a new partner.

2.7.6 Enable/Disable Partner Logging

Service providers can enable partner-specific debug logging in the partner proxy. The debug information will be found in the Admin server logs. To enable/disable partner logging, navigate to **Advanced > Manage Partner** and click on the "Enable Partner Logging" link. The link will toggle to "Disable Partner Logging". Click the link again to disable.



2.8 Managing Apps (Converge Only)

Touchscreen Apps are third-party software applications that are accessible from the touchscreen. There is no limit to the number of Apps that can be added to the Converge platform. Service providers control the deployment of an App by promoting the App to one or more Tiers or deactivating it.

Note: For SMC P5 touchscreens, Apps are known as Widgets.

From the main menu, select **Advanced > Manage Apps**. The *Apps* screen is displayed listing all the Apps that have been added, regardless of Tier or status. Click on the column headers to sort by that column.

Column	Description
ID	Name of the app.
Name	Name of the app displayed in the touchscreen.
Promoted	Whether the app is available for download to touchscreens.
URL	Path to the hosting location of the app content.
Category	Indicates whether the app is an Android or Flash app. If the value is N/A, then it is a Flash app.
Software Version	Current version number of the app.

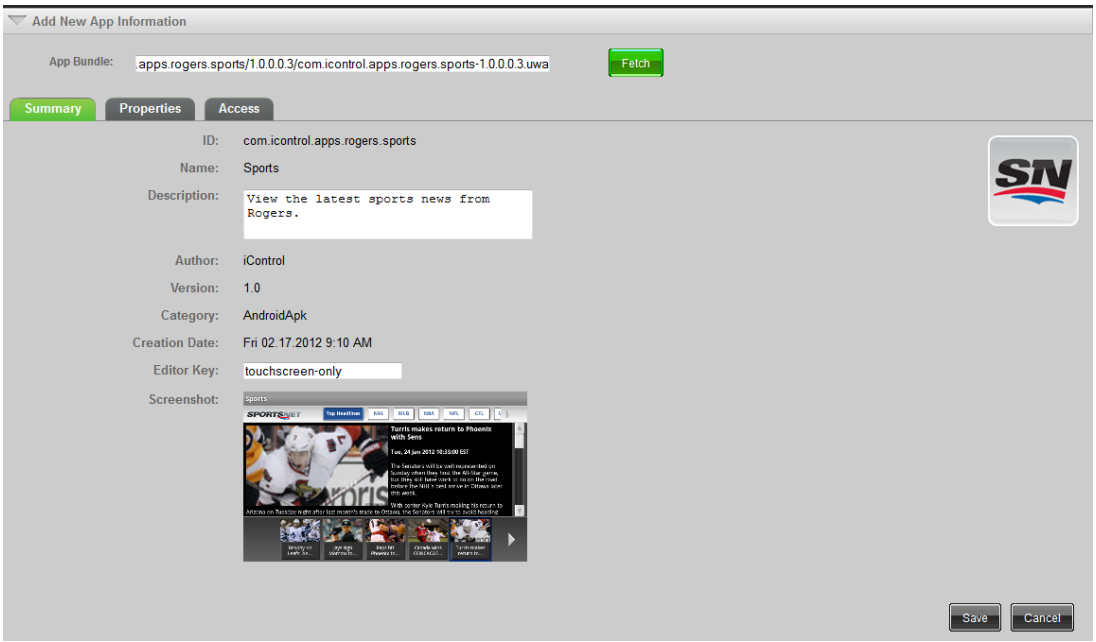
2.8.1 Add a New Touchscreen App

Adding a Touchscreen App is done in 2 steps. First it must be imported, then it must be assigned to the Tier(s) and promoted. By default, the new App is associated only to the Test Tier when it is added.

1. From the main menu, select **Advanced > Manage Apps**.
2. From the *Apps* screen click **Add**.

   The Add New App Information screen is displayed.
3. Enter the URL of the `.uwa` file of the App in the App Bundle field, and click **Fetch**.

   The fields of the Summary, Properties, and Access tabs are populated, if the information is available in the App bundle.



4. The *Summary* tab displays the basic information for the App. Update the fields, if necessary.

Element	Description
App Bundle	URL of the .uwa file of the App.
ID	Identifier for each App; This value must be unique for each promoted App. When a new App is promoted, if it has the same ID as a currently promoted App, the previous App is overwritten in the Apps screen. Naturally, the App bundle itself is not overwritten. However, to use the overwritten App, it's <id> value must be changed to a unique value and then the App must be re-added to the Apps screen.
Name	Name of the App displayed in the touchscreen;
Description	Short description of the purpose of the App
Author	Person or company that developed the App;
Version	App version.
Category	The category assigned to the App
Creation Date	Compile date of the App file.
Editor Key	Points to a file used by the App to manage the look-and-feel of the App.
Screenshot	The image located at /images/screenshot.png in the App bundle.

5. The *Properties* tab displays the defined properties for the App and is divided into three sections.

Section	Description
Defined	All the properties defined by the App developer for the Touchscreen App. If no Defined properties are available, there will not be any Admin or Premise properties.
Admin Properties	Properties listed in the Defined section for which the value of the <admin> field is true. This field is set by the developer of the App and can not be modified via the Management Portal. Admin properties govern the behavior of a Touchscreen App and do not allow the value to be changed within the App by the user. Some Admin properties can be Tier-specific. For example, how often the Traffic app checks for updated information can be a shorter period for Gold Tier subscribers.
Premise Properties	Properties listed in the Defined section for which the value of the <admin> field is false. This field is set by the developer of the App and can not be modified via the Management Portal. Premise properties govern the behavior of a Touchscreen App and their values can be changed by the user within the App. These values define the defaults for the current app when it is first installed on the Touchscreen.

Property details are listed below. Update properties as necessary.

Field	Description	
Name	Name of the property.	
Admin	The property is an Admin property if the value of the Admin field is true.	
	The property is Premise property if the value of the Admin field is false.	
Type	Value of the property such as Integer, Boolean, PairEnum, etc.	
Description	A short description of the behavior of the property.	
Default	Default value of the property.	
Multiselect	true	User can select multiple elements within this property. For example, in the News app, a category (cats) property defines the categories of news feeds displayed by the app. The user can show RSS feeds from the Sports category and from the Business category.
	false	Property does not support multiselect. For example, the pollRate property defines how often an app fetches new information for the app. If this value is false, the app will not update, for example, feed categories at separate rates.
Tier	Whether the property is available for all Tiers (Global) or only certain Tiers.	
Value	Current value of the property.	
Constraint	Limitations on the default information displayed by the app. For Premise properties, the user can modify the constraints. For example, a user of the News app might choose not to display RSS feeds from the RSS category.	

4. The *Access* tab displays all the Tiers available for the App and options for how the App is installed onto the touchscreens. Only the Test Tier is available until the App has been promoted.

Column	Description
Tier	The list of all the tiers.
Access	Checked box indicates the App is available to the touchscreens in the Tier.
Auto Push	Checked box indicates that when the App is added or modified, it will automatically be installed on all touchscreens in the associated Tier if/when they are disarmed and have a broadband connection to the servers. **Note:** If "Auto-Push" is selected but not "Add on Activation" for a Tier, all touchscreens currently activated will have the new App installed, but touchscreens that are activated subsequently will have to have the App manually installed.

Column	Description
Add On Activation	Checked box indicates the App will be installed on the touchscreen is in the associated Tier at Activation (when the touchscreen is initially installed and connected to the server). **Note:** If "Add On Activation" is selected but not "Auto Push", only the touchscreens activated after the App is added will have the App automatically installed. Touchscreens already activated will have to have the App manually installed.
Deployment	The list of deployments. Hold down the Ctrl key to select more than one. If deployments are not used, the field will not be displayed.

5. Click **Save**.

   If a previous version of the App (one having the same ID) was already associated with the touchscreens in the Test Tier, the previous version is no longer available on those touchscreens. If the previous version was associated with customer Tiers, it is still available on those touchscreens.

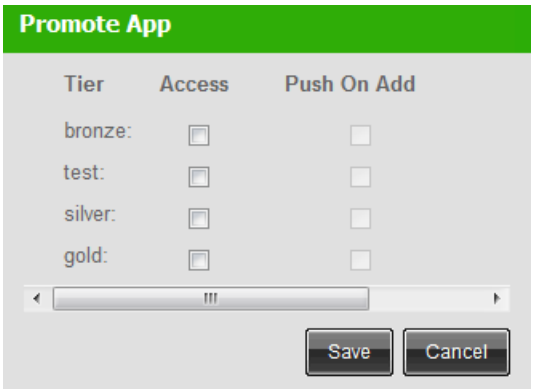
2.8.2 Promote a Touchscreen App

Once the Touchscreen App is ready to be made available to the subscribers, the App can be promoted.

1. From the main menu, select **Advanced > Manage Apps**.
2. Click the **App ID** of the App to be promoted.

   The App Information screen is displayed.

3. From the *App Advanced Actions* menu, click on **Promote**.
4. Select the Tiers that will have access to the App. When the Tier is selected, the option to "Push On Add" is available. This can be selected at this time or the App can be "pushed" to the Tiers any time after the App is promoted.

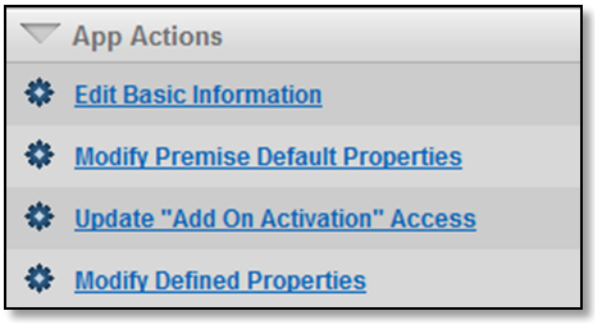


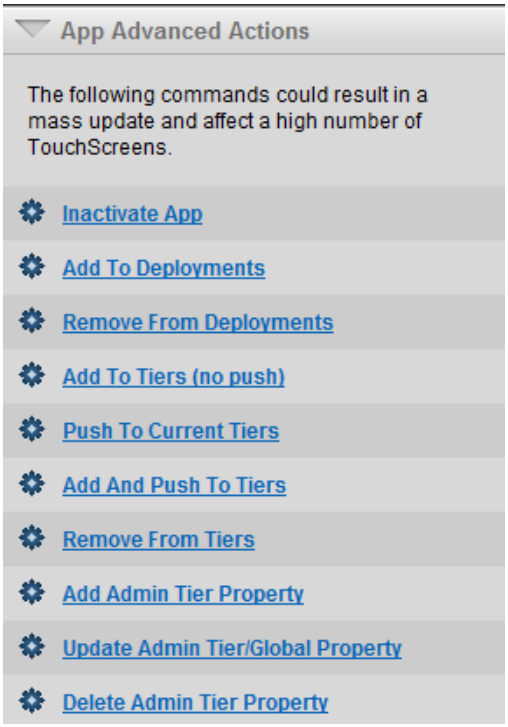
5. Click **Save**.
6. Navigate to the Apps screen and verify the App displays "Yes" on the Promoted column.

2.8.3 Touchscreen App Actions

Once an App is promoted, the following actions are available:

- Edit the information on the *Summary* tab
- Modify Tier "Add On Activation" access
- Add Tiers that have access to the App
- Push the current app to all Tiers the App is associated with
- Remove Tiers from having access to the App
- Modify App properties

Menu	Function	Description
	Edit Basic Information	Edit the Name, Description, and/or Editor Key of the App
	Modify Premise Default Properties	Edit the value(s) of a Defined property that has the Admin flag set to "false".
	Update "Add on Activation" Access	Add or remove the requirement from the Tiers associated with the App. Checked box indicates the App will be installed on the touchscreen is in the associated Tier(s) when the touchscreen completes activation. Unchecked box indicates the App must be manually installed. Modifying this field does not affect touchscreens that have already been activated. If a checkbox is deactivated, that Tier does not have access to the App.
	Modify Defined Properties	Edit Defined properties that have a value constraint.

Menu	Function	Description
	Inactivate App	Removes the App from the list of Apps, from all Tiers, and from any touchscreens that have the App installed. The App information remains in the database, however it must be imported as a new app in order for it to be activated again.
	Add To Deployments	Add the App to selected Deployments. Hold down the Ctrl key to select more than one. If a Deployment is not selected, the App will not be available to the subscribers, regardless of the Tier(s) that has access to the App. If Deployments are not used, the field will not be displayed.
	Remove From Deployments	Remove the App from selected Deployments. Hold down the Ctrl key to select more than one. If a Deployment is not selected, the App will not be available to the subscribers, regardless of the Tier(s) that has access to the App. If Deployments are not used, the field will not be displayed.
	Add To Tiers (no push)	Adds access to the App to the touchscreens on the selected Tiers. The App must be manually installed.
	Push To Current Tiers	Automatically installs or updates the App to the activated touchscreens on the selected Tiers. If a touchscreen is armed and/or broadband connection is down, the App will be installed or updated if/when it is disarmed and/or has a broadband connection to the servers.

Menu	Function	Description
	Add And Push To Tiers	Adds access to the App and automatically installs the App to the touchscreens on the selected Tiers. If a touchscreen is armed and/or broadband connection is down, the App will be installed if/when it is disarmed and/or has a broadband connection to the servers.
	Remove From Tiers	Remove access to the App from the selected Tiers. Touchscreens that have the App installed will have the App automatically uninstalled with no warning to the user. If a touchscreen is armed and/or broadband connection is down, the App will be uninstalled if/when it is disarmed and/or has a broadband connection to the servers.
	Add Admin Tier Property	If an Admin property is available, the property can be added set to a different value to selected Tiers, overriding the value set for Global Tiers. Once the action is complete, the App will be automatically reinstalled to the touchscreens that have the App already installed. If a touchscreen is armed and/or broadband connection is down, the App will be reinstalled if/when it is disarmed and/or has a broadband connection to the servers. **Note:** If the Admin Tier Property is desired on multiple Tiers, a new Admin Tier Property must be added for each Tier.

Menu	Function	Description
	Update Admin Tier-/Global Property	If an Admin property is available, the property can be modified for the assigned Tier or globally. Once the changes are saved, the App will be automatically reinstalled to the touchscreens that have the App already installed. If a touchscreen is armed and/or broadband connection is down, the App will be reinstalled if/when it is disarmed and/or has a broadband connection to the servers.
	Delete Admin Tier Property	If an Admin property has added to a Tier, the property can be deleted. Admin properties defined by the App can not be deleted. Once the action is complete, the App will be automatically reinstalled to the touchscreens that have the App already installed. If a touchscreen is armed and/or broadband connection is down, the App will be reinstalled if/when it is disarmed and/or has a broadband connection to the servers.

3 Managing Inventory

Before a CPE can be activated, the CPE must be created in the Management Portal. CPEs can be created one at a time or in batches by importing from a text file. Once the CPE is created, the information can be modified and the CPE can be deleted if the CPE has not been activated.

Converge only: If the SIM card phone number and/or cellular account number is not available when the touchscreen is created, the touchscreen can still be created however, this information must be added to the touchscreen information before the device can be activated. This information is also required to enable the central monitoring station to contact the customer through the touchscreen (two-way voice communication) in the event of an alarm.

3.1 Add a Single CPE to Inventory

1. From the main menu, select **Inventory > Create New CPE Device > Create New Converge CPE Device** or **Create New Touchstone CPE Device**.

   The Add New Converge/Touchstone CPE Device Information screen is displayed.

Field	Product	Description
CPE ID	Both	Default Ethernet MAC Address, without colons (:)
Hardware Model	Both	Model of the device
Hardware Revision	Both	Revision code of the device
Serial Number	Both	Unique ID of the device.
IMEI Number	Converge	Unique ID of the cellular module in the touchscreen.
ICC ID	Converge	Unique ID for the SIM card in the touchscreen (required if importing SIM card information).
SIM Card Phone Number	Converge	Phone number assigned to the touchscreen's SIM card.
SIM Card Account Number	Converge	Account number that the cellular service provider associates with the SIM card.
Cellular Profile	Converge	Cellular carrier (AT&T, T-Mobile, etc.) used by the touchscreen. IMPORTANT: If this value is incorrect, the touchscreen will not have cellular service even though the rest of the SIM card information is correct.
Deployment	Converge	Deployment to which the touchscreen is assigned; Only displayed for systems that use deployments.

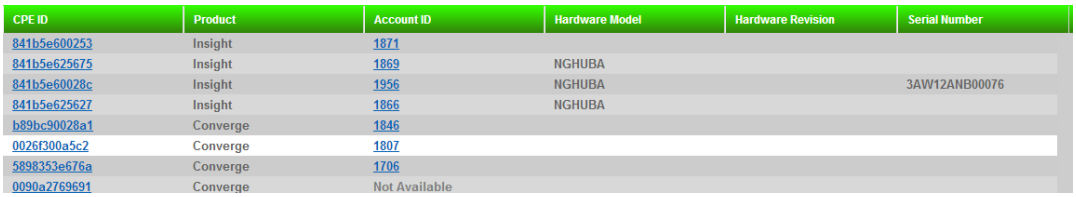
2. Enter the information for the CPE.
3. Click **Save** or **Save and New** to open a new window for creating another CPE.

3.2 Modify CPE Information

IMPORTANT: The CPE information can be viewed for all CPEs, however if the device is associated with an active account, any changes made will not take effect until the device is disassociated from the account.

1. From the main menu, select **Inventory > Search for CPE Device**.
2. In the CPE ID field, enter the full ID of the device you want to find. Leave the field empty to return a list of all CPE IDs. Partial CPE ID or wildcard characters are not supported.
3. Click **Search**.

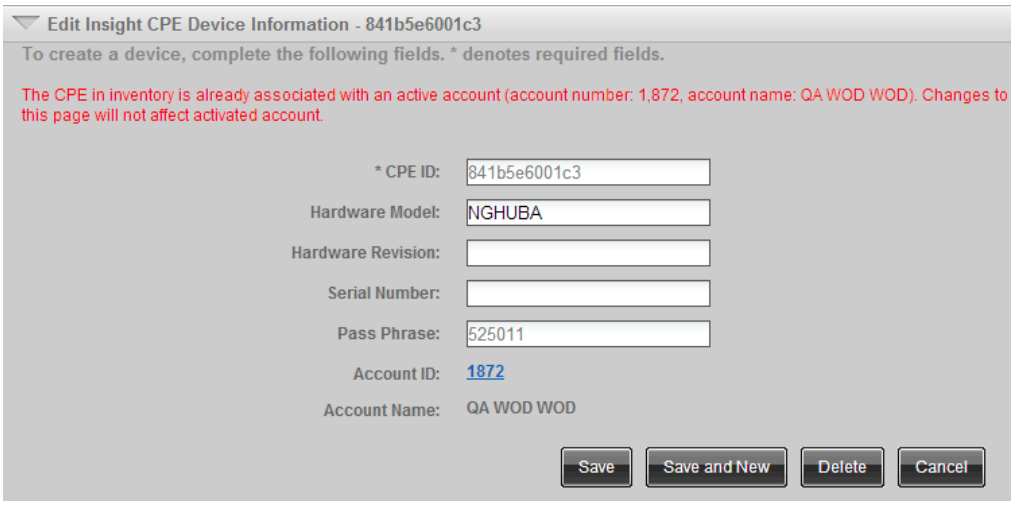
   If you did not specify a CPE ID, CPE search results are displayed. Click on any of the column headers to sort by that column.



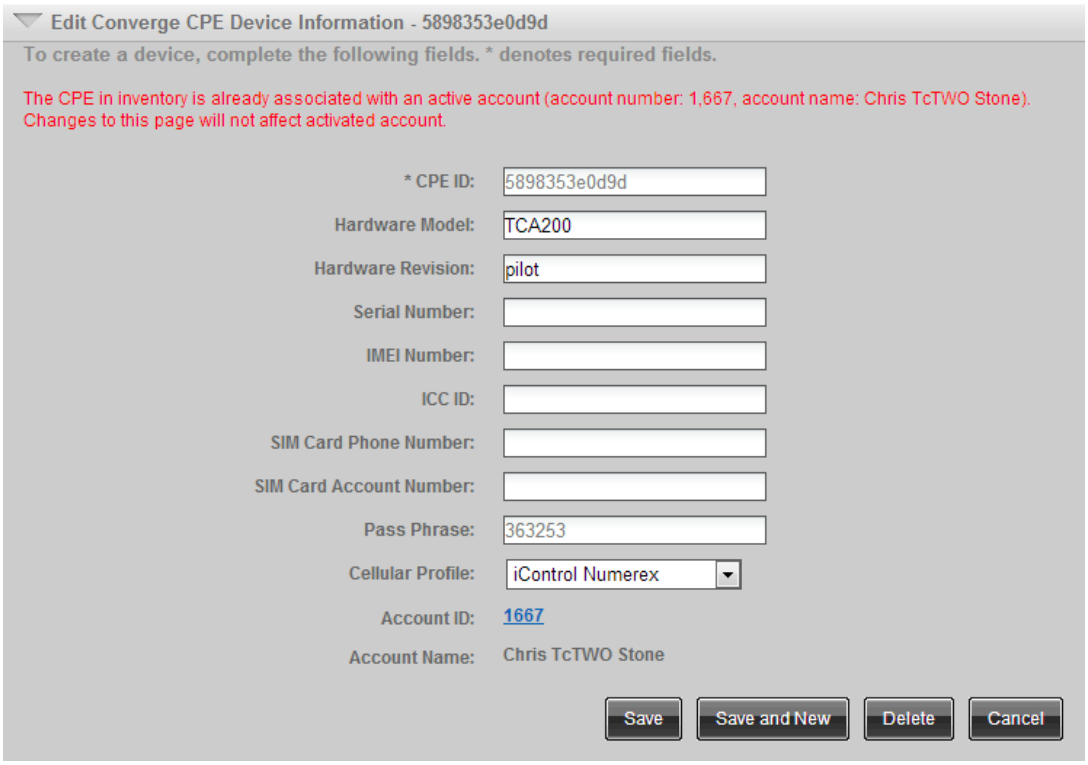
CPE ID	Product	Account ID	Hardware Model	Hardware Revision	Serial Number
841b5e600253	Insight	1871			
841b5e625675	Insight	1869	NGHUBA		
841b5e60028c	Insight	1956	NGHUBA		3AW12ANB00076
841b5e625627	Insight	1866	NGHUBA		
b89bc90028a1	Converge	1846			
0026f300a5c2	Converge	1807			
5898353e676a	Converge	1706			
0090a2769691	Converge	Not Available			

4. Click the CPE ID link to display the details of the CPE.

   If you entered the CPE ID of a Touchstone hub, the Edit Touchstone CPE Device Information screen is displayed.



   If you entered the CPE ID of a touchscreen, the Edit Converge CPE Device Information screen is displayed.



Note: Clicking the Account ID link displays the Account Information screen of the account to which the device is currently assigned.

The following table describes the elements on the *Edit Device Information* screen.

Field	Product	Description
CPE ID	Both	Default Ethernet MAC Address, without colons (:)
Hardware Model	Both	Model of the device.
Hardware Revision	Both	Revision code of the device.
Serial Number	Both	Unique ID of the device.
IMEI Number	Converge	Unique ID of the cellular module in the touchscreen.
ICC ID	Converge	Unique ID for the SIM card in the touchscreen.
SIM Card Phone Number	Converge	Phone number assigned to the touchscreen's SIM card.
SIM Card Account Number	Converge	Account number that the cellular service provider associates with the SIM card.

Field	Product	Description
Pass Phrase	Both	Default Installer keypad code on the device (not user-configurable).
Cellular Profile	Converge	Cellular profile assigned to the touchscreen. **IMPORTANT:** If this value is incorrect, the touchscreen will not have cellular service even if the SIM card information is correct. See "Managing Cellular Profiles (Converge Only)" on page 38 for more information.
Deployment	Converge	Deployment to which the touchscreen is assigned; Only displayed for systems that use deployments.
Account ID	Both	A hyperlink that takes the user to the Account Information screen of the customer account to which the device is assigned (see "Managing Accounts" on page 79 for information about the Account Information screen).
Account Name	Both	The account name assigned to the Account ID. This value cannot be edited.

3.3 Delete a CPE

1. From the main menu, select **Inventory > Search for CPE Device**.
2. In the CPE ID field, enter the full ID of the device you want to find. Partial CPE ID and wildcard characters are not supported.
3. Click **Search**.
4. On the *Edit Converge/Touchstone CPE Device Information* screen, if the error below is not displayed at the top of the information screen, the CPE can be deleted.

   The CPE in inventory is already associated with an active account (account number: 1,667, account name: Chris TcTWO Stone). Changes to this page will not affect activated account.

5. Click **Delete** to remove the CPE from inventory.

3.4 Batch-Importing CPE Devices to Inventory

Multiple Converge touchscreens or Touchstone devices can be added to the inventory at the same time by creating a comma-delimited file with the CPE data and importing the file into the Management Portal. There is no tested limit to the number of devices that can be imported and importing up to 10,000 devices has been successful, however the size of the import file must be less than 2 MB.

3.4.1 Update Server Properties

The following server properties define the contents and format of the comma-delimited file. The file must be saved as `.txt` or `.csv`.

Product	Property Name	Default Fields
Converge	cpe.import.file.format	itemNumber,poNumber,model,serialNumber, macAddress,zigbeeSN, iccId,imeiNumber,shipDate
Touchstone	cpe.import.file.format.insight	itemNumber,poNumber,model,serialNumber, macAddress,shipDate

The fields in the property can be changed or reordered by updating the property in the `custom.properties` file. See the *System Operations Guide* for details on updating system properties.

The following table describes the fields that can be listed in the `cpe.import.file.format` or `cpe.import.file.format.insight` property. Field names are case-sensitive and must not be changed if re-ordered.

Field	Description	Required?
itemNumber	The sequence number assigned to the device	No
poNumber	Purchase order number	No
model	Model of the device (P5, TCA200, etc.).	No
serialNumber	Unique ID of the device.	Yes
macAddress	Default Ethernet MAC Address of each ID (also known as CPE ID) without colons (:); For example, 00185A028020.	Yes
zigbeeSN	Zigbee serial number (Converge only)	No
iccId	Unique ID for the SIM card in the touchscreen. (Converge only)	No
imeiNumber	Unique ID of the cellular module in the device.	No
shipDate	The ship date of the device.	No
manufacturer	The manufacturer of the device, for example SMC.	No
model	The manufacturer model of the device.	No
hardwareRev	Revision code for the hardware of the device.	No
simCardPhoneNumber	Phone number assigned to the touchscreen's SIM card. (Converge only)	No
simCardAccountNumber	Account number that the cellular service provider associates with the SIM card. (Converge only)	No
wifiMacAddress	Default Wi-Fi MAC Address of each device (also known as CPE ID) without colons (:); For example, 00185A028020.	No
firmwareVersion	The firmware version installed on the device at the time it is added to inventory; This information is updated as the firmware is updated.	No

Field	Description	Required?
passPhrase	Default Installer keypad code on the device; This keypad code accesses advanced Settings menu options not available to customers.	No
module1Type	The module is the internal device that allows the CPE device to find and communicate with the sensors. Currently, the only module manufacturer that is supported is ZigBee and all devices use the same type of module.	No
module1SerialNumber		
module1FirmwareVersion		
module1Manufacturer		
module1Model		
module2Type	Although CPE devices currently have only one module installed, there is a second port available for future potential use.	No
module2SerialNumber		
module2FirmwareVersion		
module2Manufacturer		
module2Model		

The `cpe.import.log.directory` and `cpe.import.log.directory.windows` properties define the path where the log file(s) for importing CPE devices will be saved. The path can be changed by updating the property in the `custom.properties` file. See the *System Operations Guide* for details on updating system properties.

The log file(s) include the following:

- Devices that were imported to inventory
- Devices that failed to import
- Reason devices failed to import

3.4.2 CPE Import File Example

The system ignores the first line of the comma-delimited file.

The following is a sample file for importing Converge TouchScreens:

```
Item,PO #,Model # ,SN,MAC ID,ZIGBEE SN,SIM SN,GSM IMEI,Ship Date
1,9000901492,RB5701-Z RRR,M301800227,0026F300019A,
9008M3101700439,89302720400103520792,353227020977874,5/8/2010
2,9000901492,RB5701-Z RRR,M301800354,0026F300027C,
9008M3100900221,89302720400103520255,353227020977064,5/8/2010
3,9000901492,RB5701-Z RRR,M301800320,0026F300023A,
9008M3100900228,89302720400103520594,353227020977916,5/8/2010
4,9000901492,RB5701-Z RRR,M301800307,0026F3000220,
9008M3100900220,89302720400103520511,353227020976835,5/8/2010
5,9000901492,RB5701-Z RRR,M301800264,0026F30001CA,
9008M3101700744,89302720400103520552,353227020983757,5/8/2010
```

The following is a sample file for importing Touchstone devices:

```
Item,PO,Model,SN,MAC,Ship Date
1, 1234,NGHUB,6BW12AN900058,841B5E996232,3/12/2012
2, 1235,NGHUB,5BW12AN900058,841B5E995232,4/12/2012
3, 1236,NGHUB,4BW12AN900058,841B5E994232,6/12/2012
```

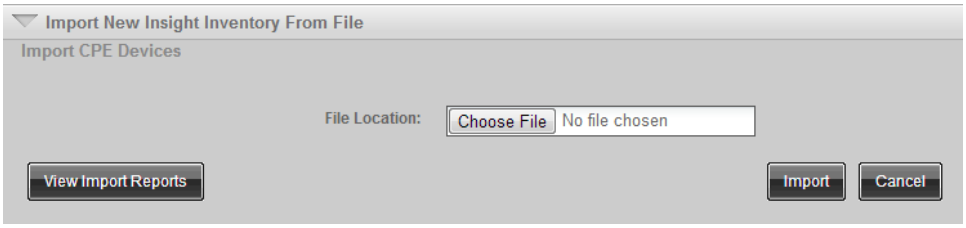
3.4.3 Import CPE Devices

1. Create a comma-delimited file with the information about the CPE devices to be added. The accepted formats are `.txt` and `.csv`.

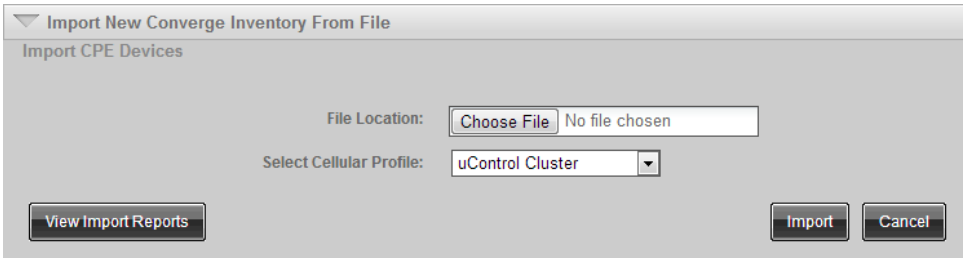
   IMPORTANT: The file size must be less than 2 MB.

2. From the main menu, select **Advanced > Import CPE Devices > Import Touchstone CPE Devices** or **Advanced > Import CPE Devices > Import Converge CPE Devices**.

   If you selected Import Touchstone CPE Devices, the following screen is displayed.



   If you selected Import Converge CPE Devices, the following screen is displayed.



Field	Description
File Location	Click Choose File to navigate to the `.txt` or `.csv` file with the details of CPE devices to be added to inventory.
Select Cellular Profile (Converge Only)	The Cellular Profile the touchscreen will use to connect to the cellular carrier. For more information, see Managing Cellular Profiles (Converge Only) on page 38. **IMPORTANT:** If the wrong profile is selected, the touchscreen will not have cellular service even if the SIM card information is correct.
Select Deployment	Select the deployment to which the added CPE device devices will be assigned. **Note:** This field is only displayed for service providers using deployments.

Field	Description
View Import Reports	Click to access reports generated by importing inventory.

3.4.4 Troubleshooting Import Problems

The `cpe.import.log.directory` (UNIX) and `cpe.import.log.directory.windows` (Windows) server properties specify the absolute root directory that contains the import error log file. The error log records the following:

- Devices that were imported to inventory
- Devices that failed to import
- Why devices failed to import

3.5 Importing SIM Card Data to Inventory (Converge Only)

When touchscreens were added to into inventory, it is possible that the following information is not available:

- SIM card cellular phone number
- Cellular account number

The information can be added to the device information as a batch by importing a comma-delimited file with the data into the Management Portal.

IMPORTANT: Before adding SIM information in a batch, each card's ICC ID must have already been associated to the information details of the touchscreen (see "Batch-Importing CPE Devices to Inventory" on page 60 and "Add a Single CPE to Inventory" on page 57).

3.5.1 Update Server Propterties

The following server property defines the contents and format of the comma-delimited file. The file must be saved as `.txt` or `.csv`.

Property Name	Default Fields
cellular.import.file.format	iccId,phoneNumber,accountNumber

The fields in the property can be changed or reordered by updating the property in the `custom.properties` file. See the *System Operations Guide* for details on updating system properties.

The following table describes the fields that can be listed in the `cellular.import.file.format` property. Field names are case-sensitive and must not be changed if re-ordered.

Field	Description	Required?
iccId	19-digit ICC ID of the SIM card in the touchscreen	Yes

Field	Description	Required?
phoneNumber	10-digit cellular phone number associated with the SIM card.	No
accountNumber	Account number that the cellular service provider associates with the SIM card/phone number.	No

The `cellular.import.log.directory` and `cellular.import.log.directory.windows` properties define the path where the log file(s) for importing SIM card info will be saved. The path can be changed by updating the property in the `custom.properties` file. See the *System Operations Guide* for details on updating system properties.

The log file(s) include the following:

- Devices that were imported to inventory
- Devices that failed to import
- Reason devices failed to import

3.5.2 SIM Card Data Import File Example

The system ignores the first line of the comma-delimited file. The following is a sample file:

```
ICC ID, Phone #, Acct #
8988216710500954195,5126989178,b89bc900b814
9563416094544278985,7125013569,5898353d02ba
7473927493847509857,5123333333,002644f8cc8c
1637485968746205863,4585129648,589835fd3c5c
8234756139573234907,5124569423,0026f300c8ab
```

3.5.3 Import SIM Card Cellular Information to Touchscreens in Inventory

IMPORTANT: Touchscreens that are already activated cannot be updated using this process.

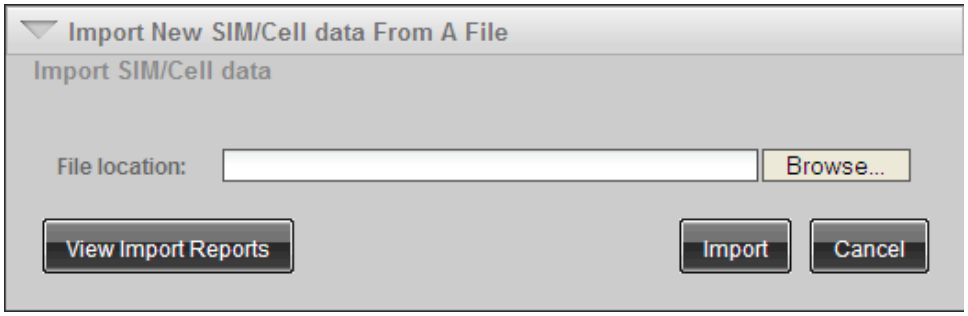
IMPORTANT: The SIM card's ICC ID number must already be included in the touchscreen's information details.

1. Create a comma-delimited file with the information SIM card information. The accepted formats are `.txt` and `.csv`.

   IMPORTANT: The file size must be less than 2 MB.

2. From the main menu, select **Advanced > Import SIM/Cell Data**.

The Import New SIM/Cell data From A File screen is displayed:



3. Click **Browse** navigate to the `.txt` or `.csv` file with the SIM card information.
4. Click **Import**.

   When the file has been uploaded, the system displays the following notice:

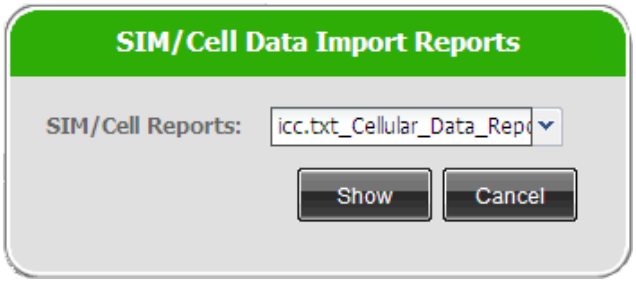
   ```
   [a] SIM/Cell data imported successfully,
   [b] SIM/Cell data failed.
   For detail information, please check the log file:
   icc.txt_Cellular_Data_Report_<timestamp>
   ```

   where:

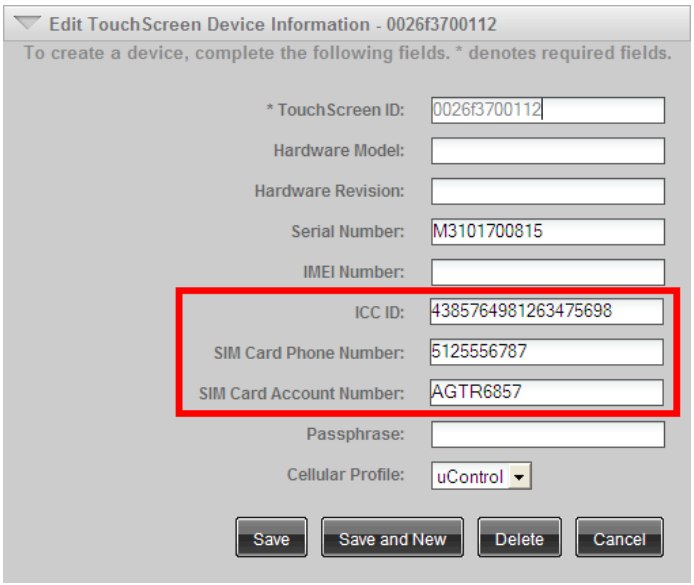
   `a` is the number of SIM cards whose information was uploaded successfully

   `b` is the number of SIM cards whose information was not uploaded successfully

5. Click **View Import Report** to display reports on previous imports.



6. When the SIM card information was uploaded successfully, the Touchscreen Device Information screen for the associated touchscreen is updated.



3.6 Managing Bundles

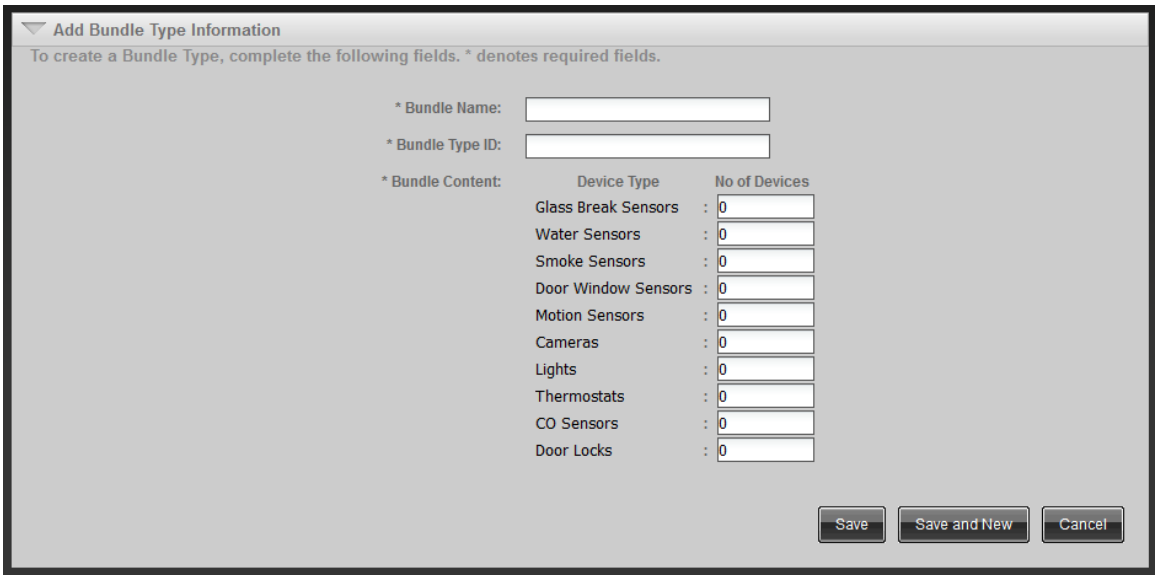
Bundling is a feature available to service providers that are deploying Touchstone on the Hitron gateway and Frictionless Activation via the Mobile App. This feature allows service providers to simplify managing the device packages they offer to their subscribers. By dealing with device packages, or bundle types, the service provider's warehouse can streamline its process by packaging the devices by bundle type, instead of individually. For more information on Touchstone on the Hitron gateway and Frictionless Activation, see: https://share-icontrol.atlassian.net/wiki/display/CSKB/Touchstone+on+a+Gateway

To access the **Advanced > Manage Bundle** menu, the employee must have "Admin", "Bundle Manager", or "Bundle User" privileges. See Management Portal Roles on page 71. Depending on the role, the options displayed are listed below:

- Manage Bundle Types
- Create Bundles
- Import Bundles
- Search Bundles

3.6.1 Create a Bundle Type

1. From the main menu, select **Advanced > Manage Bundle > Manage Bundle Types > Add** to display the "Add Bundle Type Information" screen:



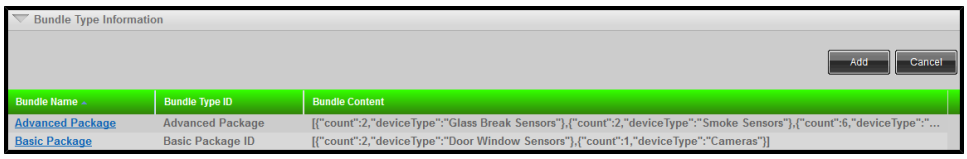
Field	Description
Bundle Name	Unique name for the bundle of devices (required field); maximum 50 characters.
Bundle Type ID	Unique ID for the bundle type (required field); maximum 100 characters.
Bundle Content	The quantity of each device that is included in the bundle type. At least one device is required.

2. Click **Save** when done then **Cancel** to return to the list of bundle types, or click **Save and New** to create another Bundle Type. Clicking **Cancel** will discard all the information entered.

3. The bundle type is now available for creating a bundle.

3.6.2 View all the Bundle Types

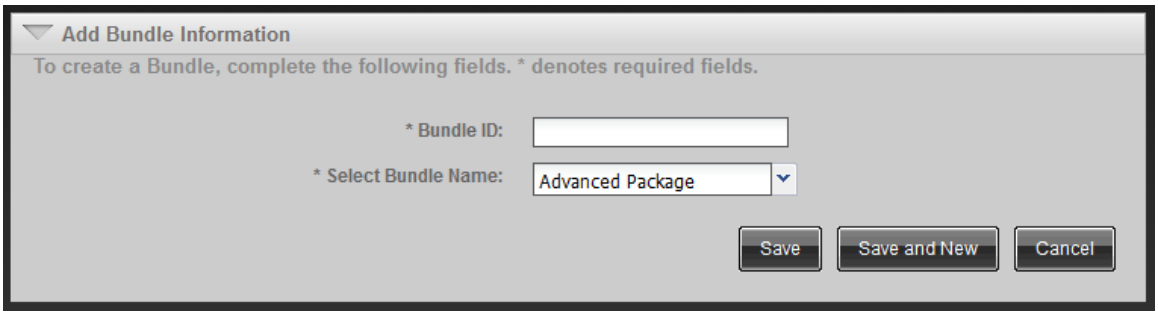
From the main menu, select **Advanced > Manage Bundle > Manage Bundle Types** to display the list of all the Bundle Types. Click on any of the column headers to sort by that column. Click on the Bundle Name to display the details of the Bundle Type. Click **Cancel** to return to the list.



3.6.3 Create a Bundle

A bundle is created when a gateway is associated with the bundle type using a unique bundle ID, usually the gateway ID. Bundles can be created individually or imported in bulk as long as they are of the same Bundle Type.

1. From the main menu, select **Advanced > Manage Bundle > Create Bundles** to display the "Add Bundle Information" screen:



Field	Description
Bundle ID	Unique ID for the bundle, usually the gateway ID (required field)
Select Bundle Name	Select from the list of available Bundle Types (required field)

2. Click **Save** when done then **Cancel** to return to the Dashboard or click **Save and New** to create another bundle. Clicking **Cancel** will discard all the information entered.

   Note: If the bundle ID already exists, it will be overwritten. The following message is displayed:

   ```
   Bundle Overwritten Successfully for Bundle ID:
   "000d6f0005233376". Old Bundle Name: "Basic Package" and
   New Bundle Name: "Advanced Package"
   ```

3.6.4 Import Multiple Bundles

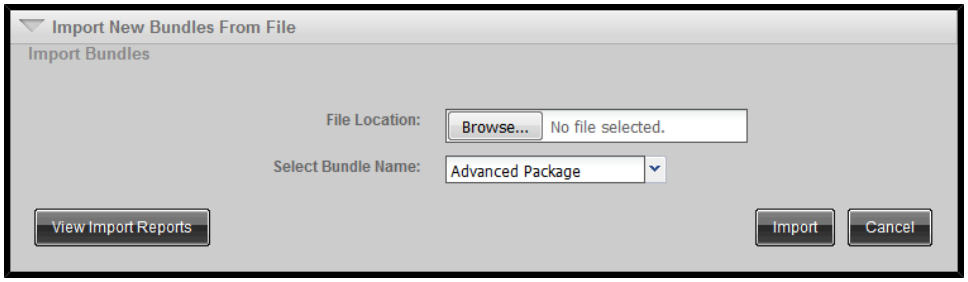
Instead of creating each bundle one at a time, up to 5,000 bundles of the same bundle type can be created in bulk by importing the information via a comma-delimited text file.

1. Create the bundle text file. The bundle IDs should be listed in the format shown below, and the file must be saved as `.txt` or `.csv`. The first line of the file is ignored.

   ```
   Bundle ID
   CPE Bundle ID 1
   CPE Bundle ID 2
   CPE Bundle ID 3
   CPE Bundle ID 4
   ```

   IMPORTANT: The file size must be less than 2 MB.

2. From the main menu, select **Advanced > Manage Bundle > Import Bundles** to display the "Import New Bundles From File" screen:



3. Click on **Browse** to select the text file that contains the bundle IDs, select a Bundle Name from the drop down menu, and click **Import**.

4. Once the import is complete, the import report will be displayed showing:

```
The total number of bundles have been imported successfully :10
The total number of bundles have not been imported : 1
The total number of bundles have been overwritten with new
     bundle type : 0
```

   Any blanks in the text file are ignored and not imported.

   Note: If the bundle ID already exists, it will be overwritten. The following message is displayed in the report:

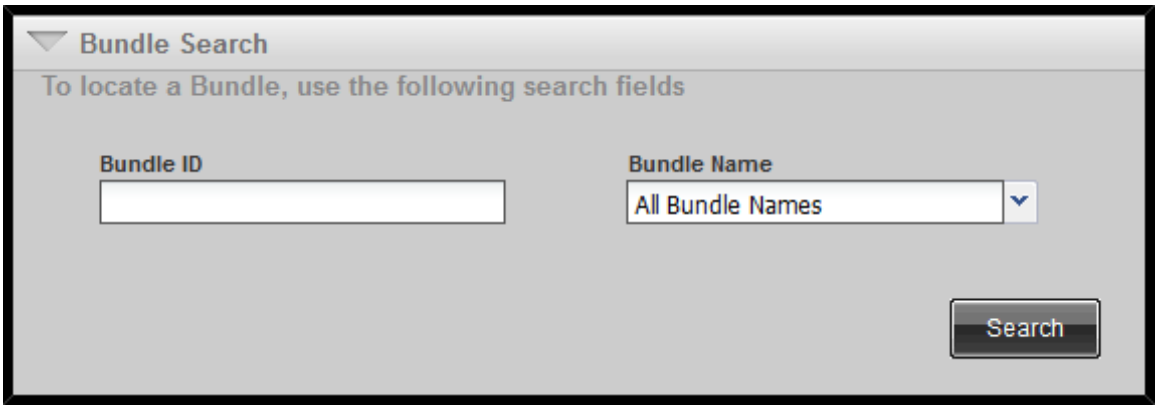
```
Existing Bundle ID: "000d6f0005233376" - Old Bundle
Name: "Basic Package" - New Bundle Name: "Advanced
Package"
```

5. To view the import report from previously imported bundles, click on **View Import Reports** and select the report from the drop down-menu. The report will be displayed in a new browser window.

3.6.5 Search for a Bundle

Searching for a bundle can be done with the bundle ID or bundle name. The search will display the bundle information, but it can not be edited or deleted.

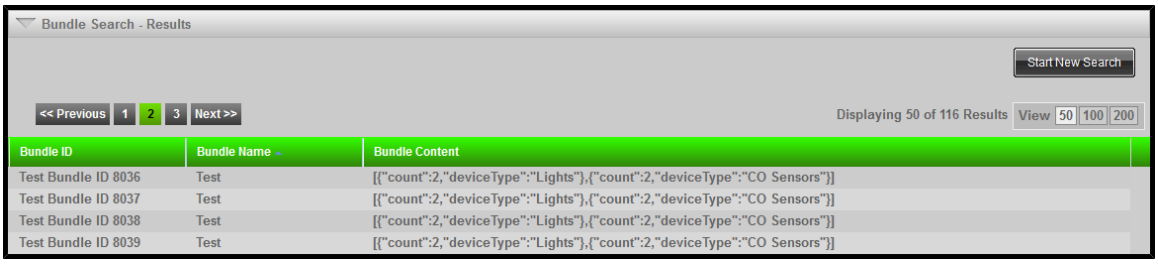
1. From the main menu, select **Advanced > Manage Bundle > Search Bundles** to display the "Bundle Search" screen:



2. Enter the bundle ID and select **All Bundle Names** to search for the ID, regardless of the bundle name.

3. Enter the bundle ID and select a bundle name from the drop-down menu to determine if that ID exists for that bundle name.

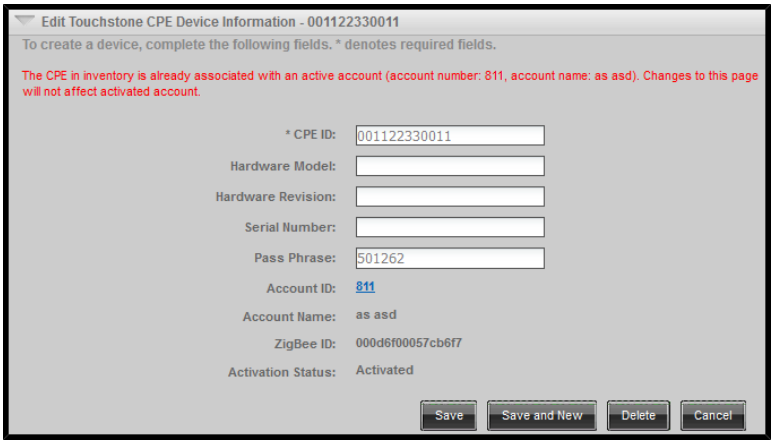
4. Leave the Bundle ID field blank to display all the bundle IDs for the selected bundle name. Click on any of the column headers to sort by that column.



5. Click on the **Start New Search** button to display a pop-up screen to execute another search. The information from the previous search is not retained.

3.6.6 Track External USB ZigBee Radio

To support ZigBee devices, an external USB device (ZigBee dongle) is required, however it is not included in the bundle type or bundle. The ZigBee radio ID of the ZigBee dongle is transmitted to the server and associated with the CPE ID during activation. Navigate to **Inventory > Search for CPE Device** and enter the CPE ID. The CPE Device Information screen is displayed:



Once associated with the CPE, the ZigBee ID is displayed on the CPE Device Information screen. The Activation Status field indicates the current status of the CPE (Unknown, Activating, or Activated).

4 Management Portal Roles

Each user is assigned a role that grants specific rights in the Management Portal. The section describes the rights of each user type. To change the privileges associated with each role, contact your Icontrol representative.

4.1 General Roles

General roles contain multiple privileges that allow an employee to perform defined tasks from the Management Portal. The following roles are defined:

- Admin
- CAT Manager (CM)
- Inventory Manager (IM)

- Tier 1, Tier 2, and Tier 3 Support (T1, T2, T3)
- User Manager (UM)

Action	UM	IM	CM	T1	T2	T3	Admin
Login Access							
Log in to Management Portal	x	x	x	x	x	x	x
User Management							
Create Employee	x						x
Modify Management Portal user	x						x
Delete Management Portal user	x						x
Manage User Managers & Admins (create, modify, delete)							x
Inventory Management							
Search for inventory items		x		x	x	x	x
Add inventory items (CPEs)		x			x	x	x
Modify inventory item details (CPEs)		x			x	x	x
Delete item from inventory (CPEs)		x			x	x	x
Import inventory items (CPEs)		x				x	x
Import SIM card		x					x
Mark customer account for RMA					x	x	x
Managing Bundles and Bundle Types							x
Subscriber Account Management							
Search accounts				x	x	x	x
Create subscriber accounts				x	x	x	x
Update time zone of subscriber account				x	x	x	x
Enable Central Monitoring				x	x	x	x
Disable Central Monitoring						x	x
Change Central Monitoring info						x	x
Access System Status reports on the Account Information Screen, excluding “Advanced Properties” Tab				x	x	x	x
Access “Advanced Properties” on the System Status Tab					x	x	x
Show current active alarm				x	x	x	x
Change Address of Customer Premises					x	x	x
Change Subscriber Username					x	x	x
Change Subscriber Password					x	x	x
Change Customer Email Address					x	x	x

Action	UM	IM	CM	T1	T2	T3	Admin
Reset Account for Activation					x	x	x
Suspend Account					x	x	x
Deactivate Account							x
Delete Unactivated Customer Account						x	x
Delete Any Customer Account							x
Mark an Account as Internal						x	x
Manage Keypad Codes of a Customer							x
Home Domain Management							
View connectivity status				x	x	x	x
View connectivity report				x	x	x	x
Reboot CPE				x	x	x	x
Reboot Router				x	x	x	x
Reboot Camera				x	x	x	x
Adjust Wi-Fi Channel				x	x	x	x
Initiate VNC				x	x	x	x
Start screen capture the touchscreen				x	x	x	x
Get diagnostic files				x	x	x	x
Access Subscriber Portal backdoor				x	x	x	x
Fetch cellular signal strength				x	x	x	x
Reset cellular connection				x	x	x	x
Resend activation email				x	x	x	x
Update individual CPE firmware to latest version				x	x	x	x
Update Individual CPE firmware to any version						x	x
View lighting device information for an account				x	x	x	x
View thermostat information for an account				x	x	x	x
Display the Command History report				x	x	x	x
Display the Quotas report				x	x	x	x
System Management							
Refresh customer connectivity status reports							x
Manage firmware versions						x	x
Batch firmware update							x
Manage Tiers							x
Manage Packages							x

Action	UM	IM	CM	T1	T2	T3	Admin
Manage Tier Properties							x
Manage Touchscreen apps							x
Manage the Central Station							x
Manage log levels							x
Manage deployments							x
Manage cellular profile							x
Manage Device Descriptor List							x
Manage Partners			x				x
Access the Server Status Check List							x
Access the system monitoring service (ICStatusCheck service and the HealthCheck service)							x
Allow access to the Server-To-Server REST API and receive events							x

4.2 Advanced Roles

Advanced roles are primarily used by external processes and services. These roles **do not** have the ability to log in to the Management Portal.

Role	Description
Account Integrator	Access the Server Status Check List
Bundle Manager	Allows the user to create and view Bundle Types, and to create, import, and search Bundles via the Management Portal and REST APIs **Note:** This role can log in to the Management Portal
Bundle User	Allows the user to create, import, and search Bundles **Note:** This role can log in to the Management Portal
Cloud Integration	Allows access to cloud integrations
OAuth Manager	Allows the user to manage the Icontrol OAuth provider, including: ❑ Access the OAuth Management Portal (browser interface) ❑ Add, update, and delete OAuth clients ❑ Revoke OAuth access tokens For more information, see the OAuth Provider Management feature guide on the Icontrol Customer Support Knowledge Base: https://share-icontrol.atlassian.net/wiki/display/CSKB/7.3+Quadra+-+OAuth+Provider+Management

Role	Description
REST Integration	Allows access to cloud integration REST APIs This role also enables the Icontrol OAuth authorization server to notify the Icontrol portal server when an access token has been deleted so that the deleted token is removed from the portal server cache. For more information, see the OAuth Provider Management feature guide on the Icontrol Customer Support Knowledge Base: https://share-icontrol.atlassian.net/wiki/display/CSKB/7.3+Quadra+-+OAuth+Provider+Management
REST MDU	Allows access to multi-dwelling unit (MDU) APIs
REST Operation	Allows access to operational REST APIs
REST Server to Server Integrator	Allow access to the Server-To-Server REST API and receive events
SSH User	Start SSH tunneling (see page 1)
System Monitor	❑ Access the Server Status Check List ❑ Access the system monitoring service (ICStatusCheck service and the HealthCheck service)

5 Managing Employee Details

You can add new Management Portal users, modify their details, or delete them altogether.

- To add a new Management Portal user, see page 76.
- To modify or delete a Management Portal user, see page 77.

To view and modify Management Portal user details:

From the main menu, select **Advanced > Manage Employee**.

The Employee Information screen is displayed. Click on any of the column headers to sort by that column.

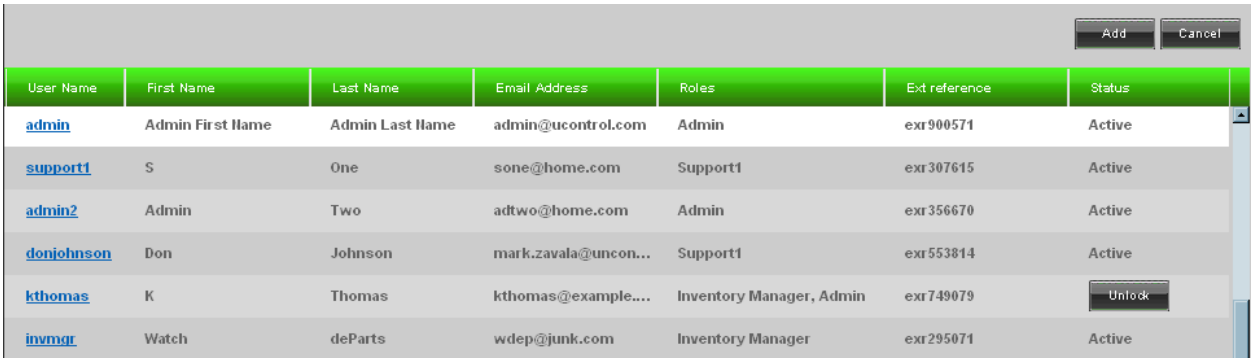


Table 1: Employee Information Screen Columns

Column	Description	
User Name	Username to access the Management Portal.	
First Name	First and last name of the Management Portal user.	
Last Name		
Email Address	Contact email address of the Management Portal user.	
Roles	Management Portal role of the user (see "Management Portal Roles" on page 71)	
Ext Reference	Employee ID of the user.	
Status	Active	Normal status.
	Locked	User cannot login because he or she entered an invalid password the maximum number of times allowed. Click the Unlock button to allow the user to log in.

To add a new user to the system:

From the Employee Information screen, click **Add**.

The Add New Employee Information screen is displayed.

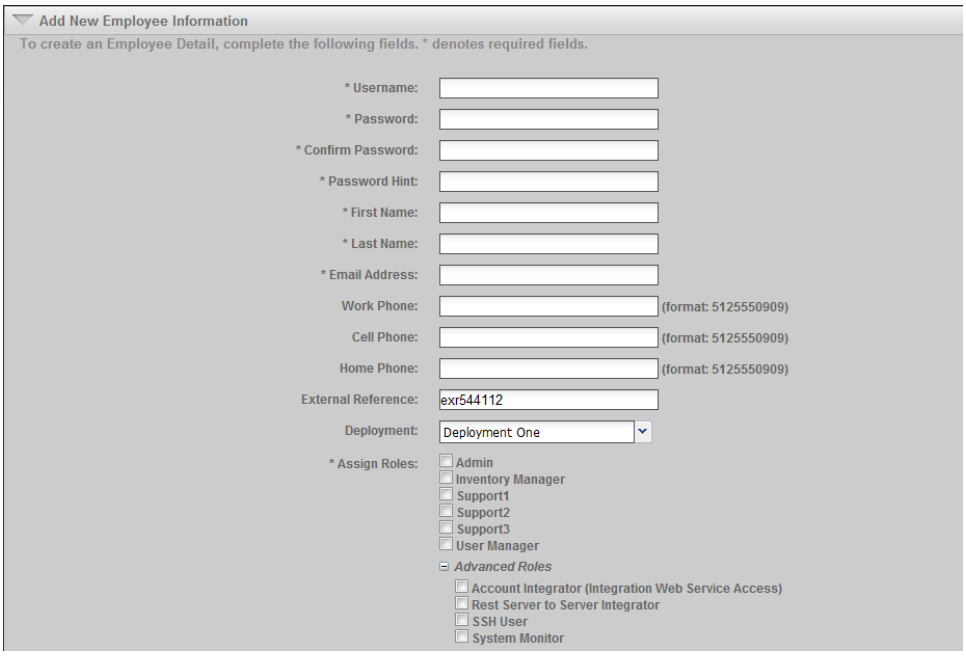


Table 2: Add New Employee Information Fields

Column	Description
User Name	Username to access the Management Portal.
Password	Default password assigned to the new user (to be changed when the user logs in).
Confirm Password	
Password Hint	A hint to remind the user of his password.
First Name	First and last name of the Management Portal user.
Last Name	
Email Address	Contact email address of the Management Portal user.
Work Phone	Contact phone numbers of the Management Portal user.
Cell Phone	
Home Phone	
Ext Reference	Employee ID of the user.
Assign Roles	Select all the Management Portal user roles applicable to the new user (see "Management Portal Roles" on page 71).
Advanced Roles	Click this label to display the Advanced user roles. ❑ Account Integrator - Whether this user can create an account via the account integration web service. ❑ REST Integration - Allows access to cloud integration REST APIs ❑ REST MDU - Allows access to multi-dwelling unit (MDU) APIs ❑ REST Operation - Allows access to operational REST APIs ❑ Rest Server to Server Integrator - Allows access to the REST server-to-server APIs ❑ SSH User - Allows the user to SSH into a CPE device ❑ System Monitor - Whether this user can access the ICHealthCheck or ICStatusCheck summary ❑ Cloud Integration - Allows access to cloud integration APIs **IMPORTANT:** These user roles do not grant login access to the Management Portal.
Save	Click to add the user to the system and return to the Employee Information screen.
Save and New	Click to add the new user and display a new Add New Employee Information screen to add an additional user.
Cancel	Click to return to the Employee Information screen without adding the user.

To modify or delete the details of a Management Portal user:

1. From the Employee Information screen, click the username of the Management Portal user.

   The Edit Employee screen is displayed with the fields empty.

2. Modify the desired details of the Management Portal user, and click **Save** to return to the Employee Information screen.
3. To delete the user, click **Delete**. A confirmation dialog is displayed. Click **Yes** to delete the user.

6 Managing Accounts

6.1 Create a New Account

Adding a new account creates a record in the system database that contains all the supplied information. After the account is added, the subscriber's CPE can be activated. An account must be created as a Converge or Touchstone Account. Once created, it can not be converted to the other.

For Converge accounts, relevant information is also sent to the central monitoring station. If the information changes, the changes are updated at the central monitoring station as well. The central monitoring station will not watch for alarms from the account until it is activated.

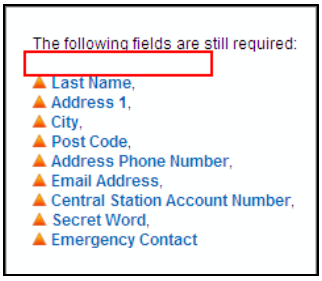
1. Select **Account > Create Touchstone Account** or **Account > Create Converge Account** in the Menu bar.

   The "Add New Touchstone Account Information" or "Add New Converge Account Information" screen is displayed.

2. Enter values for each required field.

   Empty required fields are listed in a heads-up display on the right.

   When a required field is completed, it drops off the list.



   For Converge accounts, a link to the Central Station Integration Log is displayed when the account is created.

Element	Product	Description	Req'd?
Deployment	Both	The deployment of the account. **Note:** Only displayed for systems that use deployments.	Yes, if displayed
Username	Touchstone	The user ID the user will use to log in to the Subscriber Portal. The system generates a random value automatically. This value can be replaced by typing in a new value or by clicking Auto Create.	Yes
First Name	Both	First and last name of the account owner.	Yes
Last Name	Both		Yes
Address Street 1	Both	Street address of the premises location.	Yes
Address Street 2	Both	Additional address information of the premises address, such as apartment number or building name.	No
Address Country	Both	The country in which the account owner resides	Yes
Address State	Both	The state or province location of the premises address.	Yes
Address City	Both	The city location of the premises address.	Yes
Address Postal Code	Both	The postal code/zip code of the premises address.	Yes
Cross Street	Converge	Information about the premises address to aid in locating it.	No
Address Validation Key	Converge	A key used to locate the address location automatically. Note: Only displayed for systems that use Address Validation keys.	No
Address Validation Flag	Converge	Select when the address location has been visibly verified. Note: Only displayed for systems that use Address Validation keys.	No
Address Timezone	Both	Timezone of the address the CPE is located	Yes
CPE Locale	Both	Language of the CPE device.	Yes
Address Phone	Both	Phone number of the premises location.	Yes

Element	Product	Description	Req'd?
Email Address	Both	Contact email of the account.	Yes
Monitored	Converge	Select to have the new account monitored by central monitoring.	No
Central Station Phone Number	Converge	Assigned central monitoring station and its phone number.	N/A
Receiver (Central Station) Account Number	Converge	ID of the account used by the central monitoring station.	Yes, if "Monitored" is checked
Permit Required	Converge	Select if the security system requires a permit for the address.	No
Secret Word	Converge	Default secret word for the account. In most deployments, the secret word can be changed during activation.	Yes
Confirm Secret Word	Converge		
Primary Language	Converge	Primary language of the customer.	No
Special Instructions	Converge	Additional instructions regarding the account for the installers and customer care.	No
Tier	Both	Assigned service Tier of the account.	Yes
Package	Both	The features the customers have access to.	No
External Account Reference	Both	Service provider's ID for the account. This value is automatically entered the field based on the service provider's billing system. When the account is created (the Save button clicked), this value becomes the Account Number.	No
Custom Properties	Both		No

3. For Converge, click **Add Contact** to specify at least 2 emergency contacts.

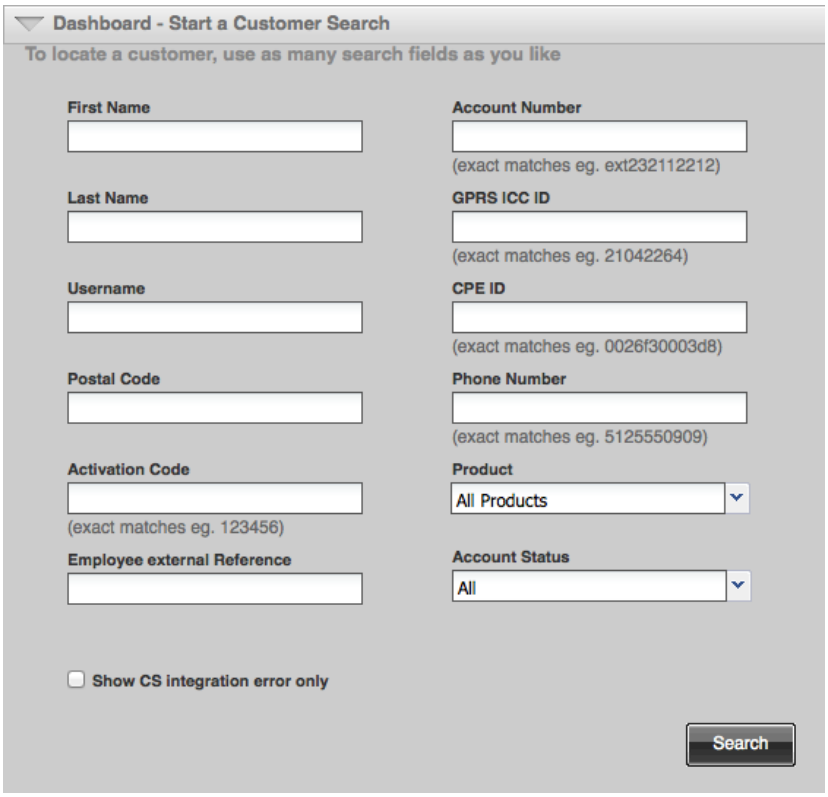
The emergency contacts are the persons that the central monitoring station calls when an alarm event occurs at the account premises to verify that an actual emergency event is occurring. By default, two emergency contacts are required. This number can be changed by editing the server `centralStation.emergencyContact.verify.min` and `centralStation.emergencyContact.verify.max` server properties. If the `emergencyContacts.0` property in the `accountreadonly.properties` file is set to true, then customers will not be able to make any changes to the first contact.

Note: Make sure you list the main contact first. The customer will not be able to change the order of the contact that is listed first.

4. Click **Save** or **Save and New** to add the new account.

6.2 Searching for a Customer Account

To search for a customer account, enter values for one or more fields in the Start a Customer Search area of the Dashboard and click **Search**.



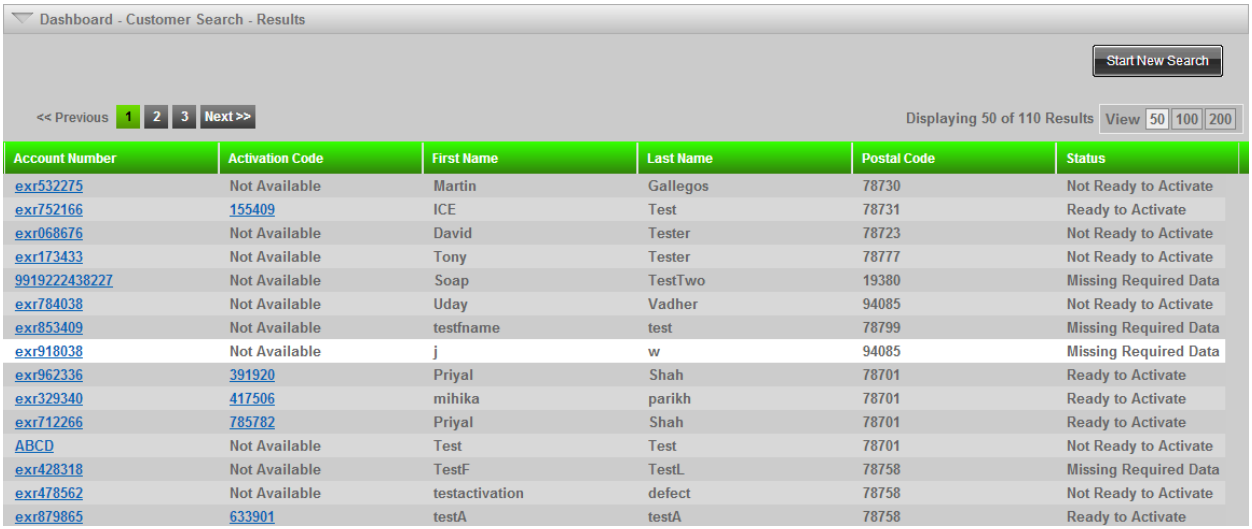
You can search for an account using any of the following fields:

Table 3: Account Search Criteria

Field	Product	Description
First Name	Both	The account holder's first name. The search is not case sensitive and returns all accounts that contain the specified string. For example, entering Ed would return instances of Ed, Edward, and Ted.

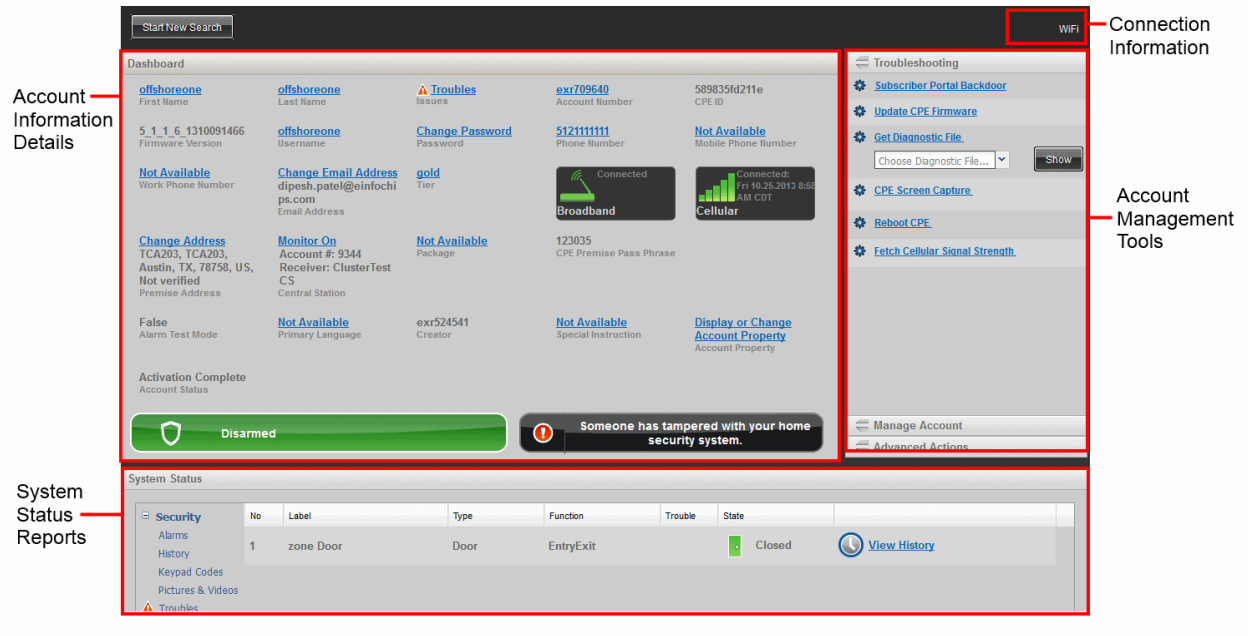
Field	Product	Description
Last Name	Both	The account holder's last name. The search is not case sensitive and returns all accounts that contain the specified string. For example, entering Smith would return instances of Smith and Goldsmith.
Username	Both	The account holder's user ID. The search is not case sensitive and returns all accounts that contain the specified string.
Postal Code	Both	The account holder's postal or zip code. The search is not case sensitive and returns all accounts that contain the specified string.
Activation Code	Both	Assigned by the system. You must specify a full activation code. Partial matches are not returned.
Employee external reference	Both	The creator of the account. The search is not case sensitive and returns all accounts that contain the specified string.
Account Number	Both	Assigned by the system. You must specify a full account number. Partial matches are not returned.
GPRS ICC ID	Converge	Identification number for a SIM card installed in a touchscreen. You must specify a full GPRS ICC ID. Partial matches are not returned.
CPE ID	Both	The ID of the Converge touchscreen or Touchstone Hub. **Note:** Select Inventory > Search for CPE Device to locate CPEs that are not currently assigned to an account.
Phone number	Both	The account holder's phone number. Partial matches are not returned.
Product	Both	Accounts that use Converge systems, Touchstone, or either
Account Status	Both	Activated accounts, only Not Activated accounts, or both
Show CS Integration error only check box	Converge	Search for monitored accounts that received an error from the central station when they tried to integrate the account. This option is only displayed if the following `custom.properties` are set to `true` in your system: - centralStation.integration.enabled - centralStation.integration.synchronous

If the search criteria results with multiple matches, the portal displays the Customer Search Results page. Click on any of the column headers to sort by that column.



Account Number	Activation Code	First Name	Last Name	Postal Code	Status
exr532275	Not Available	Martin	Gallegos	78730	Not Ready to Activate
exr752166	155409	ICE	Test	78731	Ready to Activate
exr068676	Not Available	David	Tester	78723	Not Ready to Activate
exr173433	Not Available	Tony	Tester	78777	Not Ready to Activate
9919222438227	Not Available	Soap	TestTwo	19380	Missing Required Data
exr784038	Not Available	Uday	Vadher	94085	Not Ready to Activate
exr853409	Not Available	testfname	test	78799	Missing Required Data
exr918038	Not Available	j	w	94085	Missing Required Data
exr962336	391920	Priyal	Shah	78701	Ready to Activate
exr329340	417506	mihika	parikh	78701	Ready to Activate
exr712266	785782	Priyal	Shah	78701	Ready to Activate
ABCD	Not Available	Test	Test	78701	Not Ready to Activate
exr428318	Not Available	TestF	TestL	78758	Missing Required Data
exr478562	Not Available	testactivation	defect	78758	Not Ready to Activate
exr879865	633901	testA	testA	78758	Ready to Activate

Click the account number link to display the customer's account information.



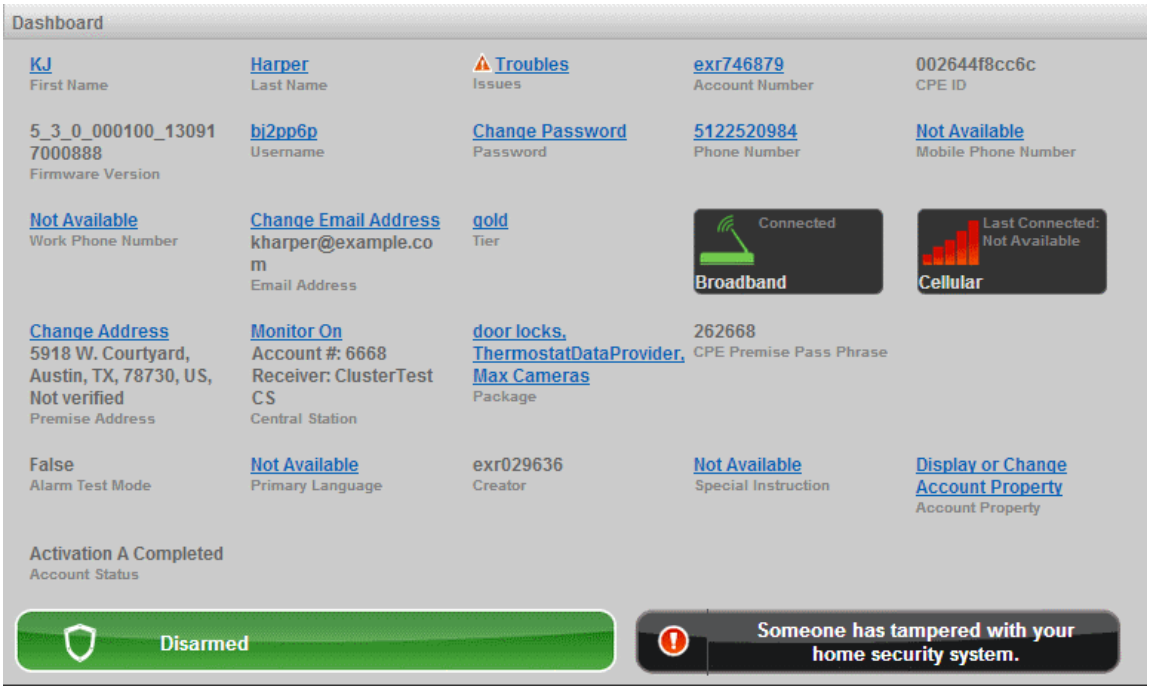
If only one account matches the search criteria, the portal displays the customer's Account Information screen. See the following subsections for more information.

The Account Information Screen contains the following areas:

Section	Description
Account Information Details	Real-time details about the account premises, equipment, zones, and a system access (see page 85).

Section	Description
Connection Info	Home domain configuration: How the touchscreen is connected to the security router and whether there are cameras connected: Wirelessly, by Ethernet, w/ Cameras or w/o Cameras.
Account Management Tools	Menus with various tools for managing and analyzing accounts (see page 87).
System Status Reports	Real-time interactive reports on the current account (see page 122).

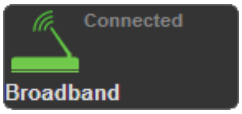
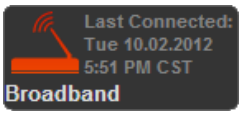
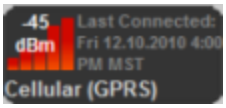
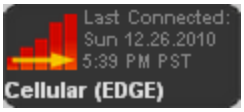
6.2.1 Using the Account Information Details Section



The following table describes the fields on the account information details section of the dashboard. If the account was created from Management Portal, many of these fields can be edited. See Modifying Account Information on page 95 for more information. If the account was created from an external source, the ability to edit these fields is determined in the `accountreadonly.properties` file.

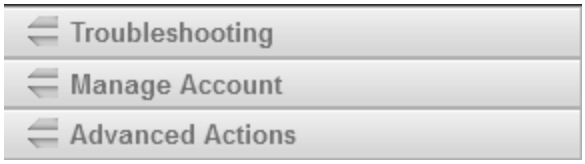
Field	Description
First Name	First and last name of the account owner (click to change).
Last Name	
Issues	See Monitoring the Status of an Account on page 100.
Account Number	Service provider ID for the current account.
CPE ID	Unique ID for the touchscreen for the current account based on the device's MAC address.
Firmware Version	Firmware version currently installed on the account touchscreen.
Username	Username to access the user interface(s) for this account. These values are not used for single sign-on and are displayed as random characters.

Field	Description
Password	Password for the username usedd to access the user interface(s) for this account. This field is not used for single sign-on accounts.
Phone Number	Home phone number for the account owner.
Mobile Phone Number	Mobile phone number for the account owner.
Work Phone Number	Business phone number for the account owner.
Email Address	Email address of the account owner.
Tier	Current tier-level of the account.
Package	Indicates the Package assigned to the account, if any.
Premise Address	Address information for the premises location and whether it has been verified by a technician.
Central Station (Converge only)	Click to toggle central station monitoring. Indicates whether the account is currently being monitored. If it is, then the following information is also displayed: ❑ Account ID assigned by central monitoring station ❑ Central monitoring station name
touchscreen Passphrase (Converge only)	ID required for making certain sensitive changes to the touchscreen. **Note:** The passphrase changes within 24 hours of being used and every 7 days from the last time the touchscreen was rebooted.
Alarm Test Mode (Converge only)	When the value is True, the touchscreen is currently armed in Test mode. Someone is currently testing alarms at the account premises. When the value is False, the touchscreen is not armed in Test mode.
Account Creation Date	Time and date that the account was created.
Primary Language	Language the monitoring station will use for communication.
Creator	Name of representative that added the current account.
Special Instructions	Information about the account added at the time of creation. This information is to be used by the central station. Click to change.
Account Property	Click to manage custom account properties.

Field	Description
Account Status	Current account status: ❑ Activation A Complete (Converge only) ❑ Activation Complete ❑ Suspended ❑ Ready for Activation
Status and Trouble Headers	The current Arming State or Mode of the account. See Monitoring the Status of an Account on page 100 for more information.
Trouble Header	The current Trouble alert displayed on the touchscreen and Subscriber Portal of the account. See Monitoring the Status of an Account on page 100 for more information.
Broadband status  	Current broadband connectivity between the touchscreen and the system servers. See Monitoring the Status of an Account on page 100 for more information.
Cellular status (Converge only)   	Current cellular connectivity between the touchscreen and the system servers. See Monitoring the Status of an Account on page 100 for more information.

6.2.2 Using the Account Management Tools Section

This section of the Account Information screen provides tools for managing the current account. It is divided into three menus:



- ❑ Troubleshooting

Actions used by Customer Care representatives to resolve problems for customers

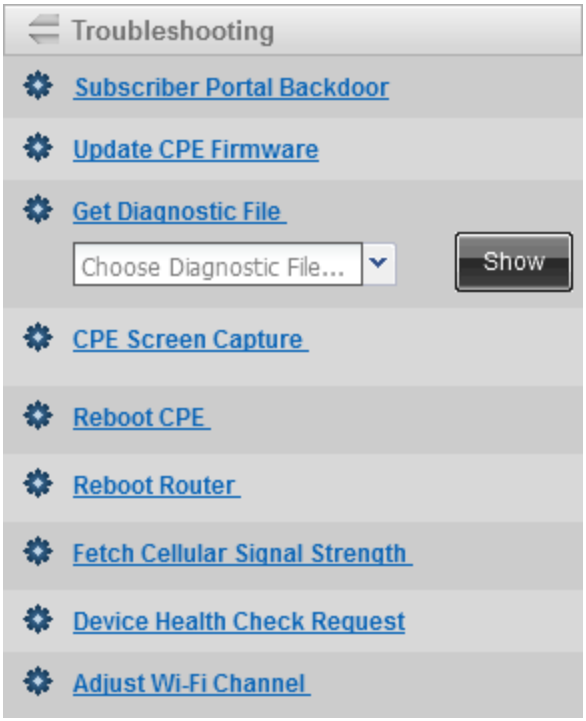
- Manage Account
  Actions related to housekeeping for the current account
- Advanced Actions
  Activities typically performed only by highly privileged users

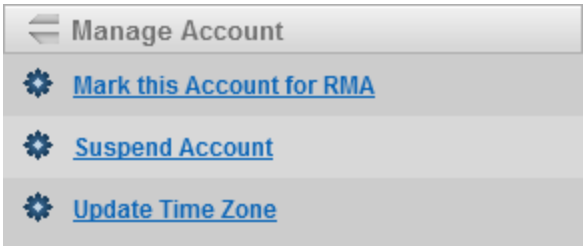
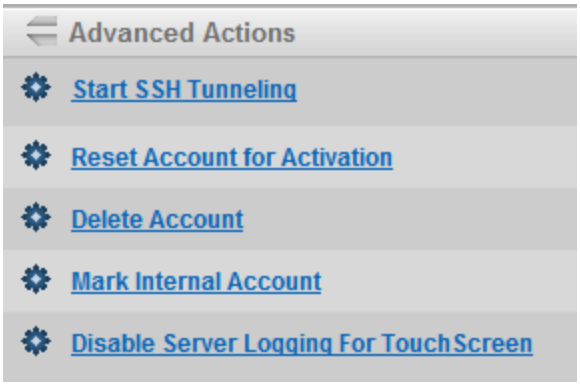
Figure 1: Account Management Tools Section

The available menu options are determined by the current user's permission.

Click  to display each menu's options and hide the other menus.

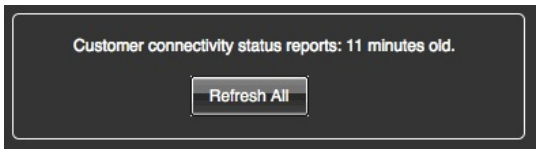
Table 4: Account Management Tools Elements

Menu	Function	Description
	Subscriber Portal Backdoor	Click to access the Subscriber Portal for the current account. This is the view the customer sees. Camera views are not available to users of the Subscriber Portal Backdoor.
	Update CPE Firmware	Click to update the firmware immediately for the current CPE device with the latest available version.
	Get Diagnostic File	Click to display the diagnostic file from the CPE of the account.
	CPE Screen Capture (Converge only)	Click to take a screenshot of the current view on the touchscreen for the account and display it. Use the menu to view previous captured screenshots.
	Reboot CPE	Remotely reboot the account's CPE device. **IMPORTANT:** Do not reboot the CPE if the CPE is armed.
	Reboot Router	Remotely reboot the account's security router.
	Fetch Cellular Signal Strength (Converge only)	Click to display the strength of the cellular signal.
	Device Health Check Request	Click to request the network health status of the devices paired to the CPE. This information should be used to detect device issues, such as connectivity.
	Adjust Wi-Fi Channel	Click to display, scan and switch the Wi-Fi channel for a security router or Touchstone hub.

Menu	Function	Description
	Mark this Account for RMA	Click to allow the account's touchscreen or hub to be replaced. Touchscreens and hubs of RMA accounts can be swapped for new ones without affecting the account's current configuration.
	Suspend Account	Click to place the account in Suspended state. Suspended accounts do not have access to the Subscriber Portal and they do not report events.
	Update Time Zone	Click to change the time zone for the account.
	Start SSH Tunneling	Click to open an SSH tunnel into the touchscreen device of the account.
	Reset Account for Activation	Click to set account to Ready for Activation state to allow the touchscreen to reset to factory default and repeat the activation process. This option is most frequently used for demonstrations.
	Delete Account	Click to delete all account information and history from the databases. IMPORTANT: Not the same as Suspend account.
	Mark Internal Account	Internal accounts do not appear on general service reports or queries (such as Connectivity (online/offline). Internal accounts are typically used for demos and testing.
	Enable/Disable Server Logging For CPE	Click to enable or disable server logging for this CPE device. Communication between the server and the touchscreen will be logged in the server log files.

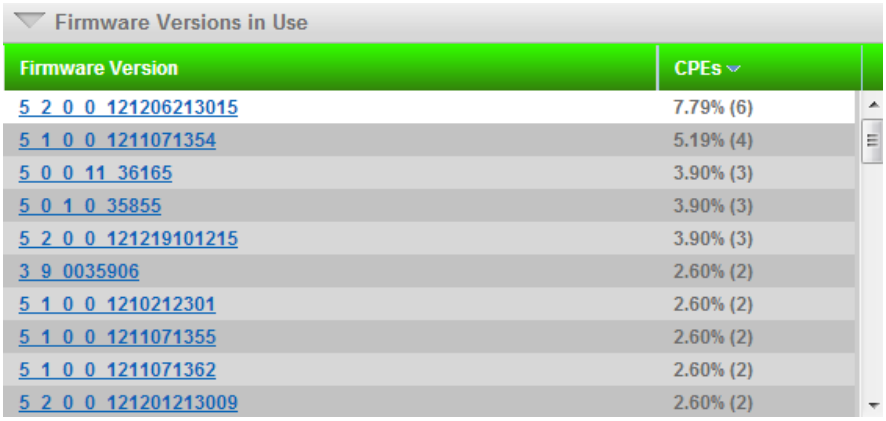
6.3 Querying Accounts

Account reports based on device firmware build and connectivity status can be run from the Dashboard. The information displayed is a snapshot of a query that is run in the background every 10 minutes. For up-to-date reports, an admin user can refresh the reports by clicking on the **Refresh All** button at the bottom of the screen.



6.3.1 Querying Devices based on Firmware Version

The Firmware Versions in Use report lists the versions of the CPE firmware that are in use. It also provides the percentage and actual number of CPEs that use each of firmware version. Click on the column header to sort by that column.



6.3.2 Querying Accounts Based on Connectivity Status

From the Dashboard, you can perform a quick query of all accounts based on their current connectivity status only. You can also perform a granulated query of accounts based on their connectivity status and geographic information such as the premise city or postal code.

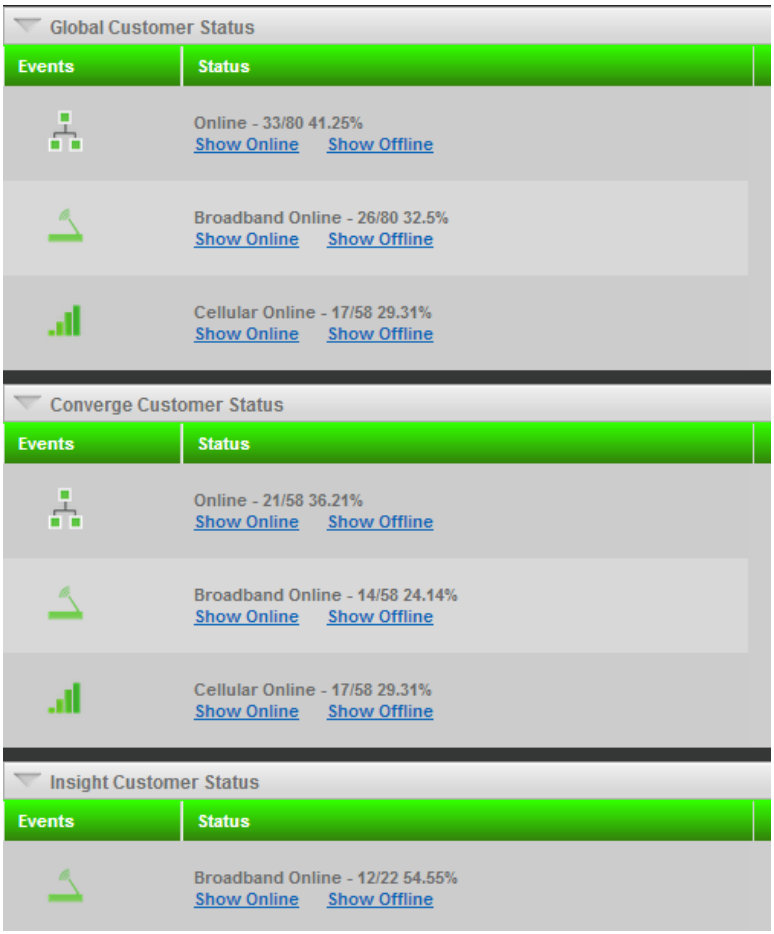
6.3.2.1 Performing a Quick Query

A Quick Query searches all accounts based on their current connectivity status such as, being online/offline on both broadband and cellular, online/offline on broadband, and being online/offline on cellular.

To Quick Search for accounts based on connectivity status:

1. Click Dashboard in the Menu bar to display the Dashboard.

   The Global Customer Status, Converge Customer Status, and Touchstone Customer Status are displayed in the Dashboard.



   The Status column displays a connectivity summary for online on both channels, broadband only, and cellular only in the format a/b c% where:

   a is the number of accounts that are online

   b is the total number of accounts

   c is the percentage of accounts that are online

2. Click a link in the Status column (see Global Customer Status Tool Options) to generate a quick report.

Table 5: Global Customer Status Tool Options

Events		Status	
	Overall Connectivity	Show Online	Click to list all accounts that are communicating to the servers via broadband and cellular.
		Show Offline	Click to list all accounts that are not communicating with servers.
	Broadband Connectivity	Show Online	Click to list all accounts that are communicating with the servers over broadband.
		Show Offline	Click to list all accounts that are not communicating with the servers over broadband.
	Cellular Connectivity (Converge Only)	Show Online	Click to list all accounts that are communicating with the servers over cellular.
		Show Offline	Click to list all accounts that are not communicating with the servers over cellular.

3. The Connectivity Customer Search Results screen is displayed. Click on the column header to sort by that column.

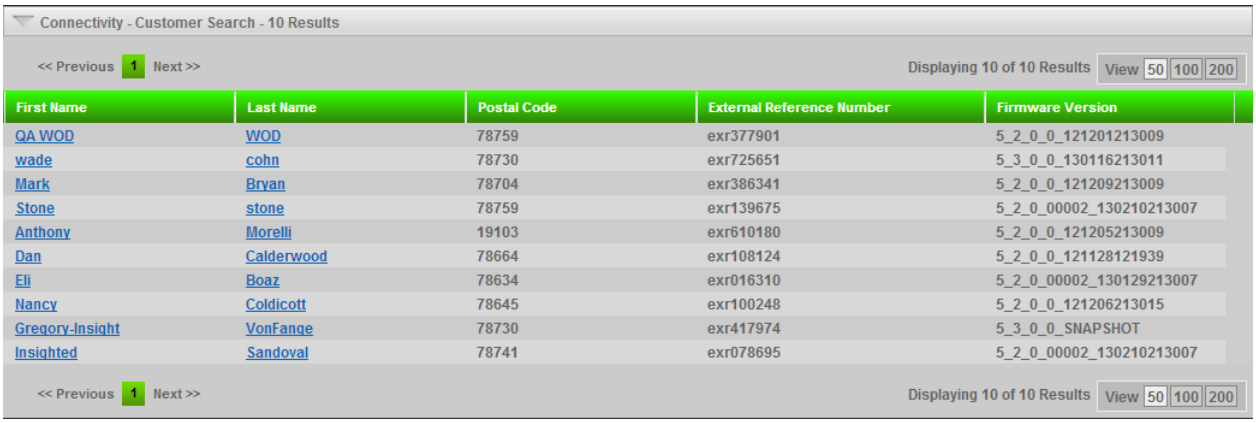


Table 6: Connectivity Customer Search Results Screen Elements

Element	Description
First Name Last Name	The first and last name of the owner of the account. Click to go to the Account Information screen of the account.
Postal Code	The postal code/zip code of the location of the account premises.
External Reference Number	Service Provider's reference ID for the account.
Firmware Version	The firmware version installed on the customer's CPE.

6.3.2.2 Performing a Granulated Query

Whereas a Quick Query searches all accounts, a Granulated Query accepts more information that can be used to filter the results.

To perform a granulated query for accounts based on connectivity status:

1. On the top menu bar on the Management Portal, click **Connectivity > Connectivity Search**.

   The Connectivity Search tool is displayed.

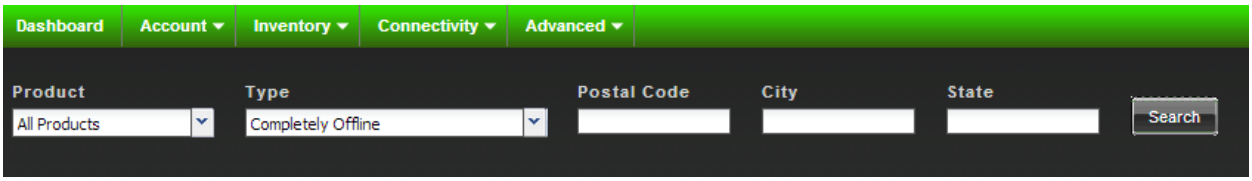


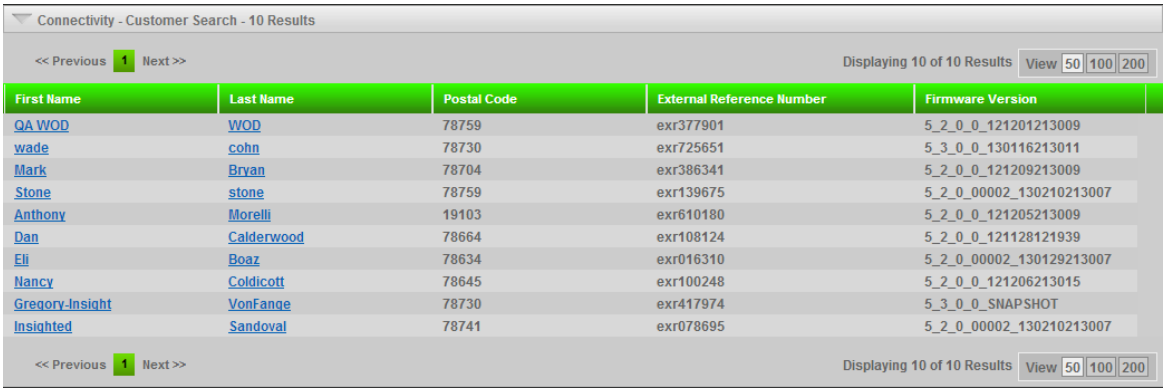
Table 7: Connectivity Search Tool Elements

Element	Description
Product	Select Converge, Touchstone, or All Products
Type	Select one of the following: ❑ Any Channel Online ❑ Both Channels Online ❑ Broadband Offline ❑ Broadband Online ❑ Broadband Offline and Cellular Online ❑ Broadband Online and Cellular Offline ❑ Cellular Offline ❑ Cellular Online ❑ Completely Offline
Postal Code	Postal code/zip code of the account premises.
City	City of the account premises.
State	The two-letter abbreviation of the state or province of the account premises.

2. Enter all the desired search criteria and click Search.

   The Connectivity Customer Search Results screen is displayed. Click on the column header to sort

by that column.



6.4 Modifying Account Information for Activated Accounts

Any recorded information can be modified before an account is activated. After activation, only specific information can be modified from the Management Portal.

On Converge TouchScreens, some information, such as the Master keypad code, can be modified only for activated accounts because the information did not exist prior to activation.

6.4.1 Modifying Account Information

The following fields can be edited from the account dashboard by clicking on the link. A pop-up window will be displayed for entering the new information and will close after clicking **Save** or **Cancel**. The system will send an email to the subscriber when the first name, last name, username, password, email address, or any phone number is changed.

Note: If the account was created from an external source, the ability to edit these fields is determined in the `accountreadonly.properties` file.

Table 8: Editable Account Information

Converge	Touchstone
First name	First name
Last name	Last name
Account number	Account number
User name	User name
Password	Password
Primary phone number	Primary phone number
Cellular phone number	Mobile phone number
Work phone number	Work phone number
Email address	Email address
Tier	Tier
Package	Package
Address	Address
Monitoring on/off	Packages
Packages	Primary language
Primary language	Special instructions
Special instructions	Display or change account property
Display or change account property	

Changing the Account Username

The username for the account must be 20 characters or less and can contain numbers (0-9), English uppercase and lowercase letters (a-z, A-Z), as well as the following non-English characters:

Ä, ä, É, é, Ö, ö, Ü, ü, ß, À, à, Â, â, Æ, æ, Ç, ç, È, è, Ê, ê, Ë, ë, Î, î, Ï, ï, Ô, ô, Œ, œ, Ù, ù, Û, û, Í, í, Ò, ò, Ó, ó, Ú, ú, Ñ, ñ, ¿, ¡

The following special characters are also supported:

! . # $ % ' * + - ? ^ _ ` { | } & / = ~

Spaces cannot be used in a username, and usernames are not case-sensitive.

Changing the Account Password

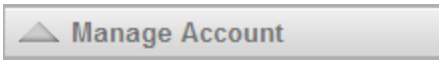
The account password must be 20 characters or less and can contain any character, and passwords are case-sensitive.

6.4.2 Modifying an Account Time Zone

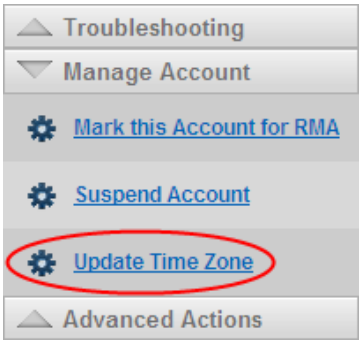
You can change the time zone for an account's premises location.

To change the time zone for an account:

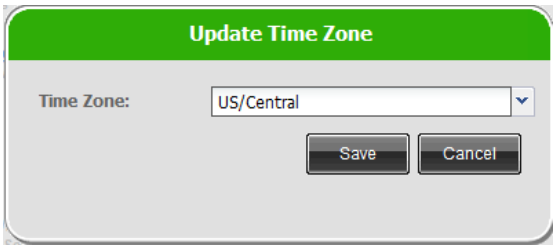
1. From the Management Portal, access the Account Information screen of a customer account.
2. Click the **Manage Account** menu in the Account Management tools.



3. Click **Update Time Zone**.



The Update Time Zone dialog is displayed.



4. Select a time zone from the menu.
5. Click **Save**.

The Account Information screen refreshes to update references to the time zone.

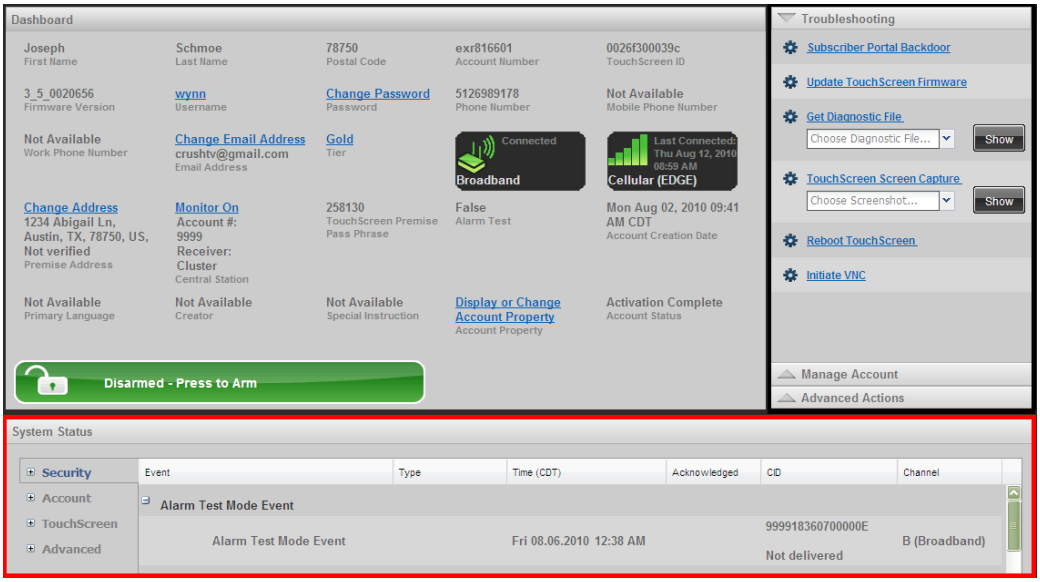
6.4.3 Modifying the Master Keypad Code for a Converge Account

This value can be changed for accounts that have completed Activation A. Only the Master keypad code can be modified from Management Portal. You must have Admin privileges to change a keypad code.

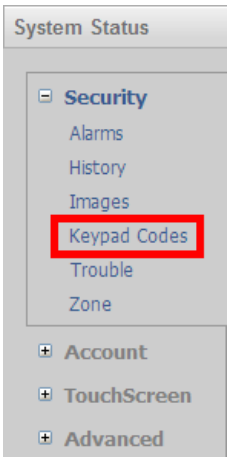
To change the master keypad code of an activated account:

1. Query for an Activated account as described on page 100.

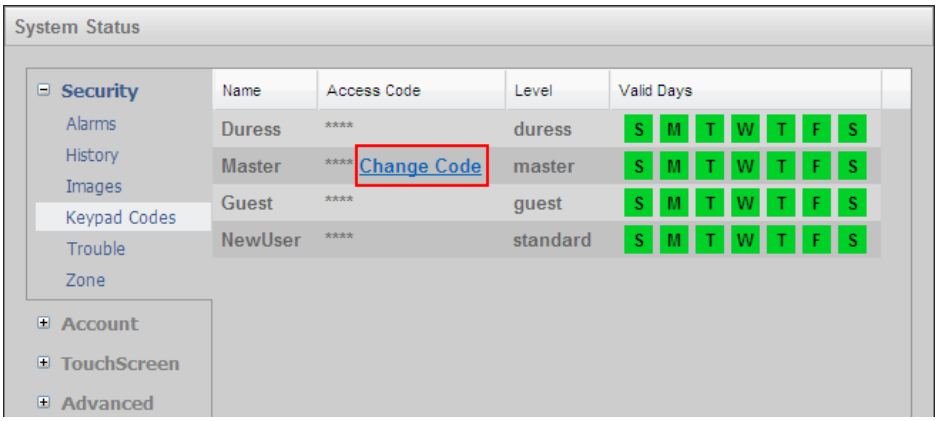
   The Account Information screen is displayed (see "Searching for a Customer Account" on page 82 for information about this screen).



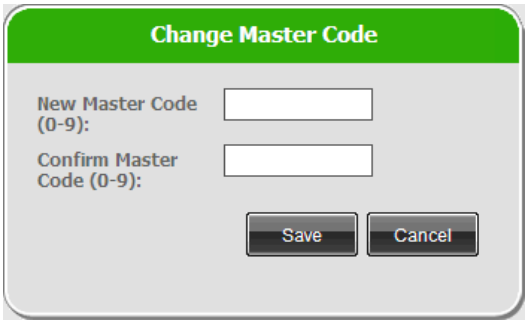
2. In the System Status Reports section, click **Keypad Codes** in the Security group.



3. Click **Change Code** next to the Master Access Code.



The Change Master Code dialog is displayed.



4. Enter the new four-digit number in the New Master Code and Confirm Master Code fields.
5. Click **Save** to modify the Master keypad code.

6.5 Modifying Account Information for Unactivated Accounts

When you search for an account that has not completed the activation process, the Management Portal displays the Edit Account Information screen. This screen is the same as the Add New Account Information screen with the following additions:

Table 9: Edit Account Information Screen Options

Element	Description	Reqd?
Account Number	Service provider ID for the account. This value is the External Account Reference prior to Activation.	Cannot be modified
Activation Status	Select All required fields filled, not ready for activation or Ready for activation.	Yes

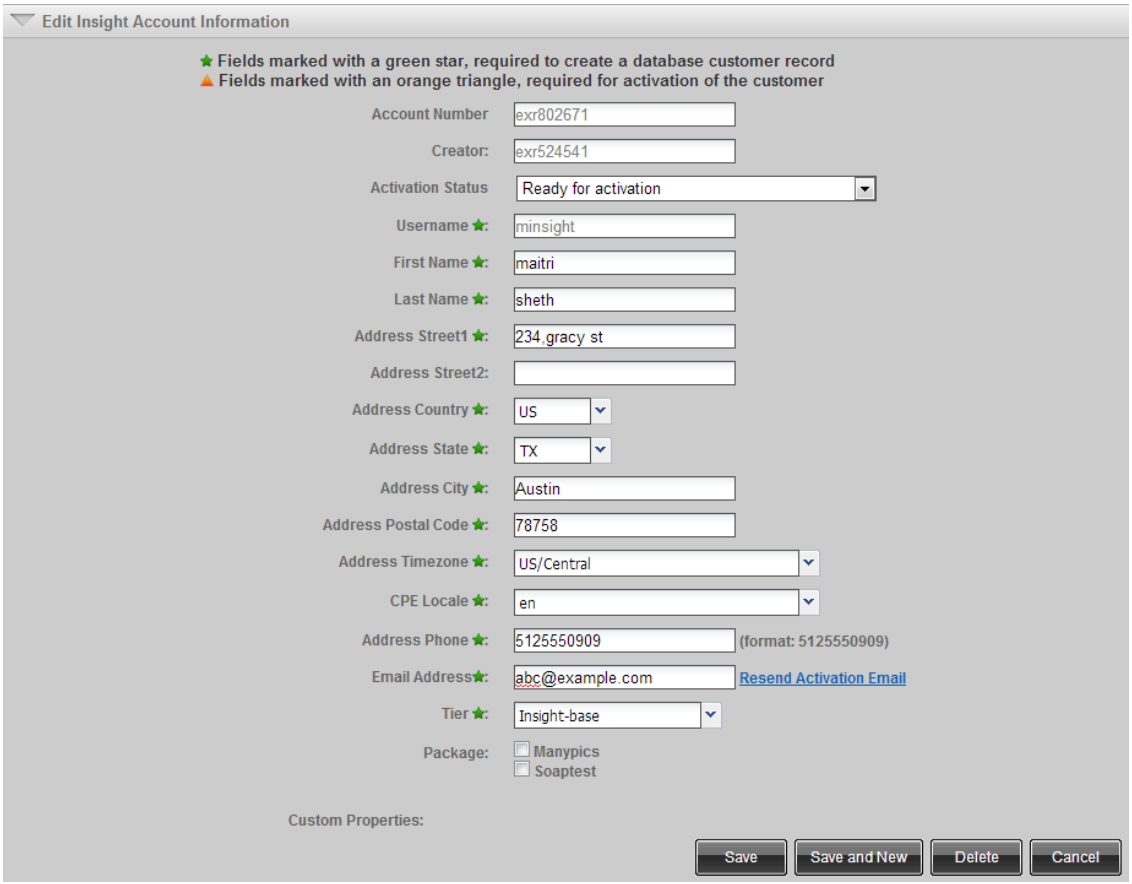


Figure 2: Edit Account Information Screen

See "Create a New Account" on page 79 for more information about the fields on the Edit Account Information screen.

6.6 Monitoring the Status of an Account

The dashboard view of an account provides important information about the account's status.

6.7 Converge Accounts

The dashboard view of a Converge account contains five areas that allow you to determine the status of the account.

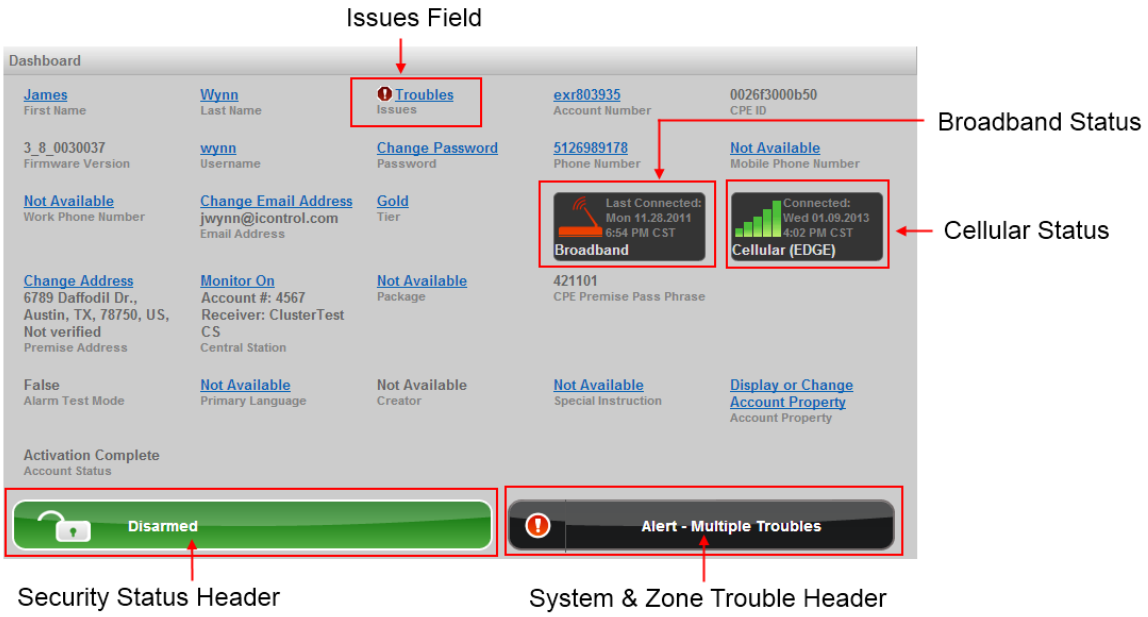
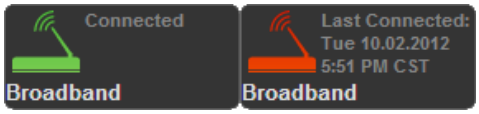
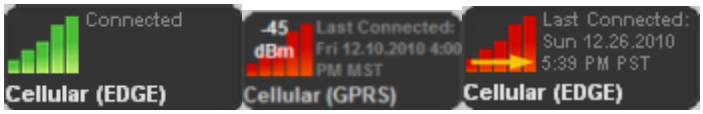


Table 10: Elements of the Converge Account Information Details Section

Area	Description
Issues field	Displays a warning icon and link if there are potential problems in the Troubles and Quotas tabs below the Dashboard.  Click the link to display a report that contains more information. If there are no issues, then the word None is displayed.
Security Status Header	The security status header indicates whether the touchscreen is armed, disarmed, or is in a state that the security system cannot be armed. (For example, a door could be open.) The touchscreen, browser interface, and mobile app also display the security status header. See *Converge User Guide* for more information.
System & Zone Trouble Header	The System & Zone Trouble only displays when there is a connectivity (cellular, broadband, etc.) or power problem with the touchscreen, when a sensor goes down (such as due to a battery failure), or a sensor is being tampered with (such as the cover being opened). The touchscreen, browser interface, and mobile app also display the security status header. See *Converge User Guide* for more information.
Broadband Status	Current broadband connectivity between the touchscreen and the system servers. If not connected by broadband (red), the last connected time/date is displayed. 

Area	Description
Cellular Status	Current cellular connectivity between the touchscreen and the system servers. In addition, the GSM version used by the touchscreen is displayed (GPRS or EDGE) based on the touchscreen's last connection. The last connected time/date is displayed, and if the cellular connection is down, the signal strength is displayed. If the signal strength is not known, then one of the following values will be displayed: ❑ NA-TS touchscreen could not determine the signal strength. ❑ NA-BB Signal strength could not be sent because the touchscreen is completely off-line. If the connectivity icon is red with an arrow through it, the connection is down in one direction. The touchscreen is able to send a cellular heartbeat, but it appears that the touchscreen is unable to receive an acknowledgment.  The Management Portal reports Cellular Down for the following reasons. 1. When the touchscreen is connected over broadband and detects that it lost the cellular PPP connection: ❑ The touchscreen sends a Cellular Down connectivity event over the broadband channel. This can happen if the cell tower kicks off the touchscreen's cellular modem. ❑ The touchscreen tries to re-establish a PPP IP Address every minute up to 5 minutes, then 15, 30, and 60 as per defined by the AT&T certification document. 2. The server reports a missed cellular heartbeat. 3. The server failed to send a Broadband Down message to the touchscreen more than the number of times defined by the server property: broadbandDownCellularMsg.max.try. When the touchscreen is in Low Power Mode (no A/C power), it disconnects broadband connections and sends alerts for alarm events over cellular. It stops sending heartbeats over cellular. The touchscreen tries to send an AC Power Loss message to the system servers over cellular (if connectivity is available). If the system servers receive the message, no Connectivity Loss trouble messages are displayed in the Account Information screen for as long as Low Power Mode continues. Instead, an AC Power Loss trouble is displayed.

Area	Description
	The Account Information screen might eventually show a Loss of Connectivity trouble instead of an AC Power Loss trouble if the AC Power Loss message was not received for some reason. Any non-alarm, non-arm/disarm events are recorded by the touchscreen but will never be forwarded to the system servers even after Low Power Mode ends. See *Converge User Guide* for more information regarding Low Power Mode.

6.7.1 Low Power Mode

During Low Power Mode, when the touchscreen has lost A/C Power, the touchscreen drops broadband connectivity and stops sending heartbeats over cellular. At this time, the touchscreen tries to send an AC Power Loss message to the system servers over cellular (if connectivity is available). If the system servers receive the message, no Connectivity Loss trouble messages are displayed in the Account Information screen for as long as Low Power Mode continues. Instead, an AC Power Loss trouble is displayed.

Note: The Account Information screen might eventually report a loss of broadband and cellular connectivity instead of an AC Power Loss trouble if the AC Power Loss message was not received for some reason.

6.8 Touchstone Accounts

The dashboard view of an Touchstone account contains four areas that allow you to determine the status of the account.

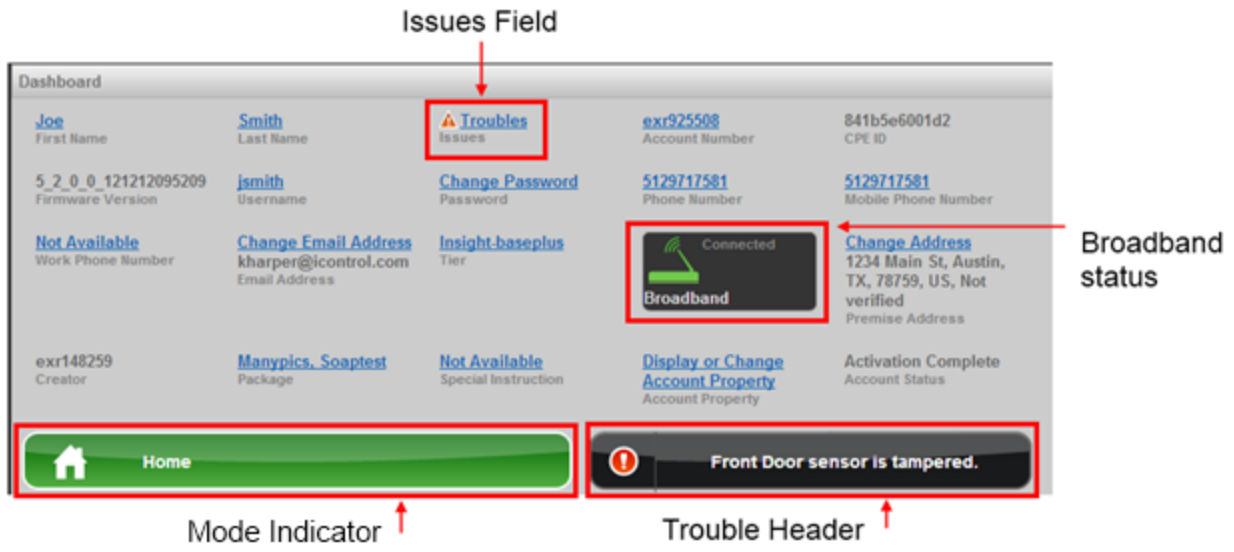


Table 11: Elements of the Touchstone Account Information Details Section

Area	Description
Issues field	Displays a warning icon and link if there are potential problems in the Troubles and Quotas tabs below the Dashboard.  Click the link to display a report that contains more information. If there are no issues, then the word None is displayed.
Broadband Status	Current broadband connectivity between the CPE and the system servers. If not connected by broadband (red), the last connected time/date is displayed. 
Mode Indicator	Specifies the current Touchstone mode. Possible values are: ❑ Home ❑ Away ❑ Night ❑ Vacation
Trouble Header	The System & Zone Trouble only displays when there is a connectivity or power problem with the Hub, when a sensor goes down (such as due to a battery failure), or a sensor is being tampered with (such as the cover being opened). The Subscriber Portal also displays the security status header.

7 General Operations

This section describes how to perform the following general operations for accounts:

- Place an account in suspended state (see page 105)
- Reset an account to allow it to be activated again (see page 109)
- Delete an account entirely from the database (see page 104)
- Resend an activation email (see page 108)
- Reset an account for activation (see page 109)
- Mark an account as internal (see page 110)

7.1 Suspending/Restoring an Account

Only accounts that have completed the Activation A can be suspended.

When an account is suspended:

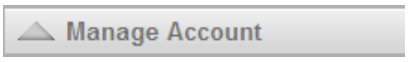
- All broadband (and cellular, if applicable) connectivity between the CPE and system server is disconnected.
- Events and alarms are not forwarded to the system servers
- CPE configuration changes are not sent to the system servers
- Account is not included in global connectivity reports. For example connectivity stats on the Dashboard will not include suspended accounts and queries based on connectivity will not include suspended accounts (see "Understanding the Dashboard" on page 12 and "Monitoring the Status of an Account" on page 100)
- Account is still included in queries for activated accounts
- Account is not included in firmware updates
- Touchscreen apps can not be added or updated
- Subscriber does not have access to the Subscriber Portal

To suspend an account:

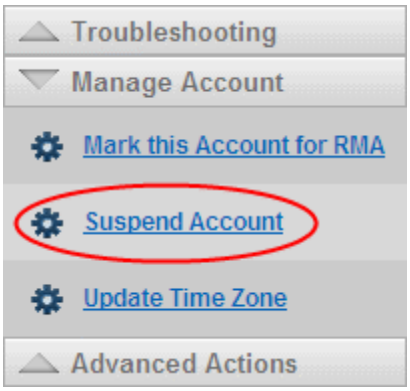
1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

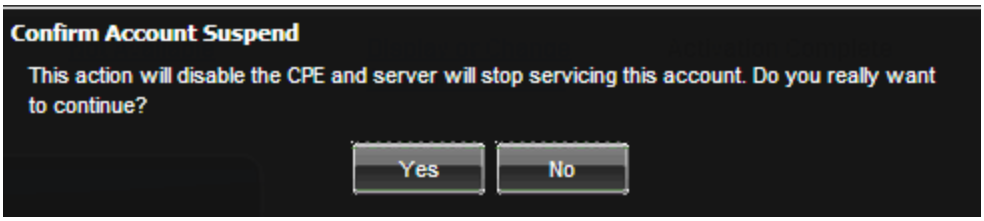
2. Open the **Manage Account** menu in the Account Management tools.

3. Click **Suspend Account**.

   A warning message is displayed.



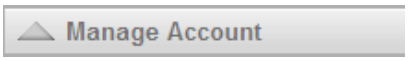
After the account is suspended, the CPE is instructed to stop communicating with the system servers. The loss of communication is not reflected in the Account Information screen until the servers miss the broadband heartbeat and (then likely later) the cellular heartbeat (for Converge accounts).

To restore a suspended account:

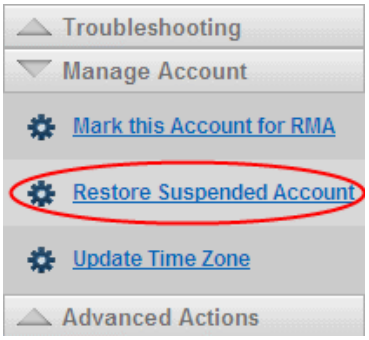
1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

2. Open the **Manage Account** menu in the Account Management tools.

3. Click **Restore Suspended Account**.

   The link changes to Suspend Account, and the account is restored.

4. Have the customer restart the CPE. Converge customers can use the Settings app on the touchscreen to access the **Advanced Settings > Reboot touchscreen** option, and restart the touchscreen to reconnect to the system servers.

7.2 Deleting an Account

A deleted account's details are not removed from the system servers. When an account is deleted:

- Account is NOT included in queries for activated or not activated accounts
- Account is not included in global connectivity reports. For example connectivity stats on the Dashboard will not include deleted accounts and queries based on connectivity will not include suspended accounts

Note: See "Understanding the Dashboard" on page 12 and "Monitoring the Status of an Account" on page 100.

- All broadband and cellular connectivity between the CPE and system server is disconnected.
- Events and alarms are not forwarded to the system servers
- CPE configuration changes are not sent to the system servers
- Account is not included in firmware updates
- Touchscreen apps can not be added or updated
- Customer does not have access to the Subscriber Portal

IMPORTANT: This operation is performed only when an end-user cancels his subscription. More often, an account needs to be merely reset for activation (see page 109) or suspended (see page 105).

To delete an account that has not been activated:

1. Query for a Not Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Edit Account Information screen is displayed.

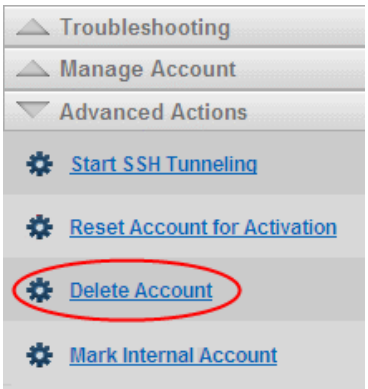
2. Click **Delete** to remove the account.

To delete an activated account:

1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed (see "Using the Account Information Details Section" on page 85 for information about this screen).

2. From the Advanced Actions menu, click **Delete Account** to remove the account.



7.2.1 Resending the Activation Email to the Customer (Converge Only)

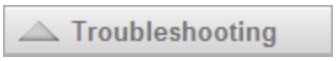
After Activation A, the system sends an email to the account email address with a link to the Subscriber Portal and initial login information (username/password). The login information will work for 14 days. If the customer does not login to the Subscriber Portal in 14 days or if the email does not arrive for some reason, a Management Portal user can reissue the Activation email.

To resend the Activation email:

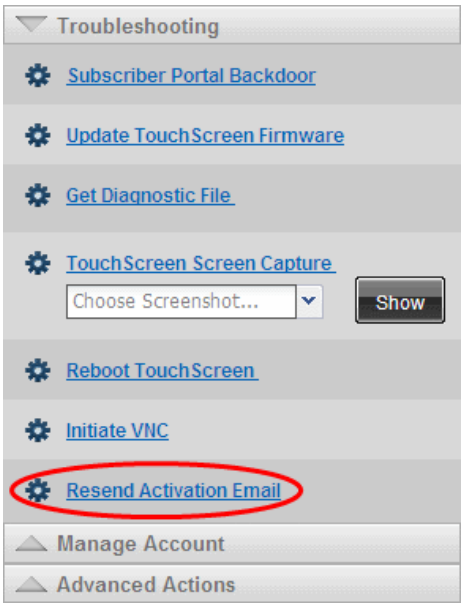
1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

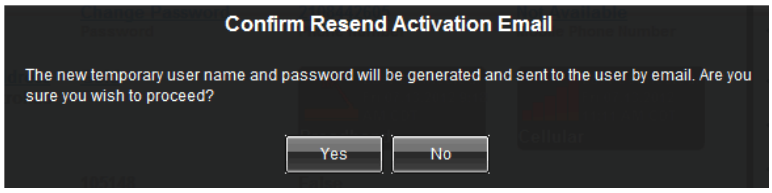
2. Click **Troubleshooting** in the Account Management tools.



3. Click **Resend Activation Email**.



   The Management Portal displays a confirmation for whether you actually want to perform this procedure.



4. Click **Yes** to resend the Activation email.

7.2.2 Resetting an Account for Activation

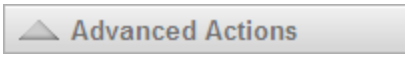
Use this procedure when the activation process must be performed on an activated account. Resetting an account for activation deletes all the CPE configuration information, and places the account in Ready for Activation status.

IMPORTANT: This is not the procedure for customers that need to replace a CPE with a new one. For that, "Marking an Account for RMA" on page 172.

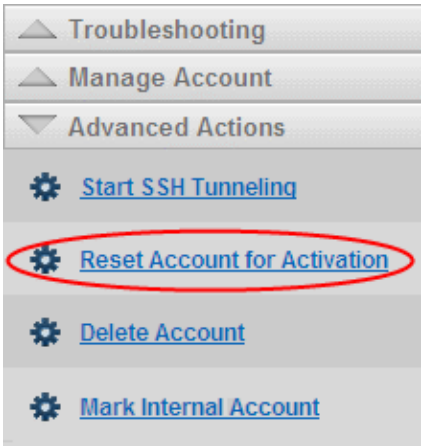
To reset an account for activation:

1. For TouchScreens, have the technician at the premises reset the touchscreen to factory default. **IMPORTANT:** This must be done first.
2. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

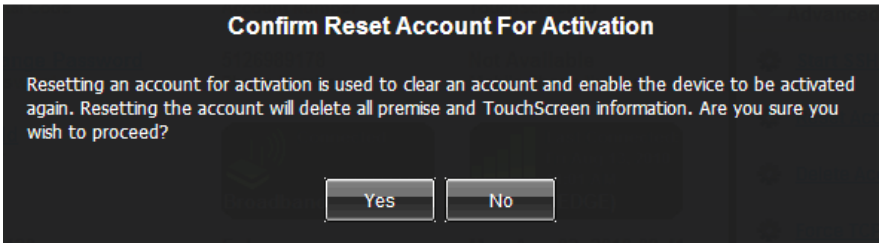
   The Account Information screen is displayed.
3. Open the Advanced Actions menu in the Account Management tools.

4. From the Advanced Actions menu, click **Reset Account for Activation**.

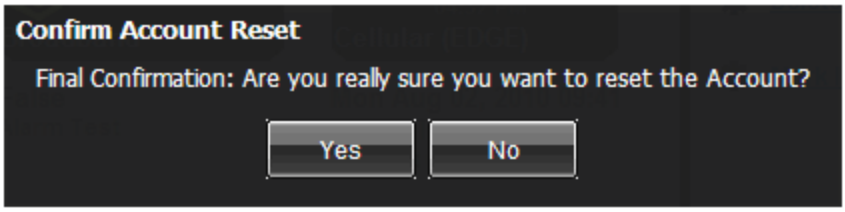
   

   The Management Portal displays a confirmation.

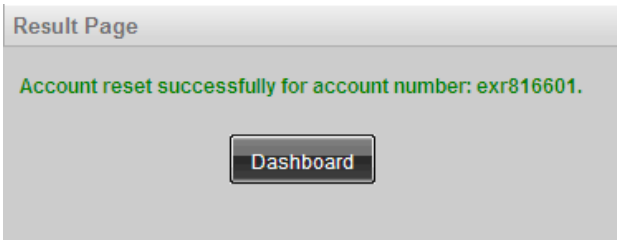
5. Click **Yes**.

   An additional confirmation is displayed.



6. Click **Yes**.

   The Results Page is displayed confirming that the account has been reset for activation.



7. Click **Dashboard** to return to the Dashboard and query for Not Activated accounts.

   When the reset account has been located, its details will display in the Edit Account Information screen and its Activation status is Ready for Activation.

7.2.3 Marking an Account as an Internal Account

Internal accounts are typically used for demos and testing.

Internal accounts do not appear on general service reports or queries (such as Connectivity (online/offline). They can use the “Round-Trip” client that simulates alarms as though they were using an actual touchscreen.

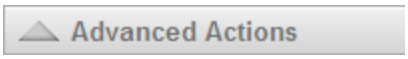
Internal accounts continue to send alarms to central monitoring if they are in Monitor On state.

To mark an account as an Internal account:

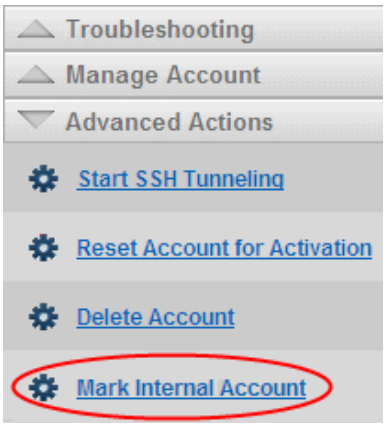
1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

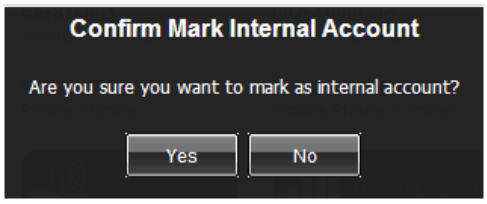
2. Open the **Advanced Actions** menu in the Account Management tools.



3. From the Advanced Actions menu, click **Mark Internal Account**.

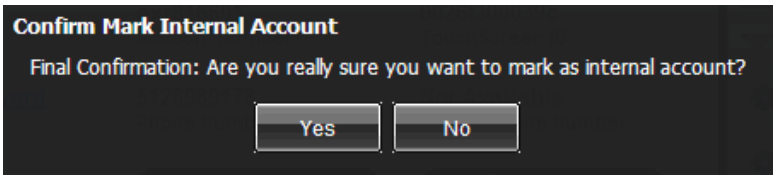


A confirmation dialog is displayed.



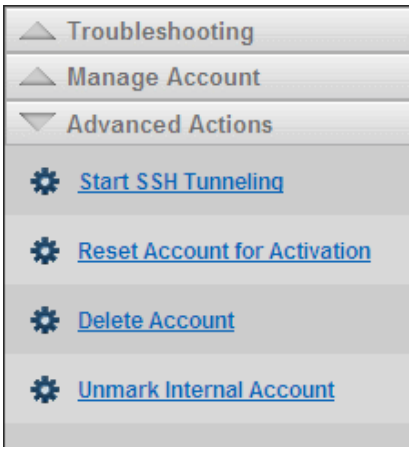
4. Click **Yes**.

   The system displays a second confirmation.



5. Click **Yes**.

   The account is marked as Internal. The link changes to Unmark Internal Account.



7.3 Updating Multiple CPEs as a Batch Job

The Firmware download/update process begins at a configured date/time. CPEs that match the criteria will have their firmware updated. TouchScreens in Armed state will wait until they are disarmed before beginning their update. You can create a Firmware update job for all CPEs matching a variety of granulated criteria, including zip code and hardware model (see Creating a Firmware Update Batch Job on page 114).

The following example explains how the batch update process works in the background:

If 1000 devices are identified for update, the system selects a sub-batch of 300 to be updated first (`batchUpdateItem.size`). Some of the devices are in Armed state and, therefore, unavailable for update; but these are updated as they become available. When an armed device is disarmed, the system waits 5 minutes before queuing the device for update (`firmware.waitTimeAfter`). This delay ensures that the firmware update will not occur if the subscriber leaves the premises, forgets something, and disarms the system to temporarily to enter the premises.

When 80% of the sub-batch (240 devices) has been updated, the system starts updating the next sub-batch (`batchUpdateItem.successPercentage`). Ten minutes after the job starts (`batchUpdateItem.timeout`) the system checks to make sure that at least 5% (15 devices) (`batchUpdateItem.percentageToAbort`) have been updated successfully. If not, the system aborts the sub-batch and starts upgrading the next sub-batch. During the job, the system intermittently (`batchUpdateTask.runInterval`) polls the devices that have successfully updated and posts the Completed % to the Firmware Update Batch List (see "Firmware Update Batch List " on page 118).

See Table 12: Firmware Update Properties below or information about the configurable batch job settings.

You can view and cancel the pending batch jobs (see "Managing Firmware Update Batch Jobs" on page 118). Successful updates are logged on the firmware_update_job table.

7.3.1 Understanding the Batch Update Server Properties

Several server properties define how the system performs a firmware update batch job. Default values are defined in the `server.properties` file, but these values can be overridden in a local `custom.properties` file. See "Update Server Properties" on page 60 for more information on the sections in the `server.properties` file. See "Viewing Batch Firmware Update Server Properties" on page 121 for information on how to view some of these values from the Management Portal.

Table 12: Firmware Update Properties

Setting	Description and Use
batchUpdateItem.size	Size of the sub-batches within a firmware update batch job; (Default is 300)
batchUpdateItem.successPercentage	Percentage above which a sub-batch is considered a success; (Default is 80%)

Setting	Description and Use
batchUpdateItem.percentageToAbort	Percentage below which to abort a batch update; (Default is 5%)
batchUpdateItem.timeout	Number of seconds until a sub-batch must have completed a configured percentage of devices (batchUpdateItem.percentageToAbort) or else it the system will stop the sub-batch and go on to the next one; (Default is 1200)
batchUpdateRequest.sleepInterval	How long to sleep between two firmware update request in milliseconds. (Default is 500)
batchUpdateTask.runInterval	How often the system checks each batch update progress in milliseconds; (Default is 250,000, that is over 4 minutes)
firmware.allowDowngrade	Whether to allow devices will be offered to install earlier than current firmware versions: True = Allow False = Do not allow (Default is false) Note: This does not affect batch updates; only individual updates.
firmware.allowUpdateViaGPRS	Whether to allow devices to update when they are only connected via cellular (GPRS); True = Allow False = Do not allow (Default is false)
firmware.waitTimeAfterDisarm	Number of seconds the system will wait after a device has been disarmed to queue the device for firmware update; (Default is 300, that is 5 minutes)
firmware.misc.directory	For Linux servers, the absolute root directory to save the files associated with firmware.
firmware.misc.directory.windows	For Windows servers, the absolute root directory to save the files associated with firmware.

7.3.2 Creating a Firmware Update Batch Job

See Managing Firmware Update Batch Jobs on page 118 for how to view created batch jobs and to cancel them.

To create a new batch job to update the firmware of CPE devices according to defined criteria:

1. From the main menu, select **Advanced > Batch Firmware Update > Create Job**.

   For service providers that use deployments, the Deployment selector is displayed.

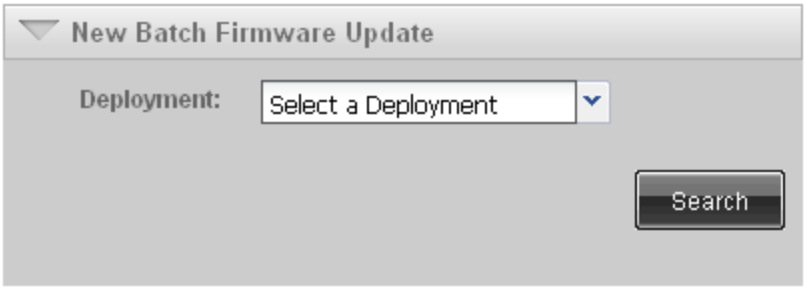


Figure 3: Deployment Selection Screen

   Note: This screen is only displayed for service providers using deployments. Service providers not using deployments skip to the followings screen.

2. Select the deployment to be updated, or select All to update CPE devices regardless of deployment.

3. Click **Search**.

   The New Batch Firmware Update screen is displayed.

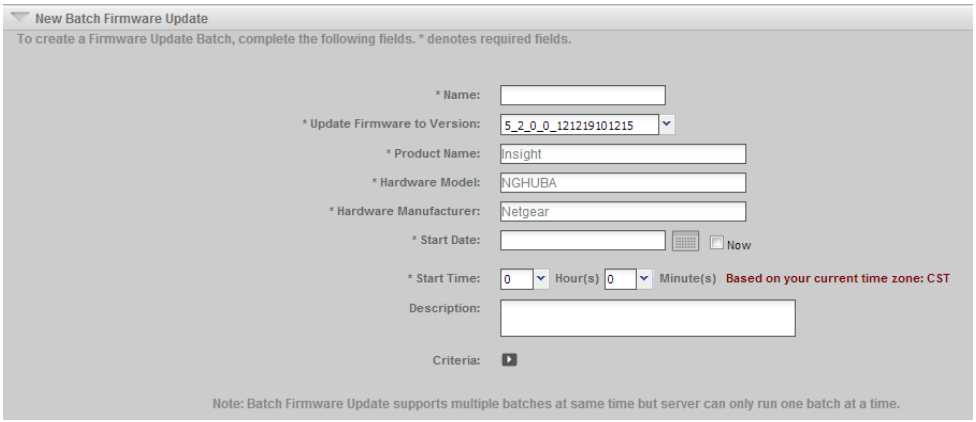


Figure 4: New Batch Firmware Update Screen

Table 13: New Batch Firmware Update Screen Elements

Element	Description	Type	Required
Deployment	The Operator Domain deployment to which the device is assigned; Note: This menu is only displayed for service providers using deployments.	Menu	Not Configurable
Name	Short descriptive name of the new Firmware Batch Update Job; This will display in the Batch Firmware Job lists.	Field	Yes
Update Firmware to Version	Version number of the firmware update	Menu	Yes
Product Name	Converge or Touchstone	Menu	Yes
Hardware Model	Model of the CPE Note: The value of this field is collected from the selected firmware version. It is not editable.	Field	Yes
Hardware Manufacturer	Revision code for the hardware of the CPE device. Note: The value of this field is collected from the selected firmware version. It is not editable.	Field	Yes
Start Date	Date/time that the system will start upgrading the identified CPE devices (excepting TouchScreens in Armed state)	Field	Yes
Start Time		Menus	
Now	Select to have the system start immediately upgrading the identified CPE devices (excepting TouchScreens in Armed state)	Check box	
Description	A brief description of the customers intended to be upgraded by the current job.	Field	No
Criteria	Click to display additional criteria for more explicit choices of the CPE devices to update (see Figure 51: New Batch Firmware Update Screen (Additional Criteria)).	Button	N/A

4. Click **Criteria** to display additional criteria for the CPE devices that will have their firmware updated:

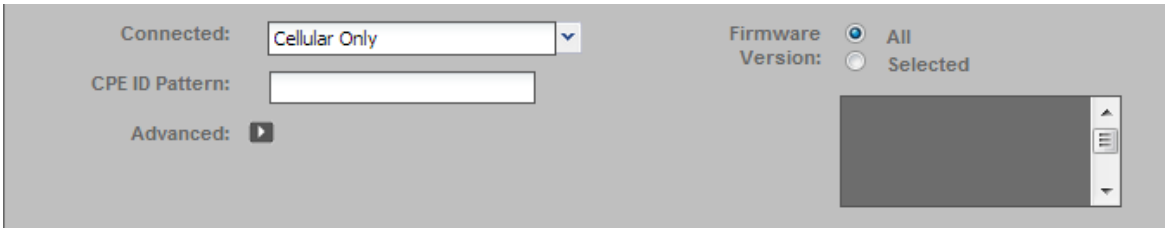


Figure 5: Figure 51: New Batch Firmware Update Screen (Additional Criteria)

Table 14: New Batch Firmware Update Screen – Additional Criteria Elements

Element	Description	Type	Required
Connected	All - All identified CPEs regardless of their connection status.	Menu	No
	Broadband Online - Only devices that with a broadband TCP connection to the Application Cluster and no cellular connection are updated.		
	Cellular Only - Only devices that with a cellular connection to the Application Cluster and no broadband connection are updated. Applicable to Converge only		
	Both Broadband and Cellular - Only devices that with a cellular connection to the Application Cluster and broadband connection are updated. Applicable to Converge only		
	Not Connected - Only devices with no current connection to the Application Cluster are scheduled for update when they re-establish a connection. Devices that are currently connected are not scheduled for update.		
CPE ID Pattern	A partial match to the initial characters of touchscreen or Hub device IDs of the devices that are scheduled for updating. For example, the touchscreen ID is based on the Ethernet MAC address of each touchscreen. If the MAC address is 00:18:5A:02:80:B8, then the touchscreen ID is 00185A0280B8. MAC IDs are typically assigned with to devices sequentially. Enter 00185A02, or 0018, or 0 to only schedule for update devices whose touchscreen ID starts with those characters.	Field	No
Firmware Versions	Devices with specific firmware versions are scheduled for update. All - Select to schedule devices for update regardless of their current firmware version. Selected - Select and Ctrl-click the firmware versions currently loaded in devices that are scheduled for update.	Option & Field	Yes
Advanced	Click to display Advanced criteria for more explicit choices of the CPE devices to update (see New Batch Firmware Update Screen (Advanced fields)).	N/A	

5. Click **Advanced** to display even more fields to refine the CPE devices that will be updated based on geographical and Tier information.

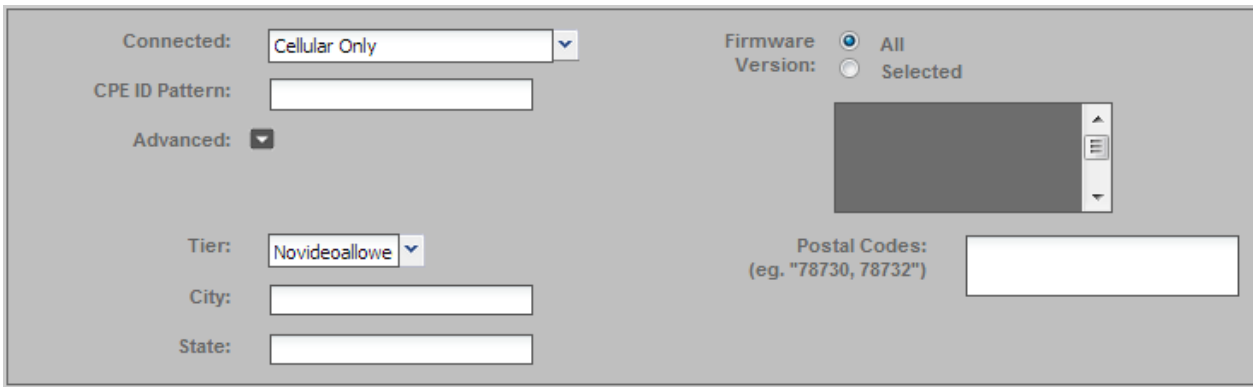


Figure 6: New Batch Firmware Update Screen (Advanced fields)

Table 15: Table 56: New Batch Firmware Update Screen — Advanced Elements

Element	Description	Type	Required?
Tier	Current Tier of the customers that will have their devices upgraded. Note: Global means devices are updated regardless of the customer Tier.	Menu	No
City	City of the customer premises that will have their devices upgraded.	Field	No
State	State of the customer premises that will have their devices upgraded.	Field	No
Postal Codes	Zip code of the customer premises that will have their devices upgraded; To include multiple zip codes in the batch list them separated by commas. For example: 78750, 78752, 78734	Field	No

6. Click **Save**.

The new batch update is scheduled. The Firmware Versions screen displays all the batch firmware versions available.

Firmware Update Batch List

Name	Creation Date	Start Time	Stop Time	State	Count	% Completed
test2	01.06.2010 07:53AM	01.06.2010 08:00AM		Aborted	2	0
test11	01.14.2010 06:50AM	01.14.2010 07:00AM		Aborted	4	0
test11	01.19.2010 06:42AM	01.19.2010 06:45AM		Aborted	4	0
jan20	01.20.2010 06:17AM	01.20.2010 06:45AM		Aborted	3	0
test14	01.27.2010 06:01AM	01.27.2010 06:15AM	01.27.2010 06:49AM	Completed	4	50
test21	02.03.2010 06:12AM	02.03.2010 06:15AM	02.03.2010 06:50AM	Completed	3	33

Figure 7: Firmware Update Batch List

Table 16: Firmware Update Batch List Columns

Column	Description	
Name	A short descriptive name for the batch job; Click to display details of a batch job or abort it.	
Creation Date	Date the batch job was created.	
Start Time	Date/time the batch job is schedule to start.	
Stop Time		
State	Aborted	Current batch job was canceled.
	Completed	All the identified CPEs were successfully updated.
	Pending	Current batch job has not yet started.
	Started	Current batch job has started but has not completed.
Count	Number of devices updated so far in the current batch job.	
% Completed	Percent of total scheduled devices that have been updated so far.	

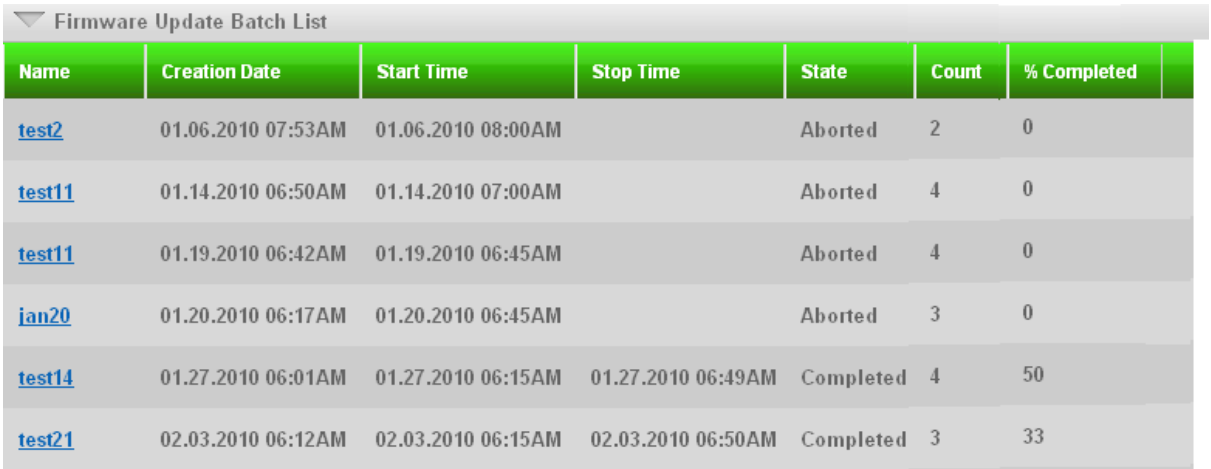
7.3.3 Managing Firmware Update Batch Jobs

See "Creating a Firmware Update Batch Job" on page 114 for how to create new batch jobs.

To view and cancel batch jobs to update the firmware of CPEs

1. From the main menu, select **Advanced > Batch Firmware Update > View Jobs**.

   The Firmware Update Batch List is displayed. Click on the column header to sort by that column.



Note: See Firmware Update Batch List Columns on page 118 for information about the columns in this list.

2. To view the details of a batch job or to cancel it, click the batch job name in the list.

   The View Firmware Update Batch is displayed.

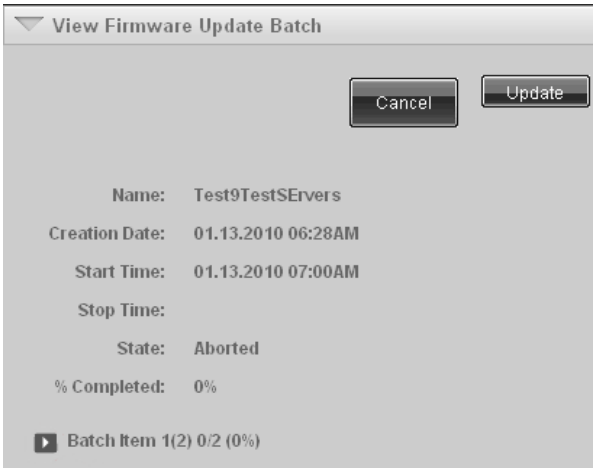


Figure 8: View Firmware Update Batch Screen

Table 17: View Firmware Update Batch Screen Elements

Element	Description	
Name	A short descriptive name for the batch job; Click to display details of a batch job or abort it.	
Creation Date	Date the batch job was created.	
Start Time	Date/time the batch job is schedule to start.	
Stop Time		
State	Aborted	Current batch job was canceled.
	Completed	All the identified CPEs were successfully updated.
	Pending	Current batch job has not yet started.
	Started	Current batch job has started but has not completed.
Count	Number of devices updated so far in the current batch job.	
% Completed	Percent of total scheduled devices that have been updated so far.	
Batch Item button	Click to view the list of CPEs to be updated in the current batch.	

Element	Description
Batch Item Summary	Summaries the state of the current bath; For example: 3(100)30/100(30%) means the following: The ordinal number of the batch is 3 The batch has 100 CPEs scheduled to be updated 30 of the scheduled CPEs have been successfully updated 30% of the total batch is complete.

3. Click the Batch Item button to display a list of CPEs to be updated in the current batch.

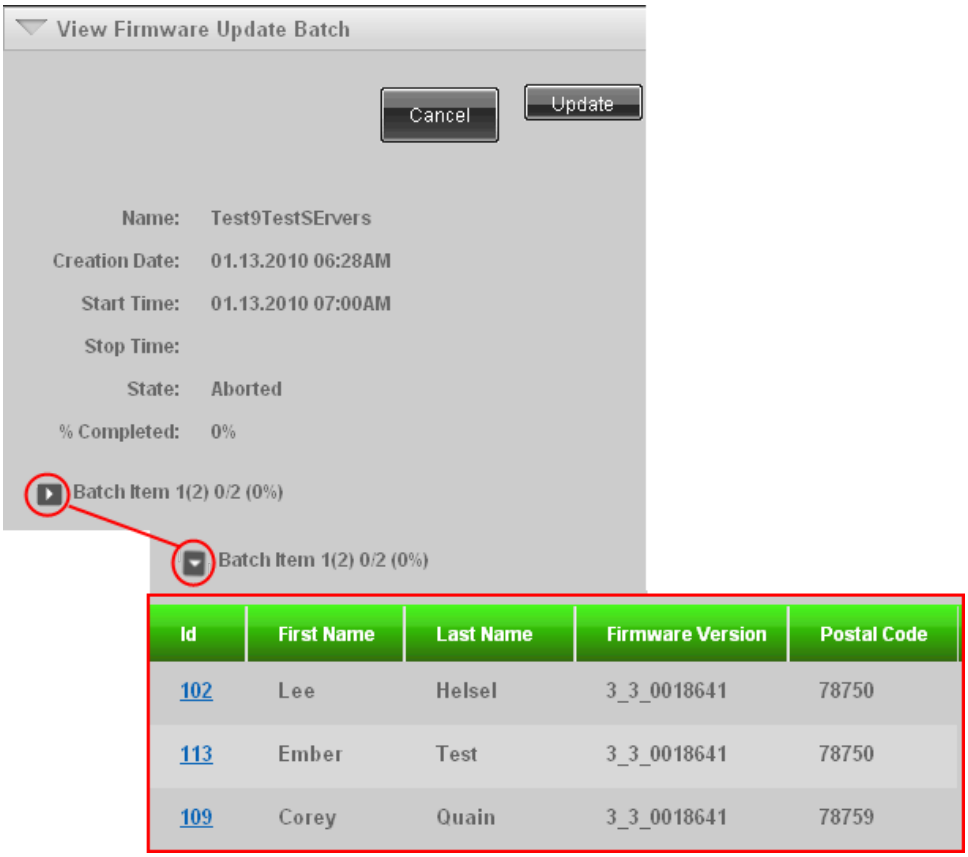


Figure 9: View Firmware Update Batch Screen: Batch Item

Table 18: View Firmware Update Batch Screen Elements – Batch Items

Element	Definition
ID	Internal identifier for the account associated with the CPE. Click to display the Account Information screen of the account.

Element	Definition
First Name	First and last name of the person associated with the CPE account.
Last Name	
Firmware Version	Firmware version installed on the CPE before the update.
Postal Code	Postal Code of the location of the premises of the CPE account.

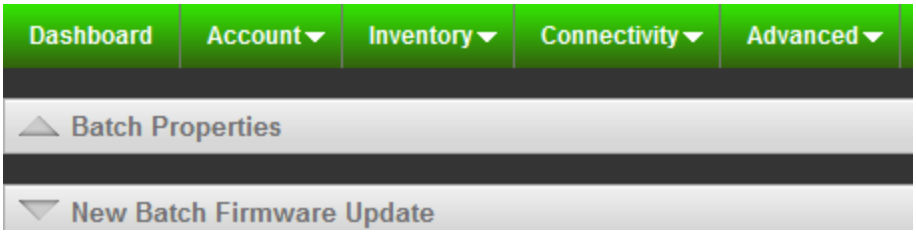
7.3.4 Viewing Batch Firmware Update Server Properties

The values of some of the server properties that control the behavior of the batch firmware update process can be viewed from the Management Portal.

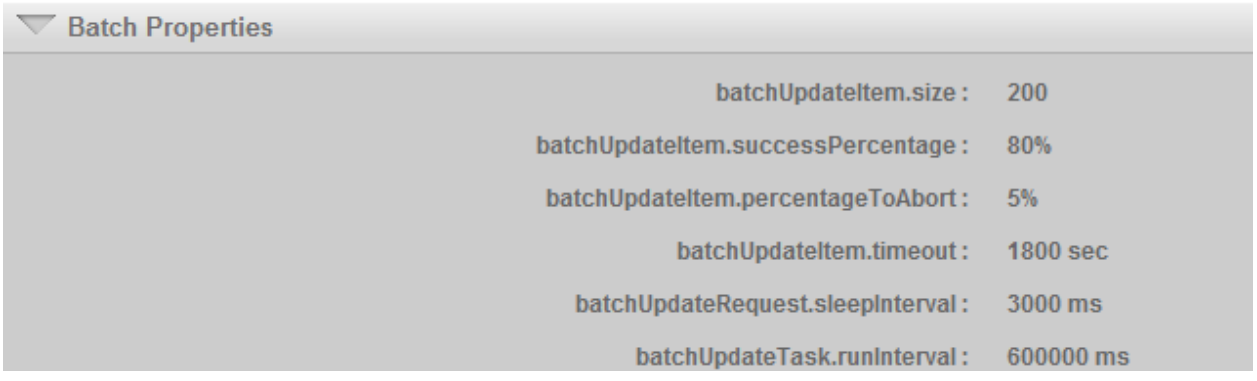
To review the current server properties values:

1. From the main menu, select **Advanced > Batch Firmware Update > Create Job** or **Advanced > Batch Firmware Update > View Jobs**.

   A screen similar to the following is displayed.



2. Click **Batch Properties**. The current server property values are displayed.



See Understanding the Batch Update Server Properties on page 112 for more information about these properties.

8 Reviewing System Status

System status tabs are available based on user roles. The full list is:

- Security (page 122)
- Account (page 129)
- CPE (page 139)
- Advanced (page 153)

8.1 Security Reports

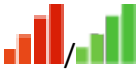
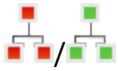
The following reports are available under the Security tab:

- Alarms (page 124)
- History (page 125)
- Keypad codes (page 127)
- Pictures and Videos (page 127)
- Troubles (page 127)
- Zone (page 129)

The following table describes the icons potentially displayed in the System Status reports on the Account Information screen.

Table 19: System Status Event Types Icons

Event Type	Description	
Alarms (Converge only)	ALARM	An alarm or test alarm was generated
	TEST	
		Panic alarm was generated / cleared
		Panic Police alarm was generated / cleared
		Carbon monoxide alarm was generated / cleared
		Fire alarm was generated / cleared
		Panic Fire alarm was generated / cleared
		Water was was generated / cleared
		Panic Medical alarm was generated / cleared
Arms/Disarms (Converge only)	System was disarmed or armed in Arm Away, Arm Stay, or Arm Night mode.	
		System armed / disarmed

Event Type	Description	
Trouble Events	System Trouble events are when the touchscreen has lost of power or has a low battery. Zone Trouble events are when a sensor has failed (perhaps due to battery power) or is being tampered with.	
		touchscreen power disrupted / restored (System Trouble event)
		Broadband connectivity disrupted / restored (System Trouble event)
		Cellular connectivity disrupted / restored (System Trouble event)
		Wi-Fi connectivity disrupted / restored (System Trouble event)
		Loss of all connectivity (System Trouble event)
		A Zone Trouble event has occurred, such as a bad battery or the cover has been removed on a sensor.
		Battery in the touchscreen or a sensor is low / restored

8.1.1 Alarms Report (Converge Only)

This report lists alarm events for the account. Emails and text messages are included in the report.

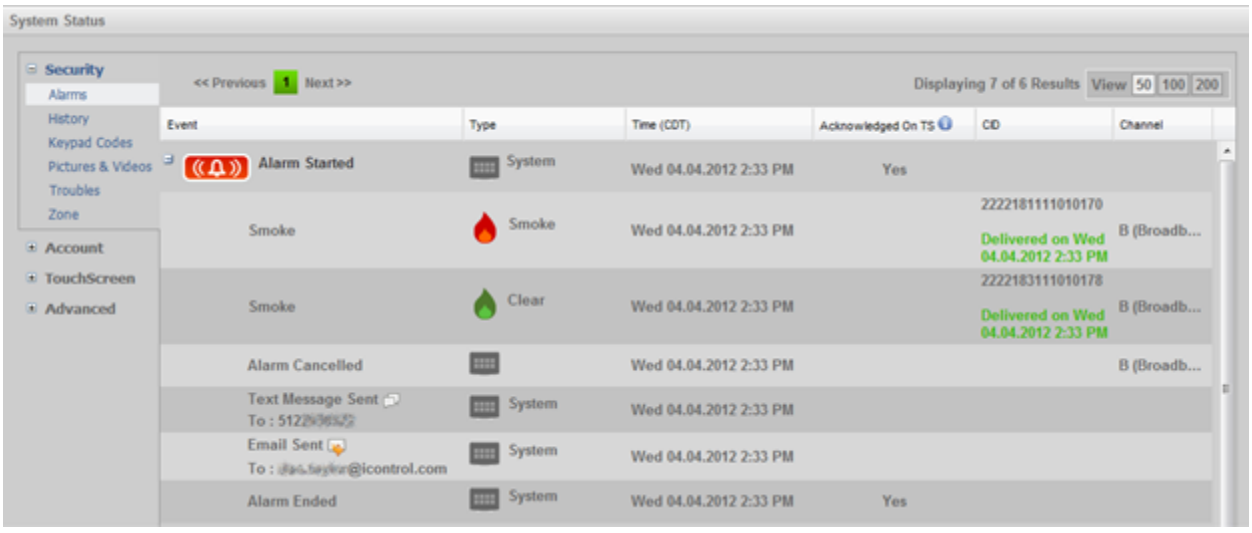


Table 20: Alarms Report Columns (System Status Reports Section)

Column	Description
Event	A description of the action taken during the event.
Type	The type of event, i.e., sensor generated, system generated, etc.
Time	Time/date that the alarm event occurred. The account's time zone is displayed in the column title, such as CDT for "Central Daylight Savings Time".
Acknowledged on TS	Whether the alarm has been acknowledged on the touchscreen.
CID	CID of the alarm event and whether the alarm was delivered successfully to the central monitoring service (whether or not an acknowledgment was received from the central monitoring service).
Channel	Method by which the alarm was reported: B (Broadband) touchscreen reported the alarm event over broadband. C (Cellular) touchscreen reported the alarm event over cellular (broadband was down). S (System) System servers reported the alarm event such as Smash & Grab which is initiated when information is not received from the touchscreen.

Note: The customer will receive SMS and email messages with the timestamp of the touchscreen broadband connectivity being restored instead of the actual timestamp of the alarm event if an alarm event occurs when the touchscreen broadband is offline and if the CPE time is one year or more behind of the server time. Only SMS and email messages are affected; the time and date in the alarm report in the Management Portal and the activity in the subscriber interface are correct.

8.1.2 History Report

The History report lists all the events reported by the system. The events can be filtered to search for specific events.

Note: If the subscriber has not cleared a trouble and the alert is reported after the reset period, the trouble notification includes the time and date the trouble was originally reported.

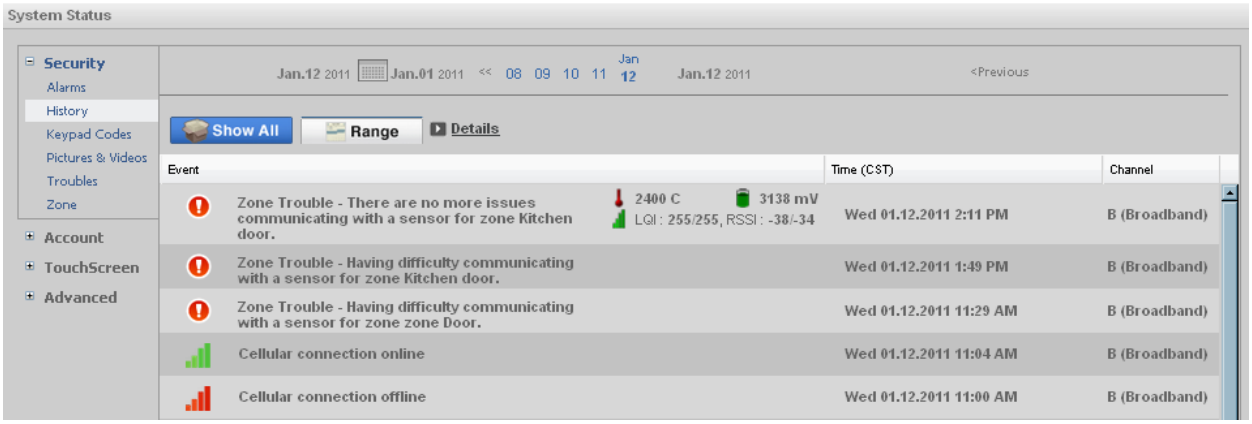
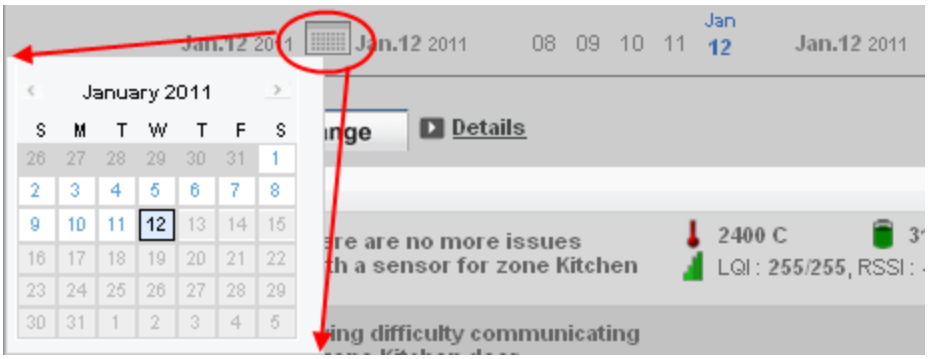


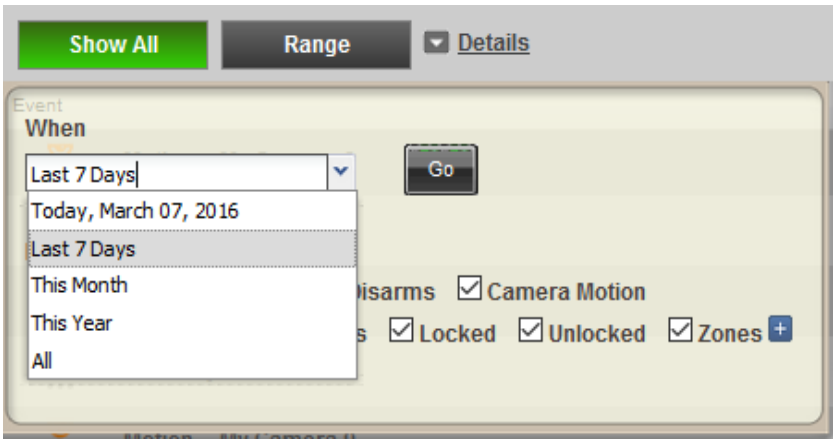
Table 21: History Report Columns (System Status Reports Section)

Column	Description
Event	Short description of the event. Some system troubles will appear only in the History report. **IMPORTANT:** Alarms generated by the Duress keypad code are recorded in the Management Portal History Report only.
Time	Time/date that the event occurred. The account's time zone is displayed in the column title, such as CDT for "Central Daylight Savings Time".
Channel	Method by which the event was reported: B (Broadband) touchscreen reported the event over broadband C (Cellular)touchscreen reported the event over cellular (broadband was down) S (System)A system reported event

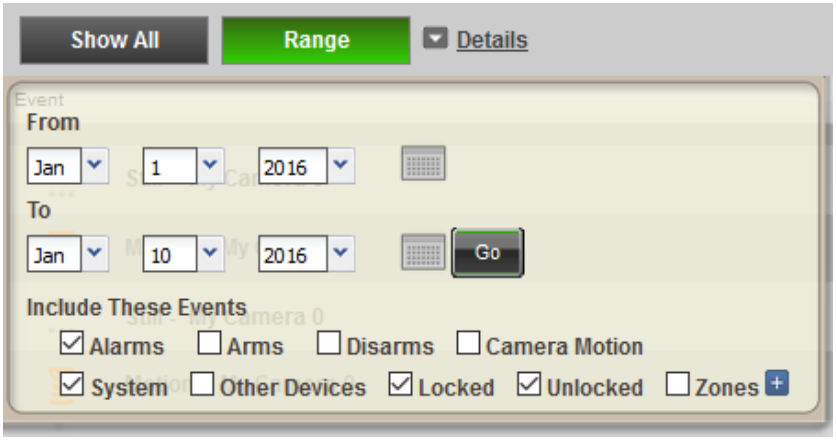
To filter the events by day, click the **Calendar** icon and click on a day to display only the events that occurred on that day.



To display the events by a preselected date range, click **Show All**, then click on the **Details** link to display a pop-up with additional filters.

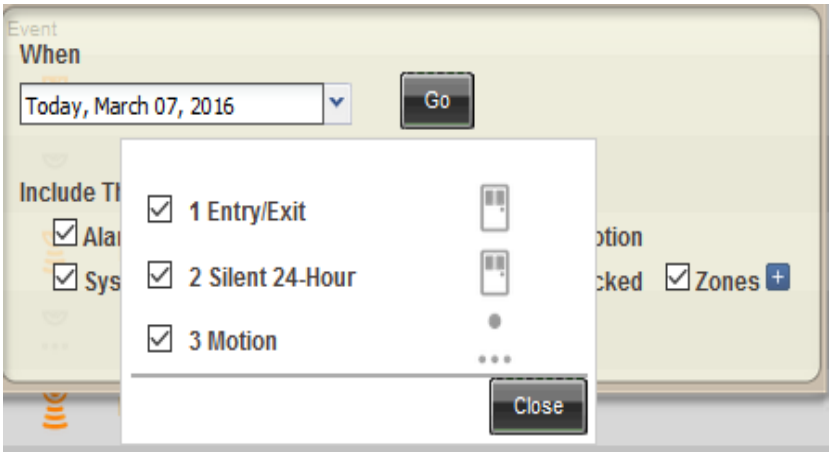


To display the events for a custom date range, click **Range**, then click on the **Details** link to display a pop-up with additional filters.



Select the events to include in the History report and deselect the events to be filtered out of the History report.

Click the plus icon next to **Zones** to filter the events from certain zones. Click **Go** to run the report.



8.1.3 Keypad Codes Report (Converge Only)

This report lists the keypad codes configured for the account.

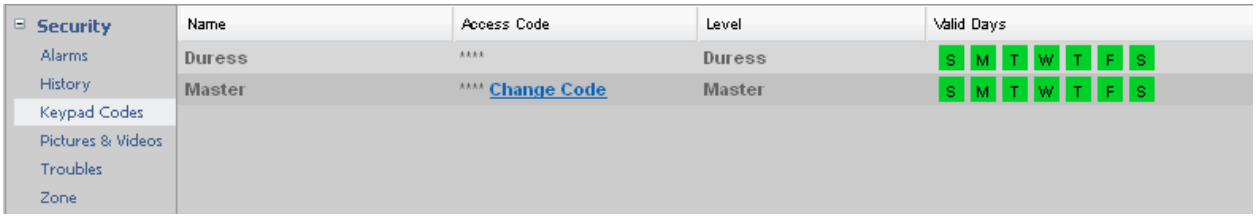


Table 22: Keypad Codes Report Columns

Column	Description
Name	Keypad code type or name for customer-configured codes.
Access Code	Value is hidden. Click **Change Code** to change the associated code (see "Modifying the Master Keypad Code for a Converge Account" on page 97). Only the Master code can be changed from this report. You must have Admin privileges to change the access code.

Column	Description
Level	Keypad code level (Standard, Guest, Arm Only, Duress, or Master).
Valid Days	Days that the keypad code can be used.

8.1.4 Pictures & Video Report

This report lists events for the account that resulted in a camera taking a picture or video, including manual images captured by the user. The actual images are not accessible from the Management Portal.

Note: The items listed on this report are not updated dynamically. To view new items taken since the current Account Information page was displayed, refresh your browser.

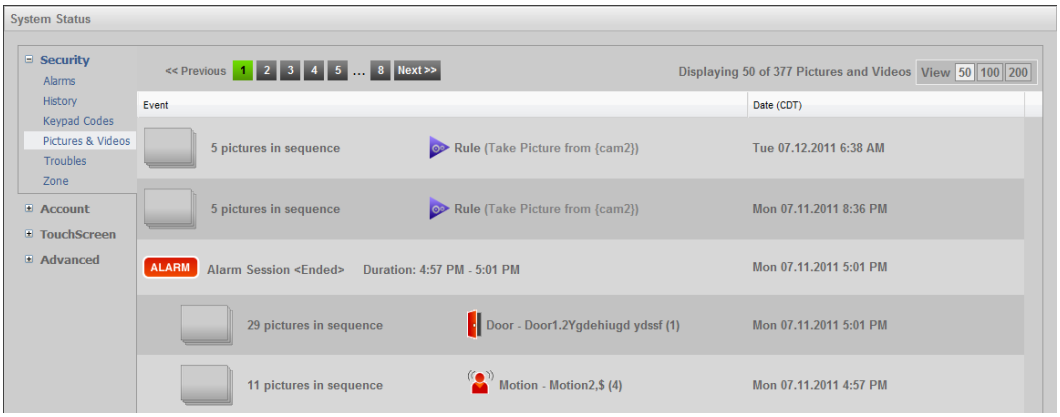


Table 23: Pictures and Video Report Columns (System Status Reports Section)

Column	Description
Event	Description of the event. Where applicable, the duration of the event.
Date	Time/date that the image or video was captured. The account's premises time zone is displayed in the column title, such as CDT for "Central Daylight Savings Time".

8.1.5 Troubles Report

This report displays any current Trouble alert being reported by the account touchscreen. If no Trouble is being reported, this report is empty. If troubles are being reported, an icon is displayed to the left of the Troubles link.

Note: If the subscriber has not cleared the trouble and the alert is reported after the reset period, the trouble notification includes the time and date the trouble was originally reported.

Table 24: Trouble Report Columns (System Status Reports Section)

Column	Description
Event	Text of the Trouble event. Some server events will be displayed in the History report only.
Time	Time/date that the trouble event was originally reported. The account's premises time zone is displayed in the column title, such as CDT for "Central Daylight Savings Time".

8.1.6 Zone Report

This report lists all the security zones in the account system and their current state.

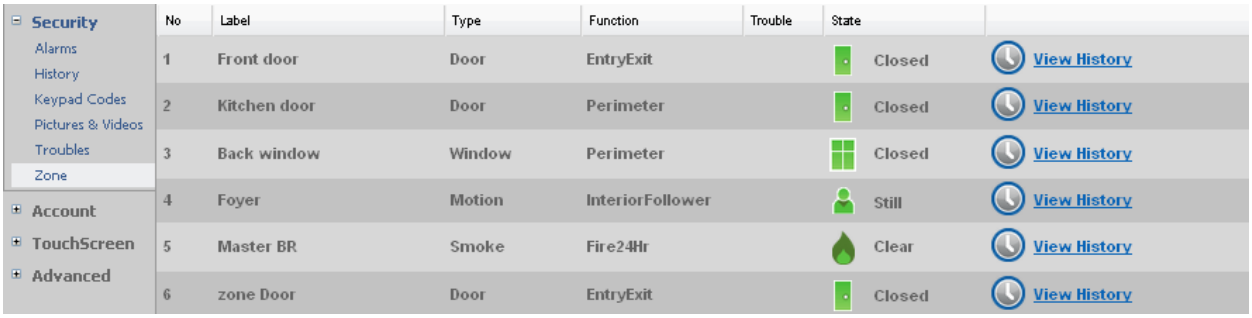


Table 25: Zone Report Columns

Column	Description
No	Number of the security zone
Label	Customer-assigned (or default) label of the security zone
Type	Sensor type
Function	Assigned function for the sensor
Trouble	Any trouble event currently being reported by the zone
State	Current state of the security zone
View	Click to view a History report (page 125) filtered for only zones.

8.2 Account Reports

This group displays reports related to account settings and logs.

- Account
- Account Log (page 131)

- Audit Log (page 133)
- Command History (page 135)
- Contacts (page 135)
- Emergency Dispatch (page 137)
- Quotas (page 137)
- Rules (page 138)

8.2.1 Account Report

This report lists details about the current account.

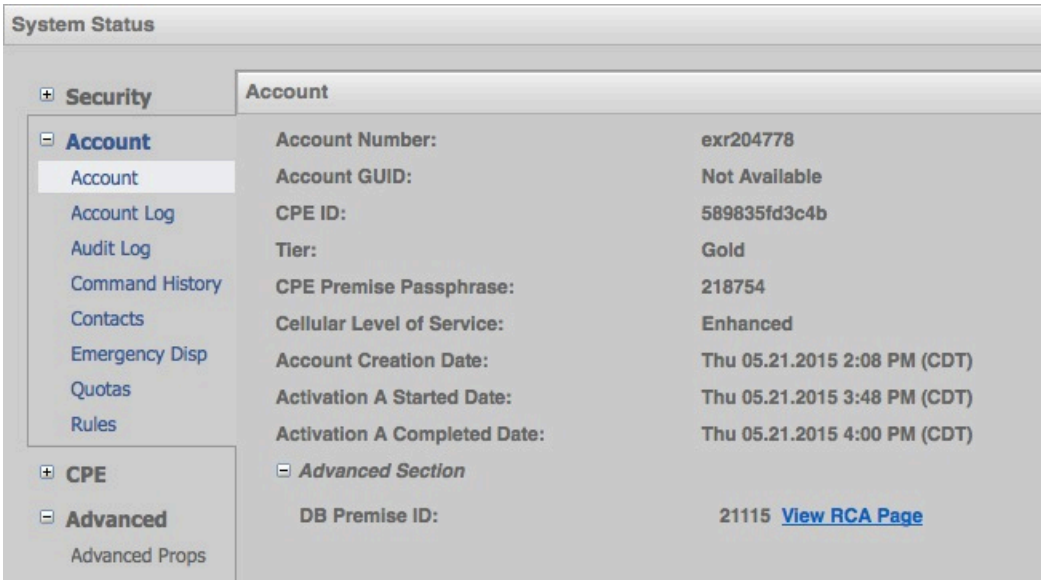


Table 26: Account Report (System Status Reports Section)

Field	Description
Account Number	Service provider ID for the current account.
Account GUID	Service provider SSO ID for the current account.
CPE ID	ID for the system, usually based on the device's MAC address.
Tier	Current Tier-level of the account.
CPE Premise Passphrase (Converge Only)	ID required for making certain sensitive changes to the touch-screen.
Cellular Level of Service (Converge Only)	Basic, Basic Plus, or Enhanced.
Account Creation Date	Time/date that the account was created.
Activation A Started Date	Time/date that activation A started.
Activation A Completed Date	Time/date that activation A was completed.
DB Premises ID	ID assigned to the premise.

8.2.2 Account Log Report

This report lists the touchscreen and zone update events that have occurred.

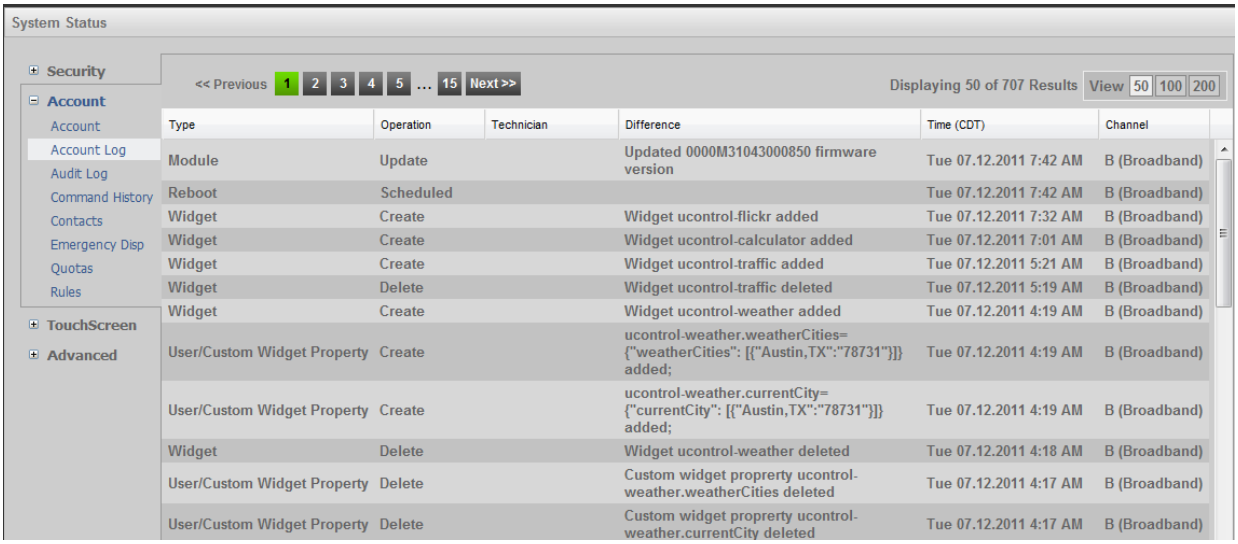


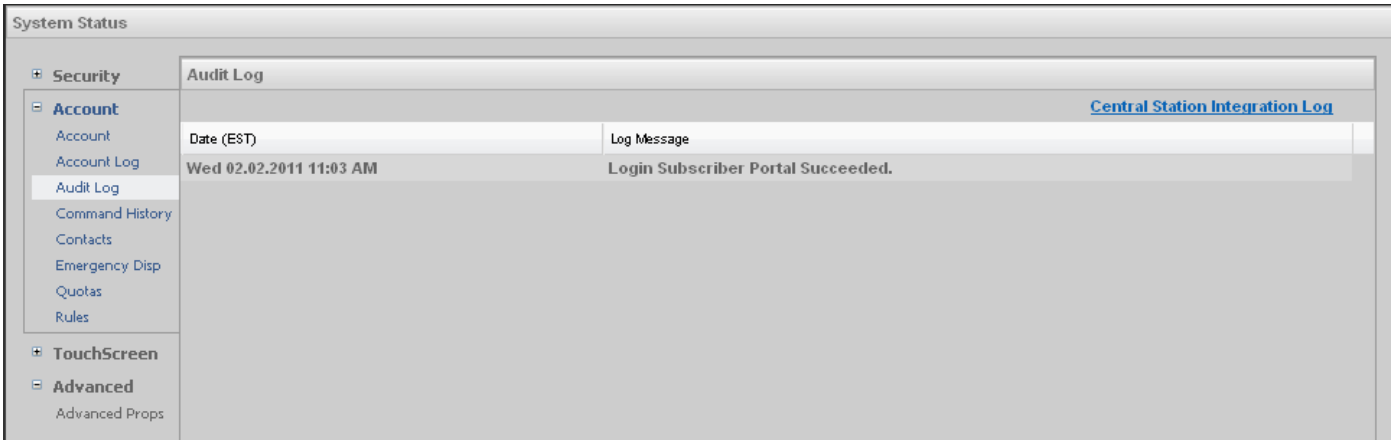
Table 27: Account Log Report

Column	Description
Type	The system element being modified: **Module**: touchscreen settings **Reboot**: touchscreen rebooted **Firmware**: Touchscreen firmware **Zone**: Security zones **Keypadcode**: Keypad codes **Property**: Tier property assigned to the account **App**: App used by the account **App Property**: App property that is not user configurable, such as the URL. **User/Customer Property**: App properties that are configurable by the customer **App Order**: Order the apps are displayed on the touchscreen **Camera**: Camera assigned to the system **Peripheral**: Key pad or key fob assigned to the system **Thermostat**: Thermostat sensor assigned to the system **CellularConnType**: Cellular connection type (GPRS or EDGE) used by the touchscreen to connect to the servers **CellularIpAddress**: Cellular IP address of the touchscreen SIM card
Operation	**DownloadComplete**: Firmware update is finished **UpdateStarted**: Firmware update process has started **UpdateComplete**: Firmware update process has completed **Create**: Item was added to the system **Update**: Item was modified **Delete**: Item was deleted **MulticastFailed**: touchscreen (Module) has lost all communication with the servers, both broadband cellular **Scheduled**: touchscreen was rebooted automatically as part of a process **Unscheduled**: touchscreen was rebooted manually by the customer or a technician

Column	Description
Technician	Name or ID of the Technician that performed the operation. Null if the operation was performed by a customer.
Difference	A description of the change
Time	Time/date that the event occurred. The account's time zone is displayed in the column title, such as CDT for "Central Daylight Savings Time".
Channel	Method by which the event was reported: **B** (Broadband) touchscreen reported the event over broadband **C** (Cellular) touchscreen reported the event over cellular (that is, broadband was down) **S** (System) A system reported event

8.2.3 Audit Log Report

This report lists the history of actions performed on the account. It also provides a link to view the Central Station Integration Log.



The following actions related to an account are recorded in the Audit Log.

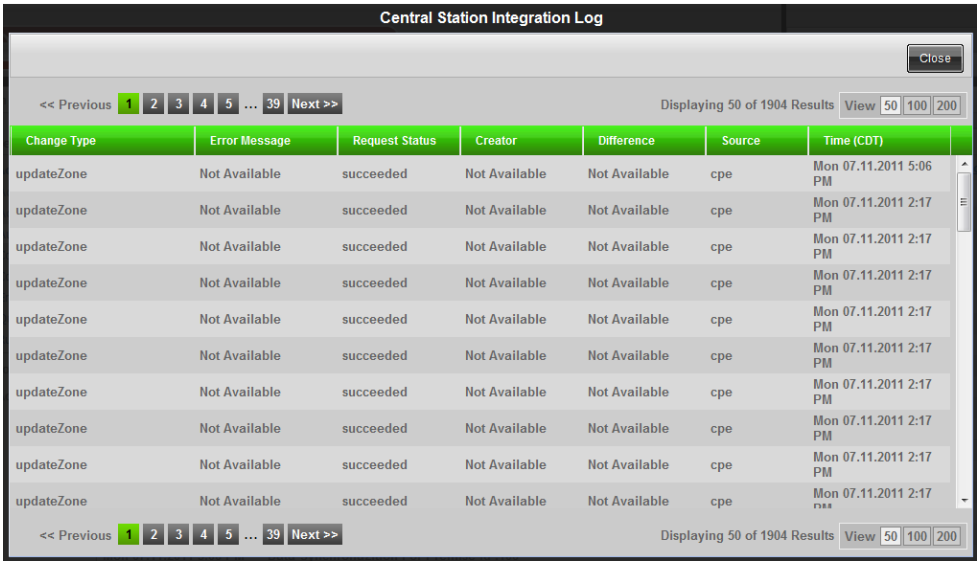
- Login attempts
- Account user name changes
- Account password changes
- Central station monitoring changes
- Central station account number changes
- Central station phone number changes
- Suspending/restore account
- Marking/unmarking account as Internal Account

- Account accessed through Management Portal Backdoor
- Resending activation email
- Deleted/deactivated accounts

Table 28: Audit Log (System Status Reports Section)

Column	Description
Date	Time/date that the login attempt occurred. The account's time zone is displayed in the column title, such as CDT for "Central Daylight Savings Time".
Log Message	Description of the action.

Clicking the Central Station Integration Log displays the following screen:



The Central Station Integration Log screen contains the following information:

Table 29: Central Station Integration Log

Column	Description
Change Type	The name of the command that was executed.
Error Message	Error message (if any) returned from central monitoring for the current communication attempt.

Column	Description	
Request Status	The current status for the communication attempt: ❑ succeeded ❑ failed ❑ queued	
Creator	Creator of the account that sent the communication to central monitoring (where applicable).	
Difference	The change requested against the “Change Type” being updated; For example, for the Change type “updateTestFlag” the Difference can be “Test on” or Test off”.	
Source	cpe	Change was initiated by the CPE.
	csr	Change was initiated by a Management Portal user.
	external	Change was initiated by the system servers or another source.
Time	The time stamp when the change request occurred.	

8.2.4 Command History Report

This report displays a list of commands executed by all users. You must use either the calendar or the date selector to search for events on a specific date, as shown in the following image. Filtering by date range is not supported.

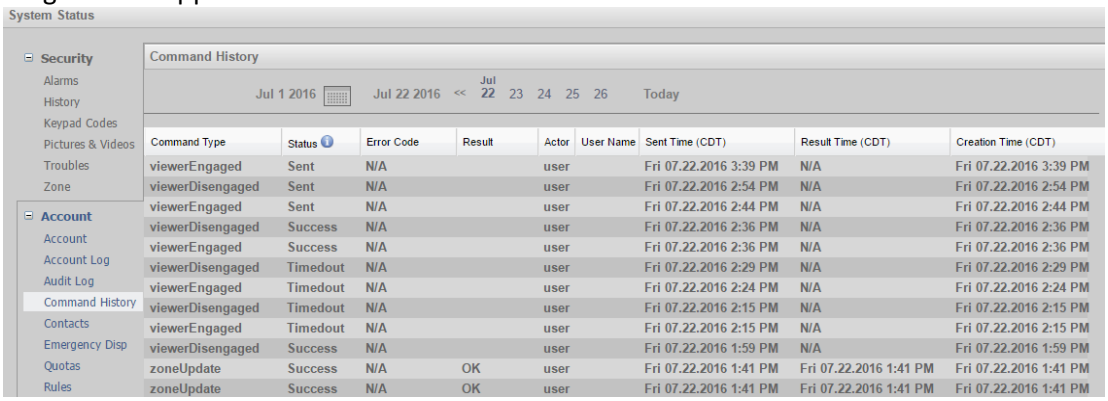


Table 30: Command History Report

Column	Description
Command Type	Type of command that was executed.

Column	Description
Status	One of: ❑ created ❑ queued ❑ sent ❑ success ❑ error ❑ canceled ❑ timed out
Error Code	Error code returned from the touchscreen.
Result	Command results, if any.
Actor	Type of user that sent the command (user, csr).
User Name	User name of the csr that executed the command.
Sent Time	When the touchscreen sent the command.
Result Time	When the command result was returned from the touchscreen.
Creation Time	When the record was created.

8.2.5 Contacts Report

This report lists the contacts that the customer has added who are available to receive email and SMS messages from rules. The account owner is added to this list by default.

Note: These contacts are not necessarily the same as the emergency dispatch contacts who verify alarms for central monitoring (see page 137 for more information).

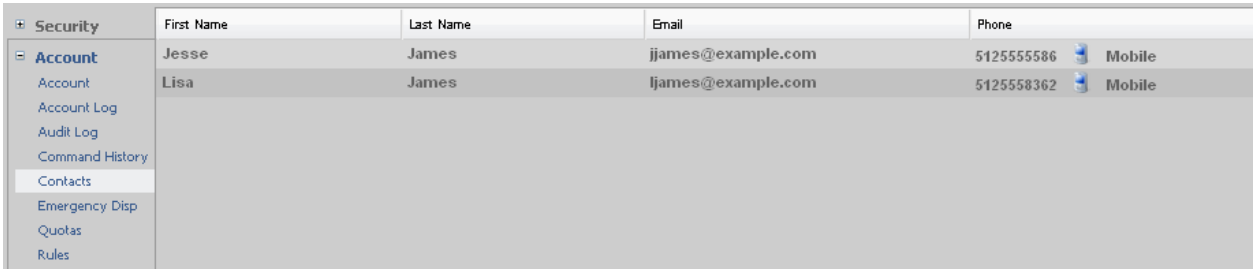


Table 31: Contacts Report

Column	Description
First Name / Last Name	The first and last name of the contact.
Email	Email address of the contact.

Column	Description
Phone	Phone number of the contact and the phone type. This information is used for sending SMS alerts.

8.2.6 Emergency Dispatch Report (Converge Only)

This report lists the contacts that the central monitoring station calls to verify an alarm.

The emergency dispatch contacts are added at the time the account is created. They can be edited from this screen and from the user portals.

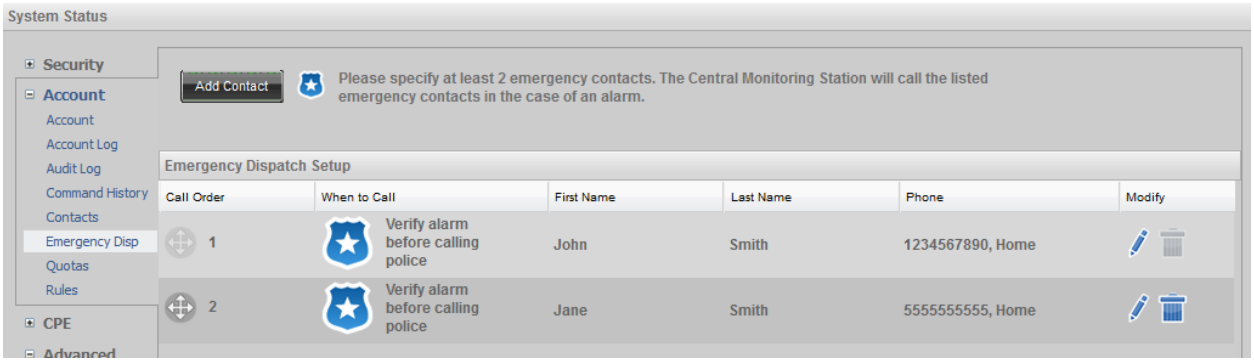


Table 32: Emergency Dispatch Report

Column	Description
Call Order	Order that central monitoring will use to contact the emergency dispatch contacts
Contact	First and last name of the emergency dispatch contact
Phone	Phone number central monitoring uses to call the contact
Phone Type	Type of phone (mobile, home, etc.) for the contact phone number
Alarm Ordinance And Permit Registration	Optional. The alarm permit number and expiration date, when applicable

8.2.7 Quotas Report

This report lists the number of pictures, videos, and SMS messages allowed for this account and indicates whether the account has reached the quota for each of these items. If any quotas are reached or near the maximum, the most severe status icon is displayed to the left of the Quotas link.

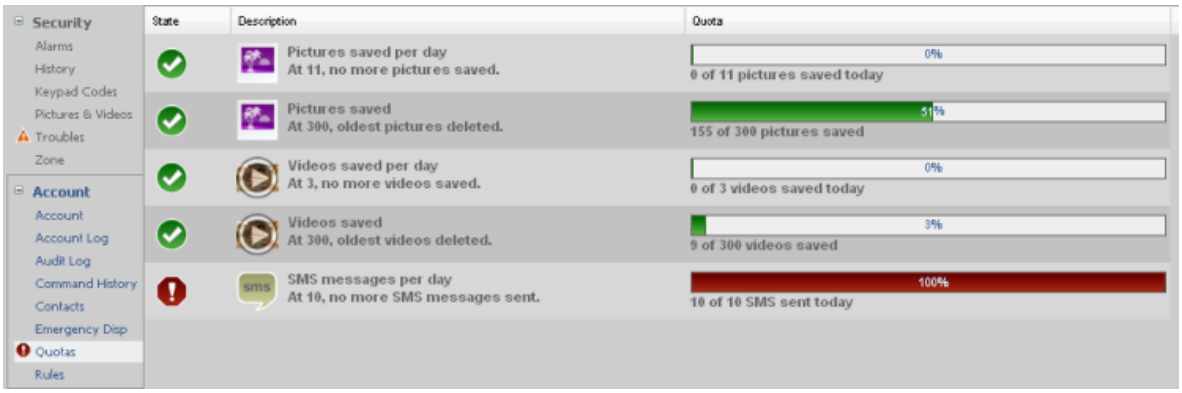


Table 33: Quotas Report

Column	Description	
State		The current count is less than 85% of the quota.
		The current count is greater than or equal to 85% of the quota.
		The quota has been reached.
Description	Lists the maximum number of pictures, pictures per day, videos, videos per day, and SMS messages per day. These values are set by the following Tier properties: ❑ image.upload.dailyLimit ❑ video.upload.dailyLimit ❑ sms.dailyLimit **Note:** The maximum number of images can be exceeded if an alarm is generated. Five pictures from each camera will be taken and stored when an alarm is generated even if the quota has been reached.	
Quota	Specifies the current and maximum values for each item and expresses the ratio in a bar graph.	

8.2.8 Rules Report

This report lists and details the rules created by the system and user.

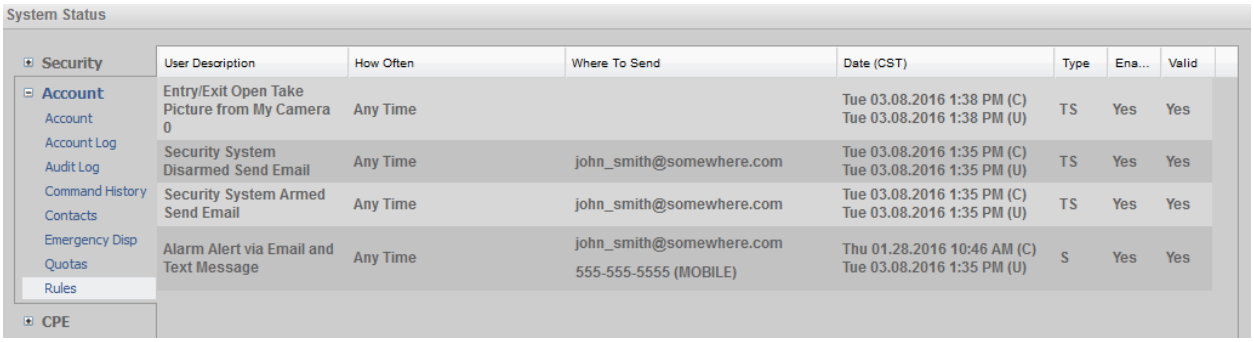


Table 34: Rules Report

Column	Description
User Description	User generated rule description (default is the auto description)
How Often	Time or time range during which the rule applies
Where to Send	Receiving phone number or email address (only for rules that send SMS or email alerts as an action)
Date	Date/time that the rule was created (C) or last modified (U).
Type	Which system executes the rule, CPE (TS) or the server (S).
Enabled	Indicates whether the rule is enabled or disabled. If the rule is disabled, it will not run when the trigger is detected.
Valid	Indicates whether the rule is valid or not. A rule can be marked as invalid if the device used in the rule is no longer paired with the CPE.

8.3 CPE Group Reports

This group displays reports related to the devices installed at the account premises:

- Cameras
- Connectivity between the touchscreen and the system servers (page 140)
- Door locks (page 142)
- Lights (page 144)
- Peripherals, such as key fobs and key pads (page 146)
- Sensors, such as door/window sensors, motion detectors, smoke detectors, etc. (page 146)
- Thermostats (page 147)
- Cloud objects (page 149)

- CPE (page 147)
- Apps installed on the touchscreen (page 152)

8.3.1 Cameras Report

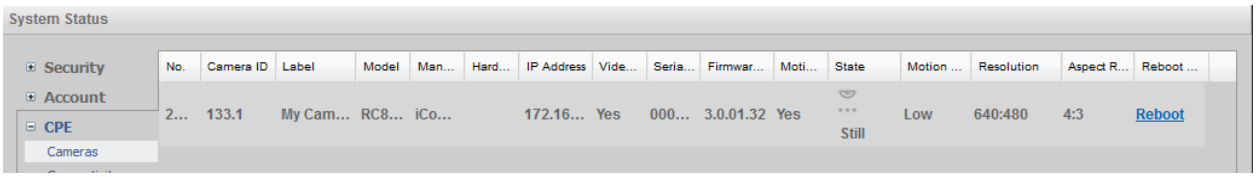
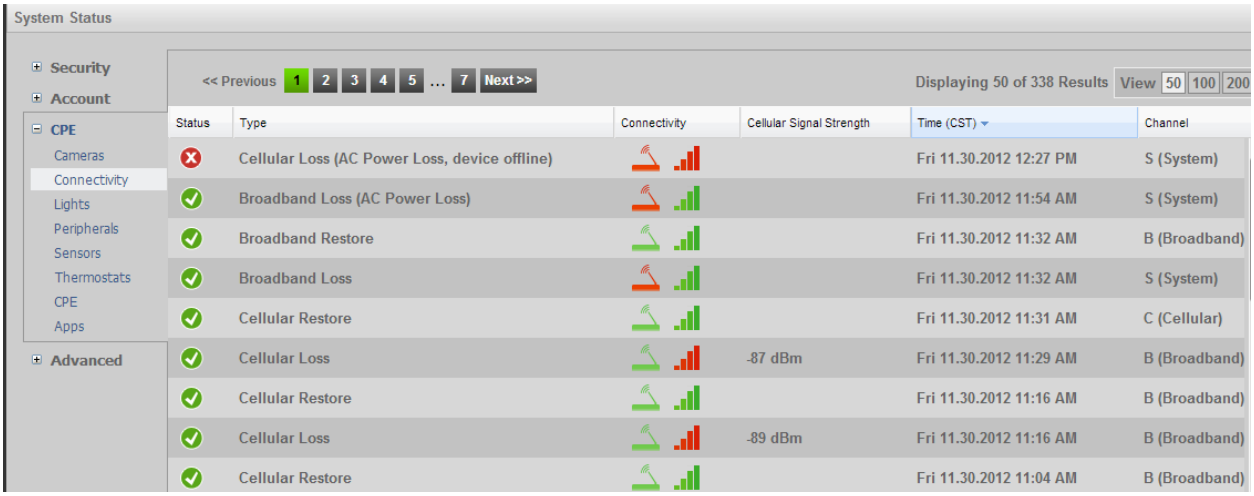


Table 35: Cameras Report

Column	Description
No.	System database number assigned to the camera
Camera ID	Unique identifier assigned to the camera by the touchscreen
Label	Name of the camera assigned by the customer
Model	Model of the camera
Manufacturer	Name of the manufacturer, if available.
Hardware Revision	Hardware revision number of the camera, if available.
IP Address	IP address of the camera
Video Recordable	Indicates whether the camera can record video (Y or N).
Serial No.	Serial number of the camera
Firmware Version	Firmware version of the camera.
Motion Capable	Whether the camera is capable of detecting motion.
State	The current state of the camera's motion detection (still or motion).
Motion Sensitivity	The motion sensitivity set on the camera (high, medium, low, off).
Resolution	Video quality setting on the camera.
Aspect Ratio	The size of the image or video captured by the camera.
Reboot Camera	Clicking on the link reboots the camera remotely.

8.3.2 Connectivity Report

This report lists the changes in connectivity between the CPE and the system servers.



The event types can be sorted or filtered by clicking on the down-arrow in the **Type** header and selecting from the drop-down menu.

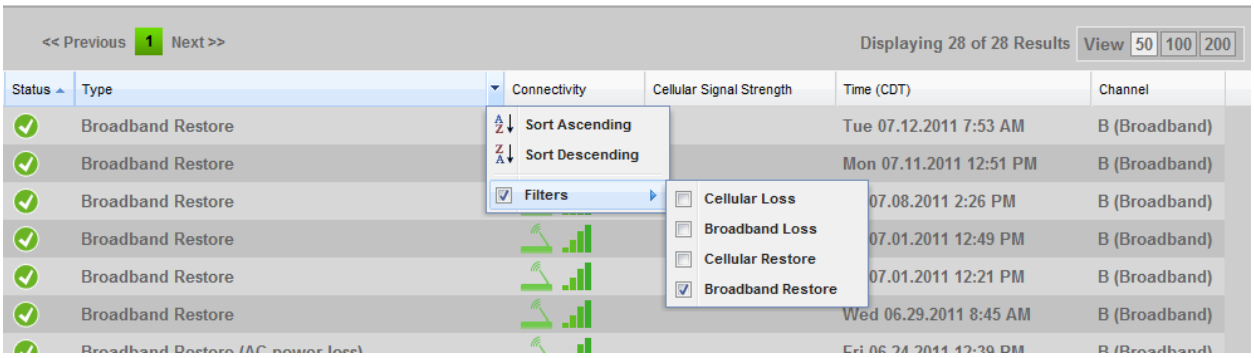


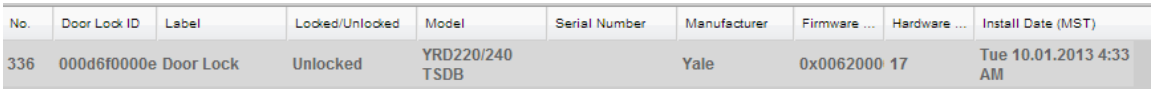
Table 36: Connectivity Report

Column	Description
	The touchscreen and system servers have at least some connectivity by either broadband or cellular
	The touchscreen and system servers have no connectivity at this time
Type	❑ Broadband Loss ❑ Broadband Restore ❑ Cellular Loss ❑ Cellular Restore

Column	Description	
Connectivity		Broadband connected
		Broadband not connected
		Cellular connected
		Cellular not connected
		Cellular is down in one direction
Cellular Signal Strength	The strength of the cellular signal, if known. Other possible values are ❑ **NA-TS** – touchscreen could not determine the signal strength. ❑ **NA-BB** - Signal strength could not be sent because the touchscreen is completely offline.	
Time	Time/date that the connectivity change occurred. The account's time zone is displayed in the column title, such as CDT for "Central Daylight Savings Time".	
Channel	Method by which the connectivity change was reported: **B** (Broadband) touchscreen reported the connectivity outage over broadband (cellular down). **C** (Cellular) touchscreen reported the connectivity outage over cellular (broadband down). **S** (System) The system servers reported the connectivity outage.	

8.3.3 Door Locks Report

The Door Locks report displays the details of the door lock devices currently paired with the CPE and the events reported by the devices.



No.	Door Lock ID	Label	Locked/Unlocked	Model	Serial Number	Manufacturer	Firmware ...	Hardware ...	Install Date (MST)
336	000d6f0000e	Door Lock	Unlocked	YRD220/240 TSDB		Yale	0x0062000	17	Tue 10.01.2013 4:33 AM

Table 37: Door Locks Report

Table	Description
No.	Database ID for each door lock device.
Door Lock ID	Unique ID assigned to the device.
Label	Name of the device given by the customer.
Locked/Unlocked	Whether the device is currently "locked" or "unlocked".
Model	Model number of the device.

Table	Description
Serial Number	Serial number of the device.
Manufacturer	The manufacturer of the device.
Firmware Version	Firmware version of the device.
Hardware Version	The revision number for the device.
Install Date	Timestamp indicating when the door lock was installed.

The Door Lock Events report displays the most recent state changes for the door locks paired with the CPE.

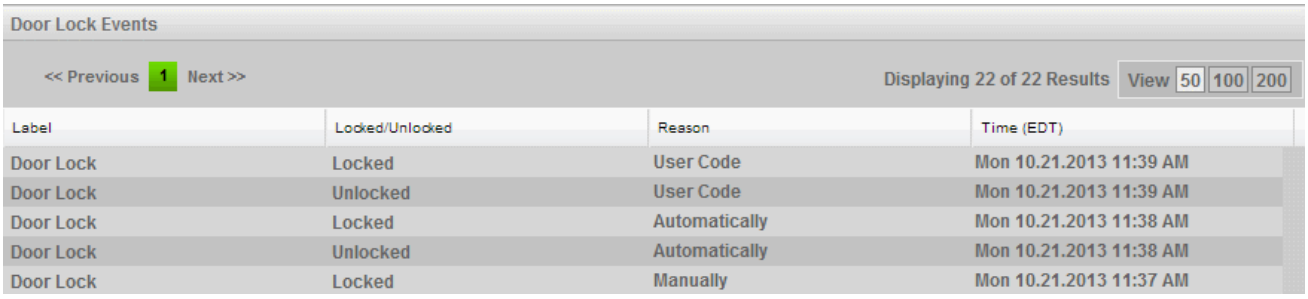


Table 38: Door Lock Events Report

Column	Description
Label	Name of the device given by the customer.
Locked/Unlocked	Whether the door lock was locked or unlocked.
Reason	Indicates how the door lock was locked/unlocked: ❑ User Code - number-pad on the lock used ❑ Manually - key or knob used ❑ Automatically - via a rule
Time	Date/time that the change occurred.

8.3.4 Lights Report

The Lights report displays the details of the lighting devices currently paired with the CPE and the events reported by the devices.

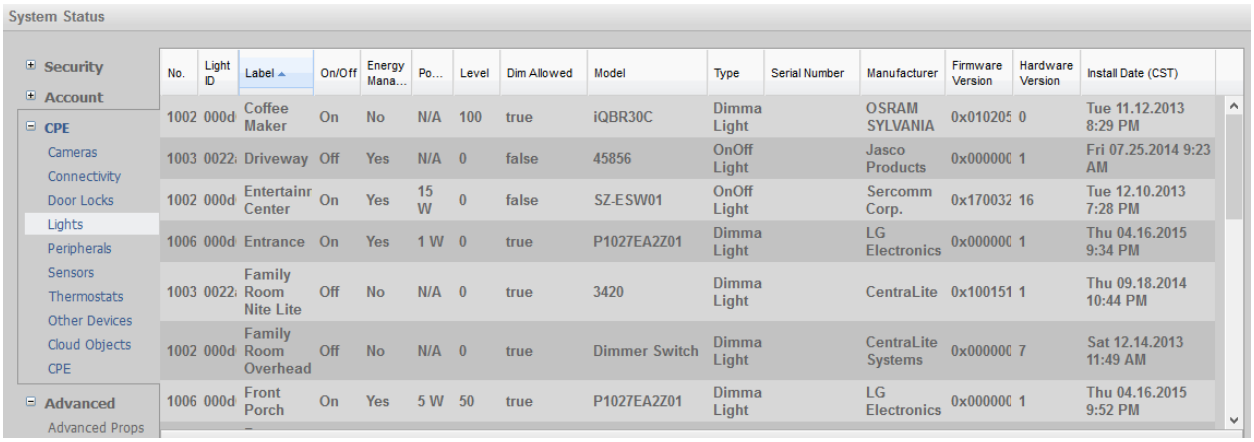


Table 39: Lights Device Report

Table	Description	
No.	Database ID for each light device.	
Light ID	Unique ID assigned to the device.	
Label	Name of the device that is modifiable by the customer.	
On/Off	Whether the light is currently turned on or off (continues to communicate with CPE either way).	
Energy Management	Whether the device is capable of reporting the energy usage of the device plugged in to the lighting device.	
Power	The wattage being used by the device plugged in to the lighting device if Energy Management = Yes.	
Level	The current dimming level (in percentage) of the device. For non-dimmable lights, the levels are only 100 or 0.	
Dim Allowed	true	Dimming capability is available and turned on.
	false	Dimming capability is not available or turned off.
Model	The device model number, if available	
Type	Whether the light is dimmable or not.	
Serial Number	The device serial number, if available	
Manufacturer	The manufacturer of the device, if available.	
Firmware Version	Firmware version of the light device.	

Table	Description
Hardware Version	The revision number of the device, if available.
Install Date	Timestamp indicating when the light was installed.

The Lighting Events report displays the changes in state, power, or level the lighting devices report.

Table 40: Lighting Events Report

Column	Description
Label	Name of the device that is modifiable by the customer.
On/Off	Whether, after the change, the light was off or on.
Power	The wattage being used by the device plugged in to the lighting device.
Level	Dimming level after the change (100 = brightest, 0= totally dark); Note: the light can still be On, even if the dimming level is 0.
Time	Date/time that the change occurred.

8.3.5 Peripherals Report

This report displays the key pads, key fobs, panel interface modules, and other peripherals paired with the touchscreen. It also displays whether there is trouble being reported for each peripheral.

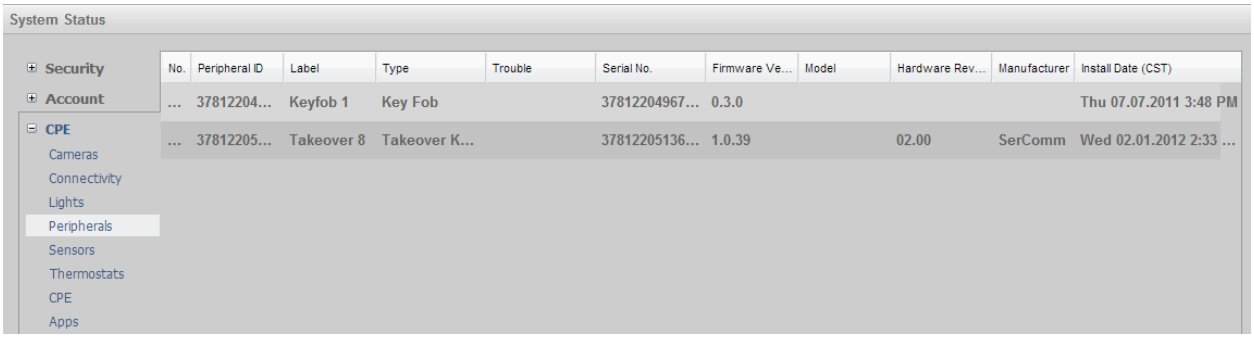


Table 41: Peripherals Report

Column	Description
No.	System database number assigned to the peripheral
Peripheral ID	Unique identifier assigned to the key pad or key fob by the touchscreen.
Label	The name assigned to the peripheral by the customer. This includes gateways and routers.
Type	The type of peripheral.
Trouble	The row is highlighted if the peripheral is currently reporting a problem. Click  to display a pop-up that details the current problem.

Column	Description
Serial No.	Serial number for the peripheral
Firmware Version	Firmware version of the peripheral.
Model	The model name of the peripheral
Hardware Revision	The revision of the peripheral
Manufacturer	The peripheral's manufacturer
Install Date	Timestamp indicating when the peripheral was installed.

8.3.6 Sensors Report

This report lists all the sensors that are currently monitored by the account touchscreen.

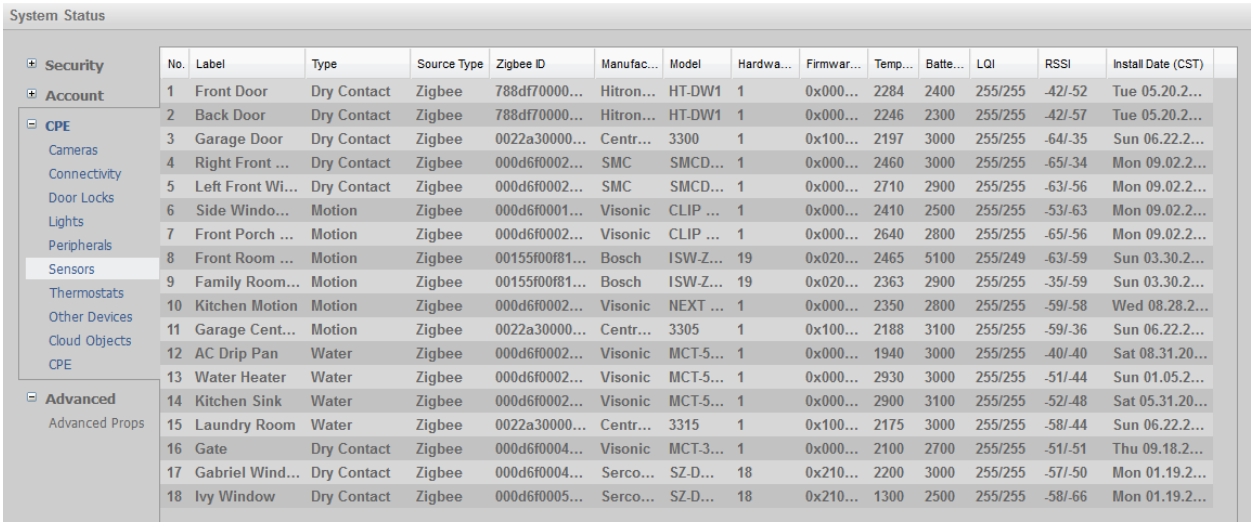


Table 42: Sensors Report

Column	Description
No.	Number assigned to the zone.
Label	Label assigned to the zone by the customer.
Type	Type of sensor.
Source Type	Only ZigBee at this time.
Zigbee ID	ZigBee radio ID of the sensor.
Manufacturer	The manufacturer of the sensor
Model	Model name
Hardware Version	Hardware version of the sensor
Firmware Version	Firmware version of the sensor.
Temperature	The temperature, in Celsius, times 100.

Column	Description
Battery Voltage	The battery's voltage, times 1000
LQI	Link quality indicator. The value indicates the near/far signal
RSSI	Received signal strength indicator. The value indicates the near/far RF
Install Date	Timestamp indicating when the sensor was installed.

8.3.7 Thermostats Report

The Thermostats report displays the details of the thermostats currently paired with the CPE and the changes reported by the thermostats.

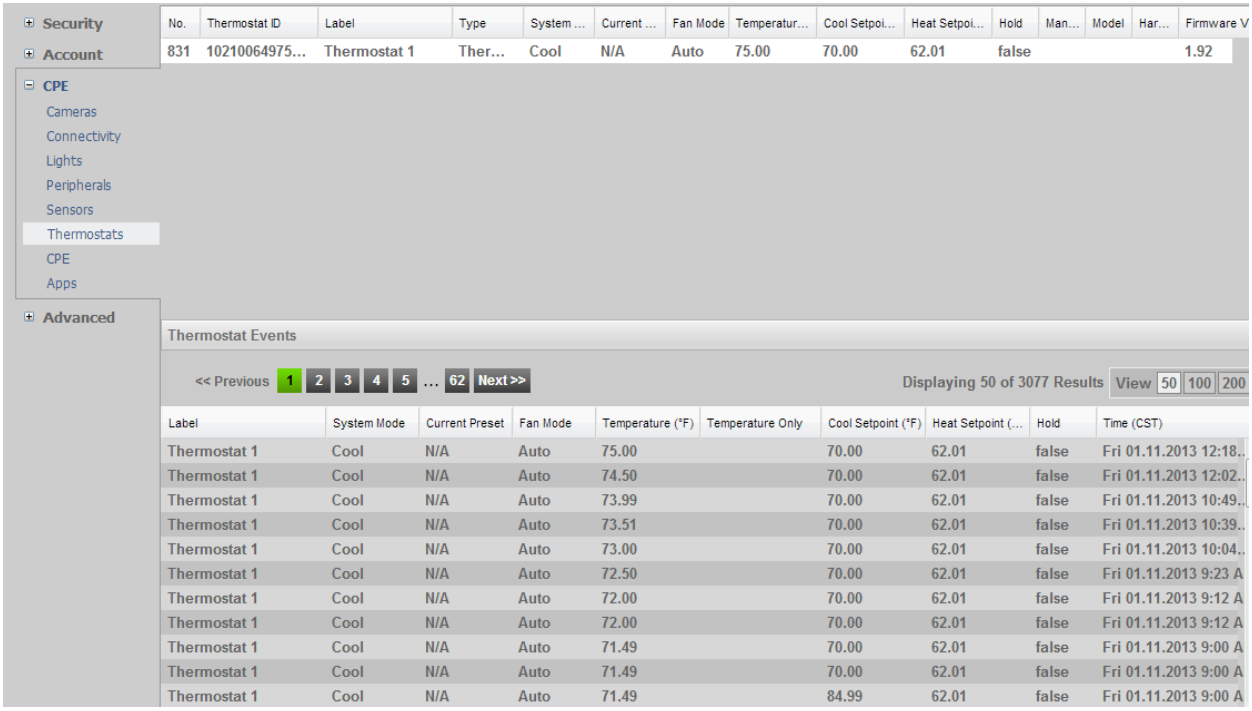
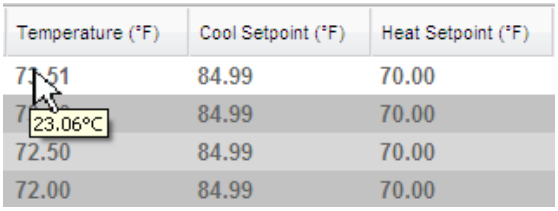


Table 43: Thermostats Device Report

Column	Description
No.	Database ID for each thermostat device.
Thermostat ID	Unique ID for the device.
Label	Name of the device that is modifiable by the customer.
System Mode	Heat
	Cool
Current Preset	Used by radiator valves
Fan Mode	Fan setting, on, off, or auto.

Column	Description	
Temperature	Current ambient temperature measured by the thermostat device. Temperatures are presented in Fahrenheit. Hover the cursor over a temperature to display the value in Celsius. 	
Cool Setpoint	The target temperature set when the system is in Cool mode.	
Heat Setpoint	The target temperature set when the system is in Heat mode.	
Hold	true	The system maintains the current mode and set point without regard to the programming on the device.
	false	When the temperature reaches the set point, it will return to programming mode and set point level for the device.
Manufacturer	The company that manufactured the thermostat	
Model	The model number of the thermostat	
Hardware Revision	Hardware version of the thermostat	
Firmware Version	Firmware version of the thermostat.	

The Thermostats Events report displays the changes reported by the thermostat(s).

Table 44: Thermostats Events Report

Column	Description
Label	Name of the device that is modifiable by the customer.
System Mode	Thermostat mode (Heat or Cool) at the end of the state change.
Current Preset	Used by radiator valves
Fan Mode	On, off, or auto.
Temperature	Ambient temperature reported by the thermostat.
Temperature Only	The event indicates a change in temperature.
Cool Setpoint	The target temperature set when the system is in Cool mode.
Heat Setpoint	The target temperature set when the system is in Heat mode.
Hold	Hold setting (true/false).
Time	Time/date of the event.

8.3.8 Other Devices Report

This report is reserved for future use.

8.3.9 Cloud Objects Report

This report lists details about third-party integrations.

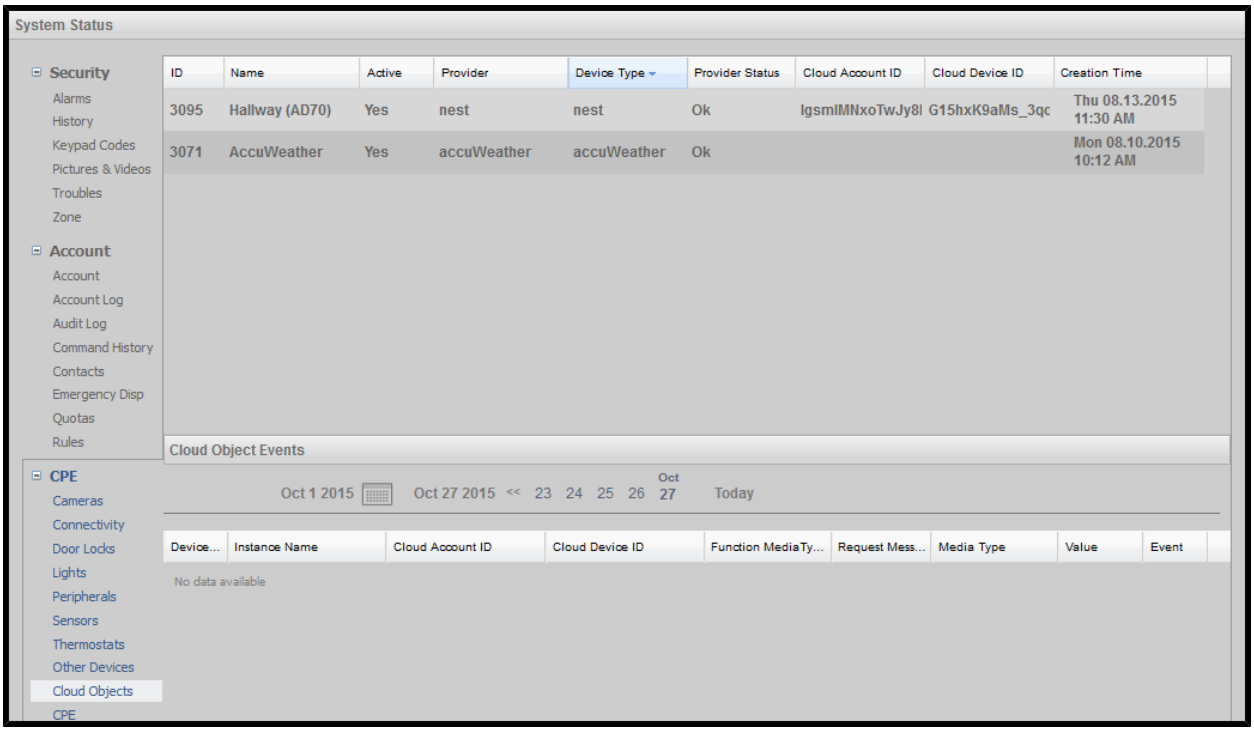


Table 45: Cloud Objects Report

Column	Description
ID	Device ID
Name	The label for the object defined by the subscriber
Active	Whether the object/partner is active
Provider	The name of the partner
Device Type	Partner description of the device/service
Provider Status	Ok or offline
Cloud Account ID	The subscriber's third-party account ID, encrypted
Cloud Device ID	Partner-defined device ID
Creation Time	Indicates when the object was created.

Table 46: Cloud Object Events Report

Column	Description
Device ID	Device ID that generated the event

Column	Description
Instance Name	Cloud object name from Cloud Objects Report
Cloud Account ID	The subscriber's third-party account ID, encrypted
Cloud Device ID	Partner-defined device ID
Function Media Type	Cloud object event
Request Message ID	ID of the event
Media Type	The media type of the object
Value	Partner defined
Event	Description of the event

8.3.10 CPE Report

This report details the information about the account touchscreen or hub.

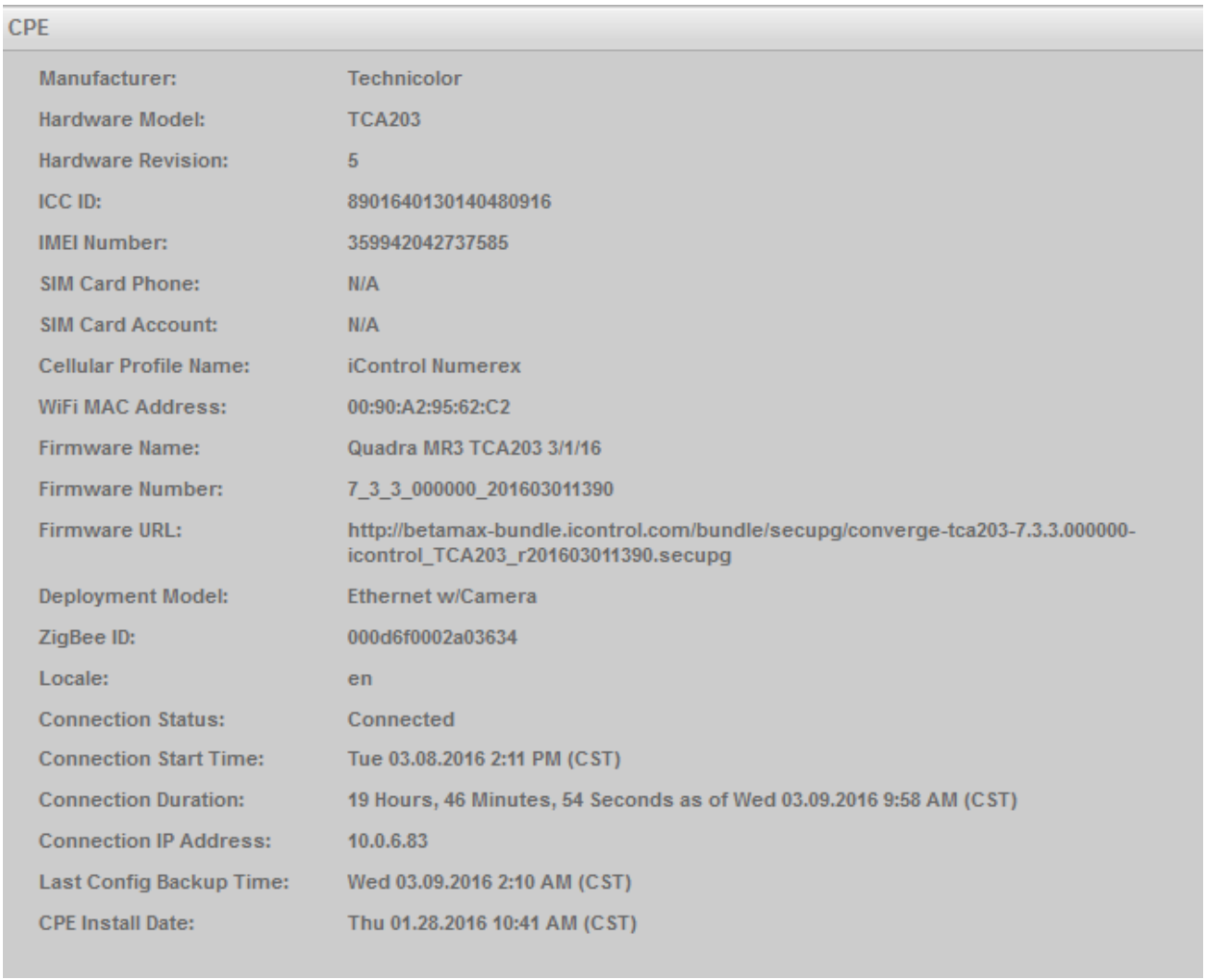


Table 47: CPE Report

Column	Description	
Manufacturer	Manufacturer of the CPE device.	
Hardware Model	Model ID of the CPE hardware	
Hardware Revision	Revision code of the CPE.	
ICC ID	Unique ID for the SIM card used by the touchscreen cellular device. (Converge only)	
IMEI Number	Unique ID of the cellular device that the touchscreen uses to connect to the cellular network. (Converge only)	
SIM Card Phone	Phone number assigned to the touchscreen's SIM card for two-way voice communication through the touchscreen. (Converge only)	Note: Two-way voice communication is managed from the `cellular.twoWayVoice.enabled` Tier Property.
SIM Card Account	Account number that the cellular service provider associates with the touchscreen's SIM card for two-way voice communication through the touchscreen. (Converge only)	
Cellular Profile Name	This value identifies a particular cellular account and its level of service. (Converge only)	
Wi-Fi MAC Address	Unique Wi-Fi identifier assigned to the device.	
Firmware Name	Name for the current CPE firmware version	
Firmware Number	Unique ID for the current firmware version	
Firmware URL	Download location of the current firmware version.	
Deployment Model	Current CPE Information. This value is also displayed at the top of the Account Information screen.	
ZigBee ID	ZigBee module ID, which is used to communicate with sensors and peripherals by radio signal	
Locale	Language version for the CPE; en = English	
Connection Status	Connected or Disconnected	
Connection Start Time	The date and time the CPE connected to the server.	
Connection Duration	The total connected time, calculated from the Connection Start Time	

Column	Description
Connection IP Address	The server IP address
Last Config Backup Time	Date/time that the CPE device settings were backed up to the system servers.
CPE Install Date	Timestamp indicating when the device was installed.

8.3.11 Apps Report (Converge Only)

This report lists the apps currently installed to the account touchscreen.

Click the expander icon (+) next to an app to display properties associated with the app, if they are available.

Apps can be hosted anywhere on in the Internet. They can be created and maintained by third-parties.

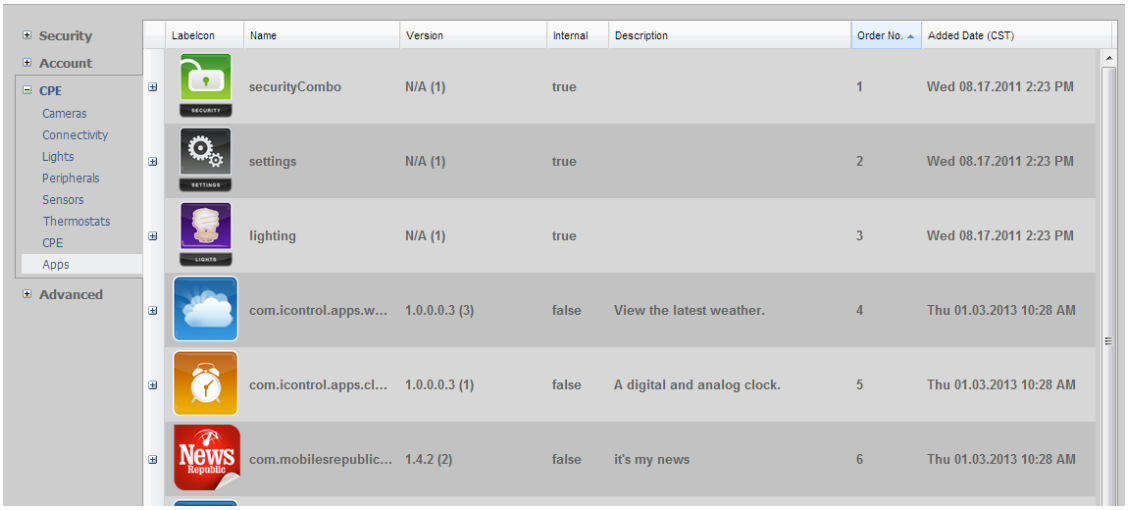


Table 48: Apps Report

Column	Description	
Labelcon	Picture for the app displayed in the touchscreen and Subscriber Portal.	
Name	Database name for the app.	
Version	Version number for the app installed on the touchscreen.	
Internal	true	App is maintained by Icontrol.
	false	App is maintained by a third-party.
Description	A short description of the purpose of the app.	
Order No.	The order in which the app is displayed on the touchscreen.	
Added Date	Date/time the app was added to the touchscreen.	

8.4 Advanced Group Reports

This group is intended to collect reports related to operations only available to Tier 2 Support and above. Currently the only report in this group is the Advanced Properties report.

8.4.1 Advanced Properties Report

This report lists properties that are available for diagnostic purposes.

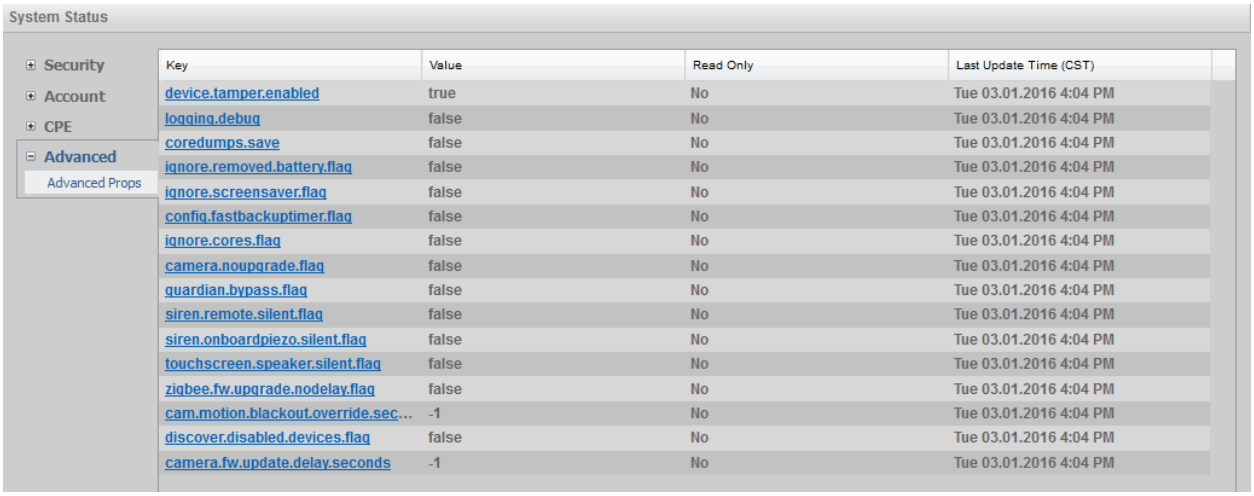


Table 49: Advanced Properties Report

Column	Description
Key	Name of the property
Value	"false" if the property is turned off "true" if the property is turned on
Read Only	<null> if the property value cannot be modified "yes" if the property value can be modified
Last Update Time	Time/date that the property value was last turned on or off. The account's time zone is displayed in the column title, such as CDT for "Central Daylight Saving Time".

IMPORTANT: Consult a supervisor or Icontrol Networks representative prior to changing the value of any key listed below.

Table 50: Advanced Property Keys

Key	Description	Default Value	Requires Rebooting CPE to Enable?
cam.motion.blackout.override.seconds	Set to an integer value, in seconds, to override the default camera motion blackout of three minutes.	-1	Yes
camera.fw.update.delay.seconds	Set to an integer value, in seconds, to override the camera firmware upgrade delay value.	-1	Yes
camera.noupgrade.flag	Set to "true" to keep cameras at the version of firmware they currently have, instead of upgrading if a new version is available.	False	No, but the property must be set prior to the first camera upgrade attempt.
config.fastbackuptimer.flag	Set to "true" to have the backup timer use minutes instead of hours when waiting to upload the CPE configuration file (default time is random, between 1 and 12).	False	Yes
coredumps.save	Set to "true" to have the CPE save the current state of the device in the event of a crash or if the device becomes unresponsive. The "core dump" is automatically uploaded (if possible) to the server for future further analysis.	False	No
device.tamper.enabled*	Set to "false" to suppress the touchscreen "System Tampered" trouble.	True	Yes
discover.disabled.devices.flag	Set to "true" to enable the CPE to discover and pair devices that are already in the database but have been disabled.	False	No
guardian.bypass.flag	Set to "true" to bypass the ZigbeeService Guardian on the touchscreen.	False	Yes
ignore.cores.flag	Set to "true" to prevent core/anr/tombstone monitoring and the CPE from uploading and deleting debug files automatically.	False	Yes
ignore.removed.battery.flag	Set to "true" to suppress the touchscreen "Battery Removed" trouble.	False	No

Key	Description	Default Value	Requires Rebooting CPE to Enable?
ignore.screensaver.flag	Set to "true" to turn off the screensaver on the touchscreen.	False	No
logging.debug	Set to "true" to have the CPE log diagnostic events at the debug level.	False	No
pwrmon.enabled	Turn on (true) to enable the power monitoring feature. **Note:** SMC P5 touchscreens only	False	No
siren.onboardpiezo.silent.flag	Set to "true" to mute the touchscreen piezo during an alarm.	False	Yes
siren.remote.silent.flag	Set to "true" to mute a remote siren during an alarm. If a touchscreen does not have a remote siren paired with it, this property does not apply.	False	Yes
sshd.enabled	Turn on (true) to have the touchscreen allow SSH tunneling in to the device. **Note:** SMC P5 touchscreens only	True	No
telemetry.fast.upload.timer.flag	Set to "true" to reduce the telemetry gathering random upload delay from up to 1 hour to up to 1 minute.	False	No
touchscreen.speaker.silent.flag	Set to "true" to mute the touchscreen speaker.	False	Yes
zigbee.fw.upgrade.nodelay.flag	Set to "true" to schedule firmware upgrades immediately after a device descriptor update notification instead of waiting the default delay of 2 hours after boot or after device descriptor list updates.	False	No

* The `device.tamper.enabled` CPE and server properties must both be set to "**true**" for the tamper trouble and tamper trouble cleared events to be sent to the server. For more information on server properties, see the "server.properties" section in *System Operations Guide*.

Note: If the touchscreen is in a tampered state when the CPE or server property is set to "**false**", the tamper clear event will not be sent when the touchscreen becomes no longer tampered. If the server property is modified, the touchscreen must be rebooted to clear the trouble from the touchscreen and user interfaces. If the CPE property is modified, the trouble will clear from the touchscreen, but it will not clear from the user interfaces until the touchscreen is rebooted.

9 Troubleshooting Operations

The following operations are commonly used by Customer Care representatives to aid customers in resolving problems.

- Reboot a touchscreen remotely
- Reboot a security router remotely
- Reboot a camera remotely
- Adjust the Wi-Fi channel for a security router or Touchstone hub (see page 170)
- VNC to a touchscreen to operate it remotely(see page 176)
- Take a screen capture of the current touchscreen view (see page 166)
- Access the diagnostic file of a touchscreen (see page 163)
- Create SSH tunnel to a touchscreen (see page 168)
- Mark an account for RMA (see page 172)

9.1 Rebooting a CPE Remotely

From the Management Portal, users can remotely reboot an account's CPE.

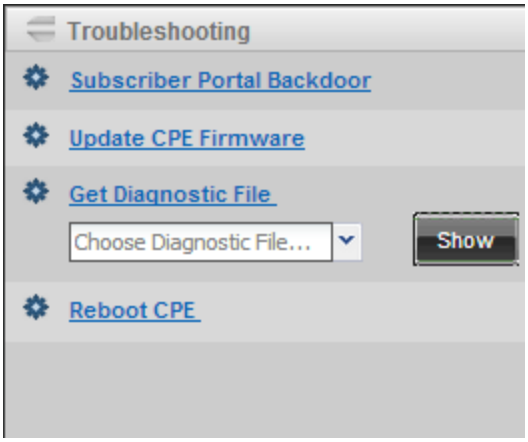
IMPORTANT: Do not reboot a CPE if the CPE is armed.

To reboot a CPE remotely:

1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

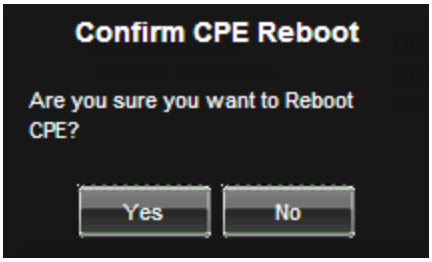
   The Account Information screen is displayed.

2. Open the Troubleshooting menu in the Account Management tools.



3. Click **Reboot CPE**.

   The Management Portal displays a confirmation.



4. Click **Yes**.

   The Reboot CPE option displays a spinning icon to its right until the reboot process is complete.

9.2 Rebooting a Security Router Remotely (Converge only)

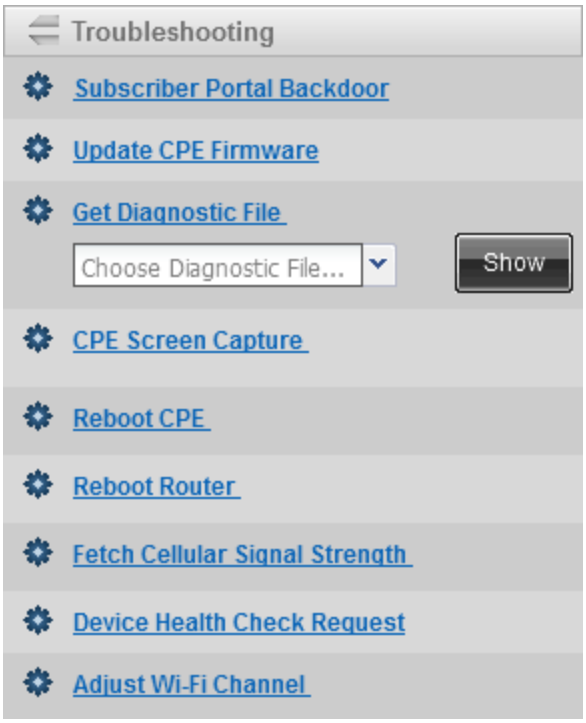
From the Management Portal, users can remotely reboot an account's security router.

To reboot the security router remotely:

1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

2. Open the Troubleshooting menu in the Account Management tools.



3. Click **Reboot Router**.

   The Management Portal displays a confirmation.

4. Click **Yes**.

   The Reboot Router option displays a spinning icon to its right until the reboot process is complete.

9.3 Rebooting a Camera Remotely

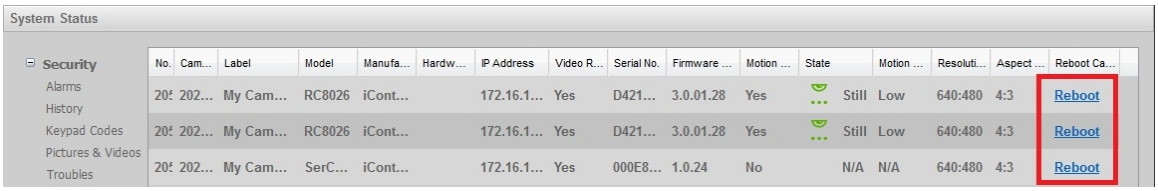
From the Management Portal, users can remotely reboot a camera in a subscriber's home.

To reboot a camera remotely:

1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

2. Navigate to **System Status > CPE > Cameras**.



3. Click on **Reboot** for the camera you wish to reboot.

4. The result of the command is displayed under **System Status > Account > Command History**. However, this does not correspond to the status of the camera. It requires several minutes to reboot and rejoin the network.

9.4 Accessing the Subscriber Portal Backdoor

This tool allows a Management Portal user to access the Subscriber Portal for an account for troubleshooting. The Subscriber Portal Backdoor provides all the privileges of a logged in customer except it does not display captured images or live video.

The following operations are not allowed for the Backdoor:

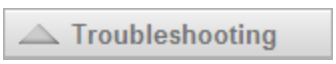
- Door locks cannot be locked or unlocked.
- Zones cannot be turned off (bypassed) or turned on.
- Camera App is not available. Images and video cannot be viewed or manually captured.
- Saved Pictures and videos cannot be accessed, nor is there an option to do so in the History pages.
- Emergency Dispatch options cannot be modified.

To view a subscriber's Subscriber Portal via the Subscriber Portal Backdoor:

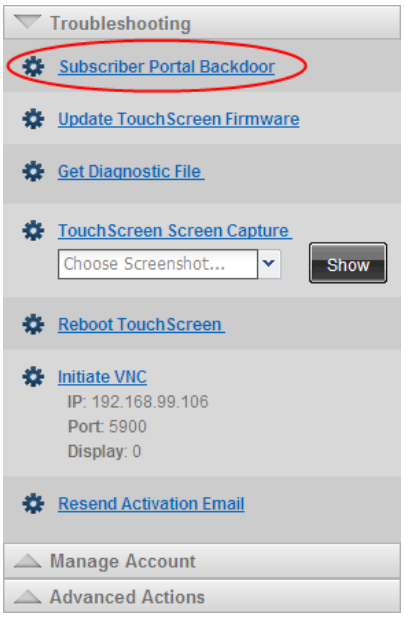
1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

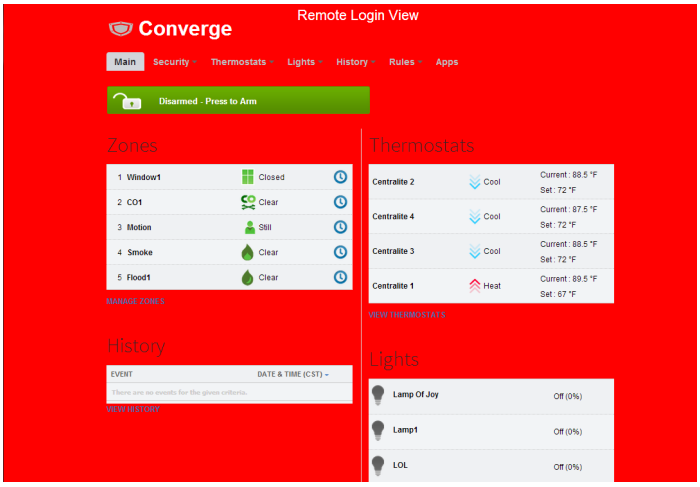
2. Click **Troubleshooting** in the Account Management tools.

3. Click **Subscriber Portal Backdoor**.



The Subscriber Portal for the account is displayed.



The background of the Subscriber Portal is red as a reminder that the information is being viewed via the Subscriber Portal Backdoor.

9.5 Updating the Firmware on a Single Device

You can update the firmware on the touchscreen or hub of a particular customer from the Management portal.

Note: If the user does not have privileges to manage the device firmware, the Management Portal link will not be displayed on the Account Information screen.

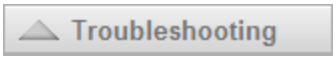
If the subscriber does not have broadband connectivity with the server cluster, the following error message is displayed when they try to update CPE firmware using this method:

To check for a new firmware update for a CPE device from the Management Portal:

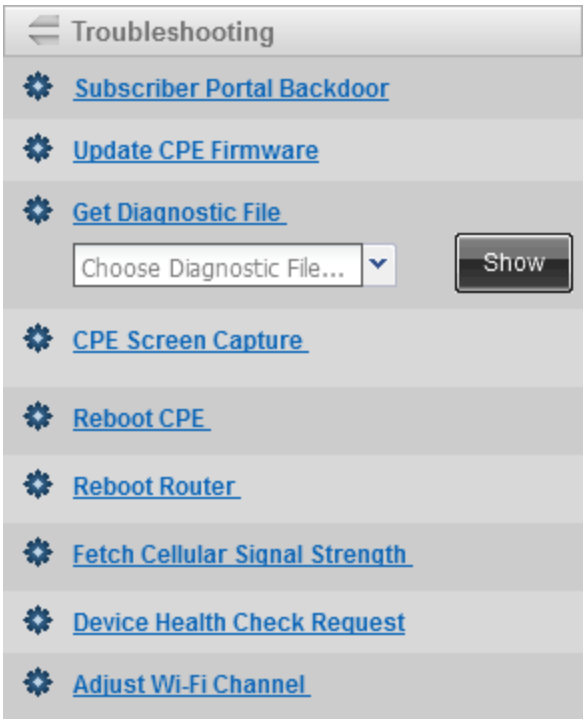
1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

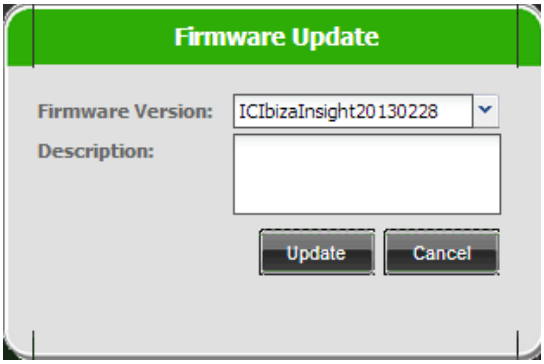
2. Click **Troubleshooting** in the Account Management tools.

3. Click **Update CPE Firmware**.



The Firmware Update dialog is displayed.

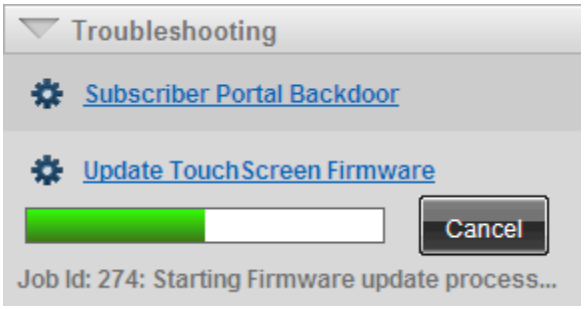


4. Select the firmware version to upgrade to and click Update.
5. An upgrade signal is sent out from the server that a firmware upgrade is available.

   On Converge systems, when the upgrade signal is received, the touchscreen checks its current state:

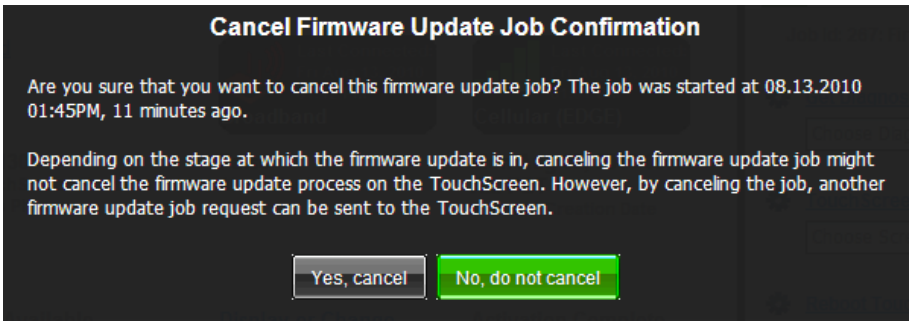
   - If the system is armed, the servers wait until it is disarmed to upgrade the touchscreen. When the system is disarmed, the system waits five minutes before queuing the touch-screen for an update. The time period is configurable by the firmware.waitTimeAfter Tier property. This delay ensures that the firmware update will not occur if the subscriber leaves the premises, forgets something, and disarms the system to temporarily to enter the premises.
   - If unarmed, the touchscreen begins the upgrade process immediately.

The download is started. A progress bar displays under the Update touchscreen Firmware link as the system updates the touchscreen firmware.



6. Click **Cancel** to stop the update process before it is complete.

   The system displays a confirmation dialog before cancelling the update process.



9.6 Accessing the Diagnostic File for a CPE

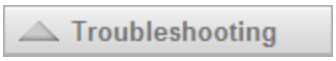
From the Management Portal, users can retrieve the diagnostic file on a CPE.

To view the diagnostic file of a CPE:

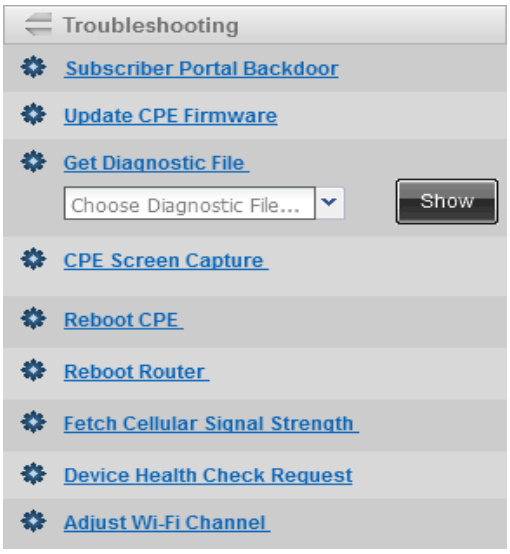
1. Ensure pop-up blocking is turned off for your browser.
2. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

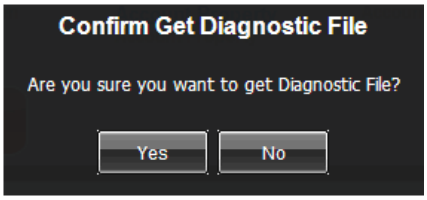
3. Click Troubleshooting in the Account Management tools.



4. Click Get Diagnostic File.



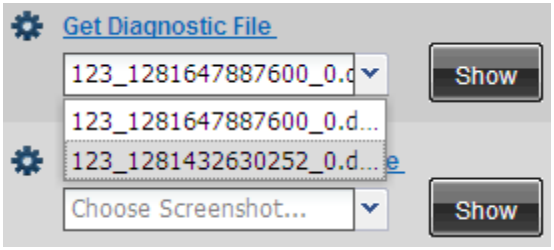
A confirmation is displayed.



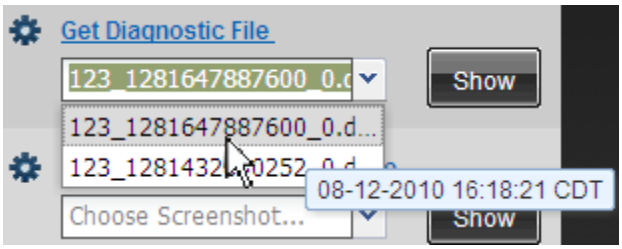
5. Click Yes.

   A new browser is opened to display diagnostic file.

6. To view a previous, recently retrieved diagnostic file, select it from the Get Diagnostic File menu and click **Show**.



7. Hover the cursor over a filename in the menu to view the date/time that diagnostic file was retrieved.



9.6.1 Understanding Diagnostic Files & Core Dump Files

A diagnostic file is generated automatically by the CPE and uploaded to the server when the following occurs:

- A CPE reboot was initiated from the Management Portal.
- A touchscreen reboot was initiated from the Settings app.
- The touchscreen's High Availability Manager (HAM) has initiated a reboot due to a crash of the uc-keypad process.

In addition, when any other important touchscreen process crashes, a diagnostic file and a core dump file of the crashed process are generated by the touchscreen and uploaded to the server.

See Understanding the Diagnostic File/Core Dump File Upload Path in the following subsection for an explanation of the path to which core dump and diagnostic files are uploaded.

If the upload directory has only a diagnostic file for the applicable time frame:

A reboot was initiated from the touchscreen Settings app or the Management Portal, or the HAM initiated a reboot due to the crash of an important process.

If the upload directory has a diagnostic file and a core dump file for the applicable time frame, an important process other than uc-keypad crashed.

Whenever a touchscreen uploads a generated diagnostic file or core dump file, the following alert is displayed on the History Report screen of the account (see "History Report" on page 125 for more information):

"System Trouble—touchscreen Firmware Trouble: Core or Diagnostic File Generated and Saved on Server (dump filename). This can happen when the firmware running on the touchscreen has generated an internal error. Please work with your Icontrol Networks representative for further assistance."

Note: If the dump filenames (such as `3/1/1_17081_0.dmp`) does not display in the parentheses, it means the file is currently being generated. Refresh your browser screen to view the filename.

To customize this message:

1. Add the following property to the custom.properties file:

```
trouble.type.system.software = touchscreen Firmware Trouble:
Core or Diagnostic File Generated and Saved on Server ({0}).
This can happen when the firmware running on the touchscreen has
generated an internal error.  Please work with your Icontrol
representative for further assistance.
```

2. Modify the text as needed.

Note: In this message `{0}` is the dump filename.

9.6.2 Understanding the Diagnostic File/Core Dump File Upload Path

The path where the diagnostic files and core dump files are stored is generated based on the Premises ID of the subscriber of the account. The Premises ID is a unique ID based on the subscriber's address. Files are always saved to the following path:

```
[root]/[some directoryname]/ [some directoryname]/
[some directoryname]/[event id]/[diagnostic file]
```

The directory name is generated in the following way:

1. Based on the Premises ID, the system calculates a SHA1 hash code.

   For example, if the user's Premises ID is 1561, the hash code might be 77cwes90.

2. The system creates a directory path based on the first character of the generated hash code.

3. The system creates a new directory at the generated path based on the Premises ID of the account.

4. The system saves the diagnostic file to the final directory.

   For example, if the Premises ID is 1561 and the generated hash code is 77cwes90, then the files are saved to 7/1561/, where:

   - 7/ is based on the first three characters of the generated hash code
   - 1561 is the Premises ID of the account

9.7 Taking a Screen Capture of a Remote touchscreen (Converge Only)

From the Management Portal, users can take a screen capture of the current screen content on a remote touchscreen. This feature is not available if camera images are currently displayed on the touchscreen.

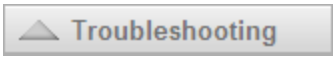
To take a screen capture of a touchscreen's current screen content:

1. Ensure pop-up blocking is turned off for your browser.

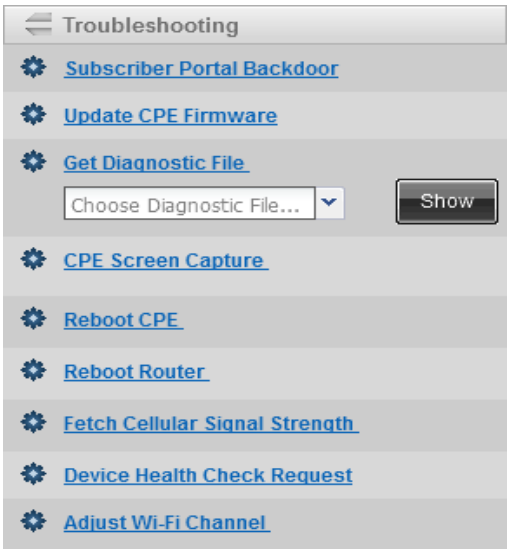
2. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

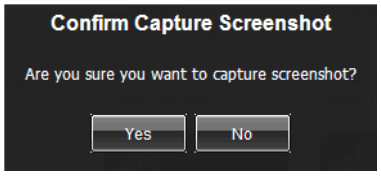
3. Click **Troubleshooting** in the Account Management tools.

4. Click **touchscreen Screen Capture**.



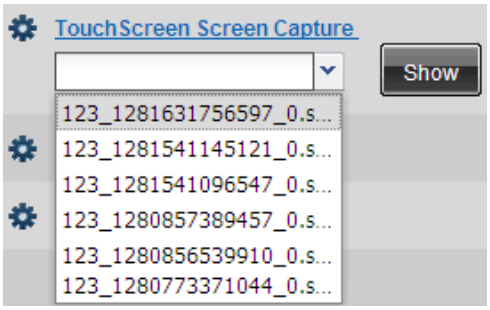
A confirmation is displayed.



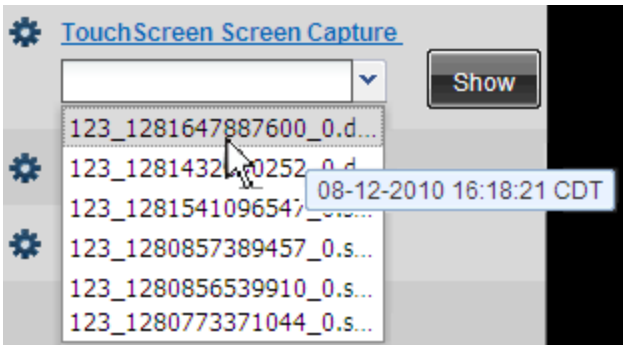
5. Click **Yes**.

   The currently displayed screen contents of the account's touchscreen are captured to a PNG image file. The image file is saved to a Management Portal directory. A new browser is opened to display the captured image.

6. To view a previous, recently saved screen capture, select it from the CPE Screen Capture menu and click Show.



7. Hover the cursor over a file in the menu to view the date/time that the image was captured.



9.8 Determining the Strength of the Cellular Signal (Converge Only)

To display the cellular signal strength of a touchscreen:

1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

2. Click **Fetch Cellular Signal Strength**.

   The strength of the signal and time are displayed.

9.8.1 Resetting the Cellular Connection (Converge SMC P5 Touchscreen Models Only)

If a cellular provider re-provisions the SIM card with a new phone number or upgrades the card so that it supports 2-Way Voice, the cellular modem on the touchscreen must be rebooted.

Note: Repeatedly rebooting the cellular modem will reduce GPRS connectivity.

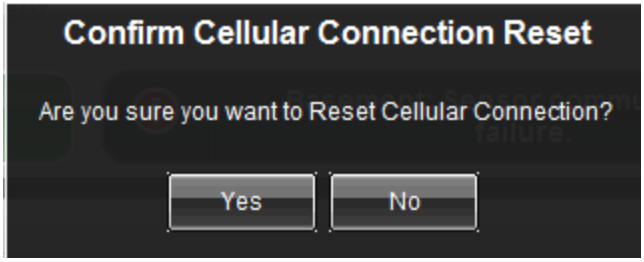
To reset the touchscreen Cellular Connection:

1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

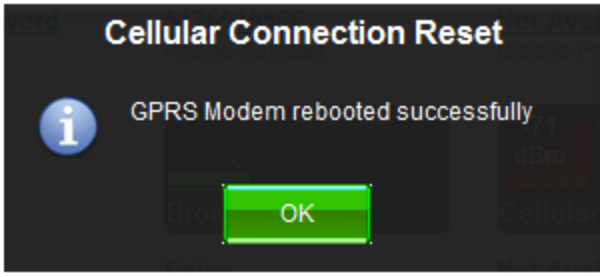
2. Click **Reset Cellular Connection**.

   A confirmation dialog is displayed.



3. Click **Yes** to continue.

   When the modem has rebooted, the following dialog is displayed.



4. Click **OK** to return to the Dashboard.

9.9 Device Health Check Request

A user with Rest Operaton privileges can conduct an overall health check of the device-to-CPE network in subscriber's premise.

A completed device health check includes the following information:

- Timestamp of last update
- Device name
- Device battery status
- Device type: ZigBee or WiFi
- RSSI
- LQI
- Near and far
- Parent

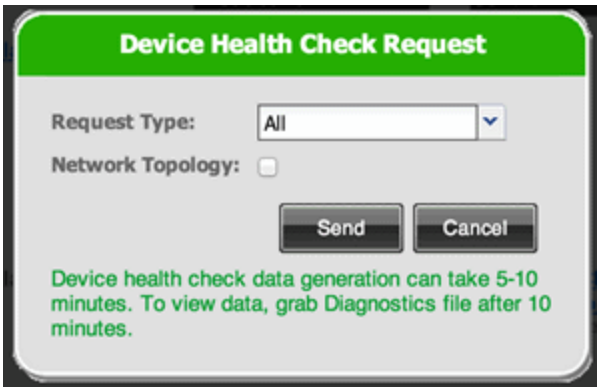
If the user does not have Rest Operator privileges, nothing will happen when he clicks this option.

Unless the CPE build is Lanai or later, the call will be ignored as an unrecognized API.

To perform this operation:

1. In the Management Portal, access the Account Details Information screen of the subscriber.
2. Open the Troubleshooting tab.
3. Click Device Health Check Request.

   The Device Health Check Request dialog is displayed.



4. 4. In the Request Types drop-down, you can choose to get health check data on the entire subscriber system or only on specific elements:
   - All
   - All Wi-Fi
   - All ZigBee
   - Sensors
   - Peripherals
   - Cameras
   - Thermostats
   - Door Looks
   - Relays+ Device
5. Select the Network Topology check box to choose to gather information about the how each device is connected to the CPE, such as:
   - Whether it is communicating directly with the CPE.
   - Whether it is a “child” device, communicating through a repeater device such as a light module (the “parent” of a child device).
6. Click **Send**.

   The premise’s device health and all relevant topology are gathered and stored for viewing in the new diagnostic file.
7. Wait 5 to 10 minutes for the system to gather the requested data.
8. Click **Get Diagnostic File** to generate a new diagnostic file, and access the newly generated health check information.

   The health check information is grouped under config/healthcheck.

9.10 Adjust Wi-Fi Channel

From the Management Portal, the user can scan for a better Wi-Fi channel if a subscriber is having issues with router or camera connectivity.

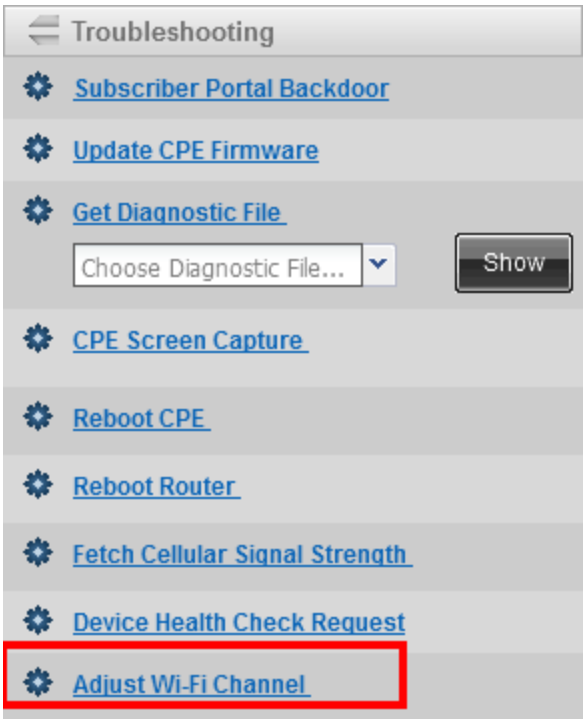
Note: This option will not be available for devices that do not support this feature, i.e. gateways and Wi-Fi clients.

To adjust the Wi-Fi channel of a security router or hub:

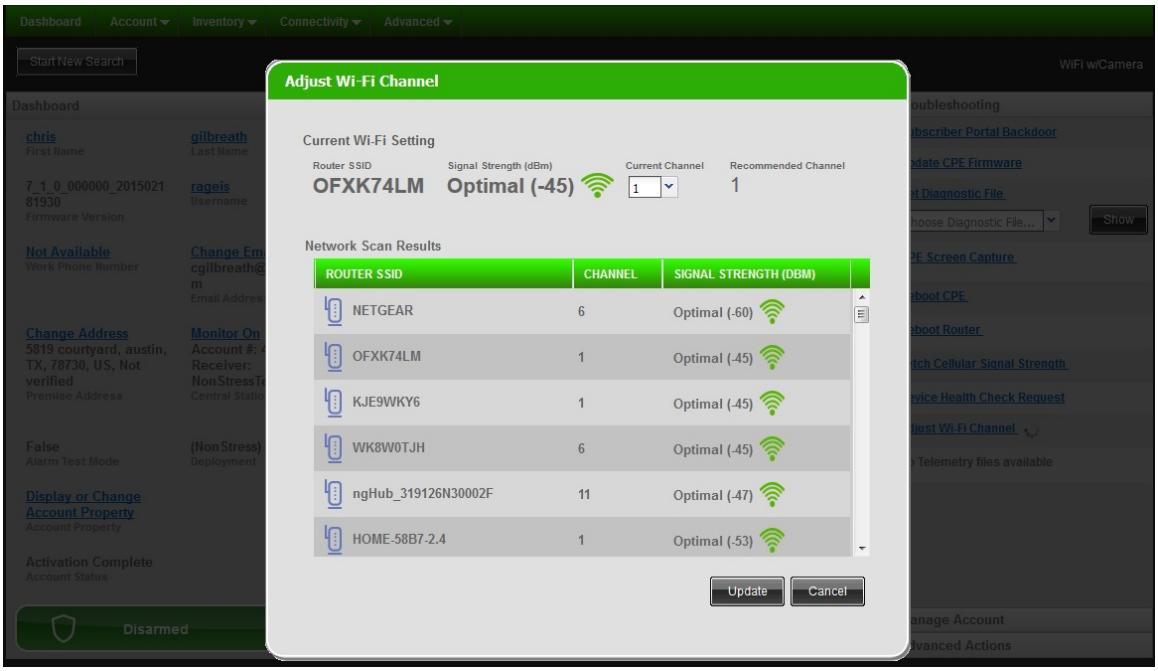
1. Ensure pop-up blocking is turned off for your browser.
2. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

3. In the *Troubleshooting* menu in the *Account Management* tools, click **Adjust Wi-Fi Channel**.



The Adjust Wi-Fi Channel screen pops up.



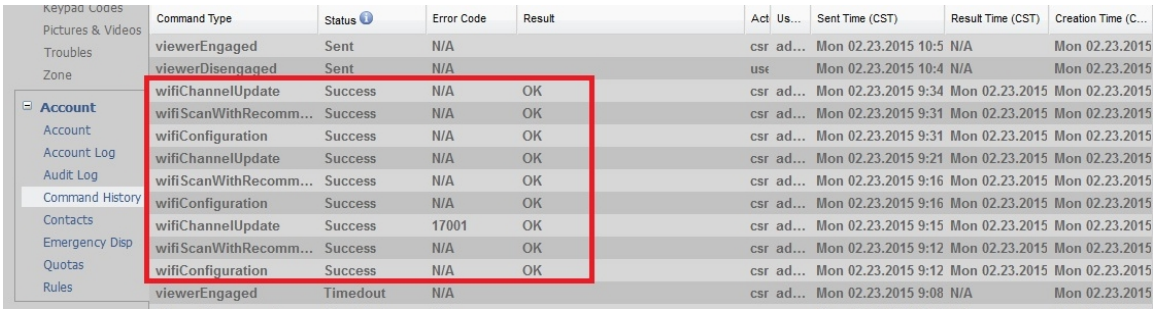
4. The scan returns networks found in the immediate area and displays their signal strength.

   IMPORTANT: If more than 50 networks are found, only the first 50 will be displayed

5. If the scan found a better channel and the *Recommended Channel* is not the *Current Channel*, the user can select the subscriber's *Router SSID* from the *Network Scan Results*, change the *Current Channel* value and click **Update** to apply the change.

   Note: Selecting a different network will result in a failure and the channel will remain the same.

6. The result of the command is displayed under **System Status > Account > Command History**.



9.11 Marking an Account for RMA

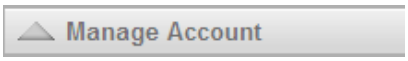
An account that has been marked for Return Material Authorization (RMA) can only have a new CPE device installed. After the new device has been activated for the account, the old CPE can be activated for a different account (after it has gone through a Refurbishment process).

To mark an account for RMA:

1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

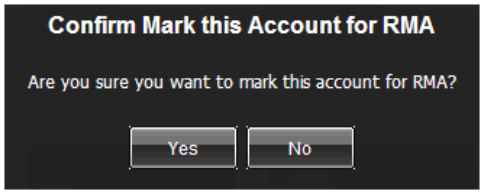
   The Account Information screen is displayed.

2. Open the Manage Account menu in the Account Management tools.



3. Click **Mark this Account for RMA**.

   A confirmation dialog is displayed.



4. Click **Yes**.

   The screen displays the notification Marked this Account for RMA successfully. Instead of a Premises Passphrase, the RMA Activation Code is displayed. The RMA Activation Code is required

for the Installer to activate a new device with this account.

9.12 Secure Shell (SSH) Tunneling to a CPE

Management Portal users can connect to the directory structure of a CPE through an SSH tunnel. The SSH User advanced employee role is needed to perform this procedure. Tunneling into a CPE adds an entry into the account Command History report.

Note: SSH tunneling must enabled for SMC P5 touchscreens by setting the `sshd.enabled` property to "true" under the **System Status > Advanced > Advanced Props** account report.

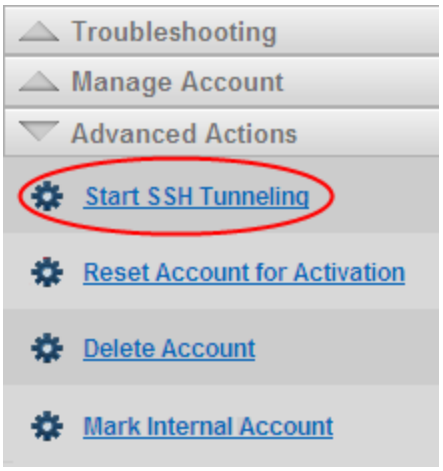
To SSH tunnel to a CPE:

1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

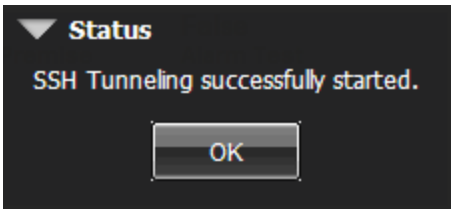
   The Account Information screen is displayed.

2. Open the Advanced Actions menu in the Account Management tools.

   From the Advanced Actions menu, click Start SSH Tunneling to open the CPE to tunnel.

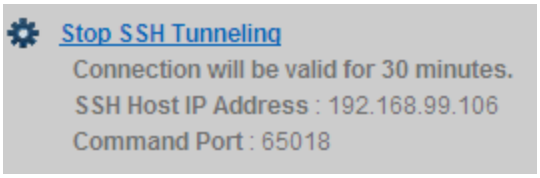


A confirmation is displayed.



3. Click **OK**.

   Beneath the link, the connection information is displayed.



4. Use terminal emulator software (such as PuTTY) to access the CPE with the provided connection information.

   Note: The connection times out automatically after 30 minutes, whether the user started tunneling or not. After the port closes, a new session must be restarted.

9.13 Creating a VNC Connection to a touchscreen (Converge SMC P5 Touch-screens Only)

From the Management Portal, users can initiate a Virtual Network Computing (VNC) connection to a particular touchscreen. A VNC connection allows a Management Portal user to remotely view the screen of a touchscreen device and control it.

The touchscreen must have broadband connectivity to initiate a VNC connection.

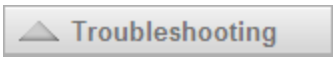
To connect to a touchscreen using VNC:

1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

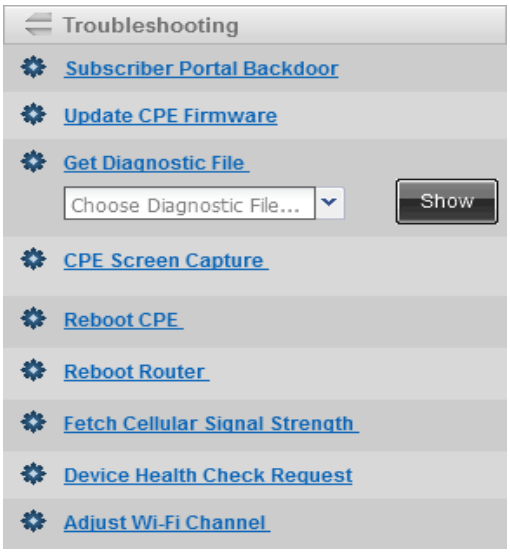
   The Account Information screen is displayed.

2. Note the account's touchscreen Premises Pass Phrase.

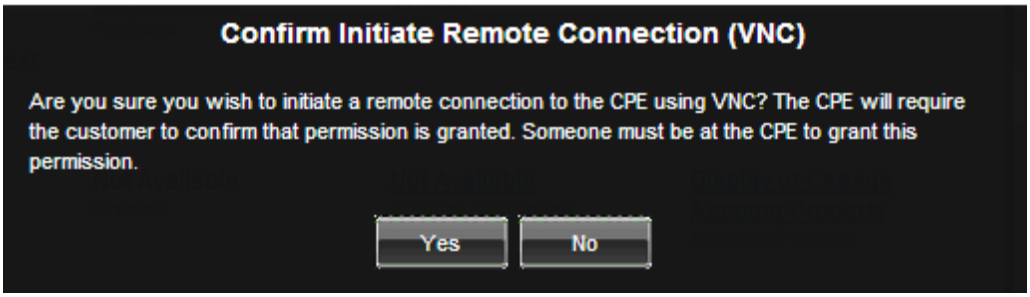
3. Click **Troubleshooting** in the Account Management tools.

4. Click **Initiate VNC**.

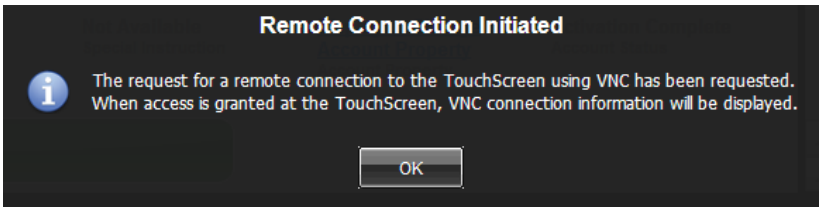
   

   The Management Portal displays a confirmation for whether you actually want to perform this procedure.



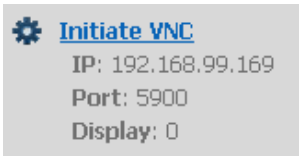
5. Click **Yes** to begin the process of connecting to the touchscreen by VNC.

   The system reports that it has determined the connection settings necessary connect to the touchscreen by VNC.



6. Click **OK**.

   The VNC connection settings are displayed under the Initiate VNC link.



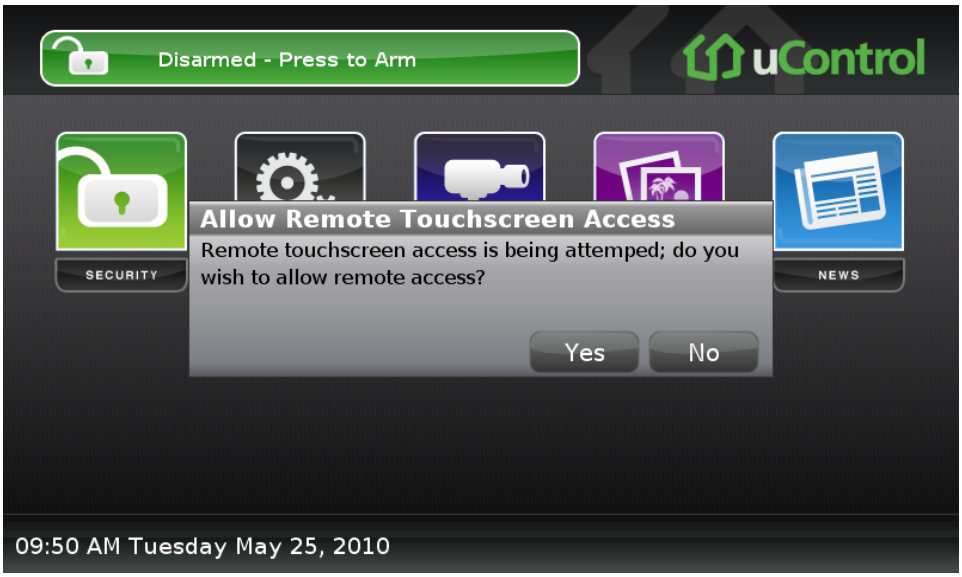
7. Use a VNC viewer application to connect to the touchscreen using the provided IP and port.

   Note: When a password is required by your VNC viewer application, use the touchscreen Premises Pass Phrase.

   Note: The VNC server port, located in the touchscreen, remains occupied until you attempt to establish a VNC connection and that attempt is either denied or accepted.
   If you click Initiate VNC a second time without attempting to establish a connection, the system displays the following error:

   To resolve this error, attempt to connect to the touchscreen using the settings provided previously. If you do not have those settings, reboot the touchscreen.

   The remote touchscreen device displays a confirmation screen.



The customer taps **Yes** to allow the Management Portal user access to the touchscreen device.

The VNC viewer displays a real-time view of the touchscreen's screen contents. The apps and tools are accessed with mouse-clicks in the same way they would be accessed directly by touching.

Note: Camera content is not displayed through a VNC connection. If a touchscreen is on a screen with a camera, then the whole VNC screen becomes gray. The customer must change to a different screen for the VNC session to display.

9.14 Enabling/Disabling Logging to the Server

You can set a touchscreen to log all communications between the touchscreen and the server. This information is written to the server log file and can be used for debugging. When touchscreen logging is enabled, the system writes entries into the log that contain the string SingleDeviceDebugger.

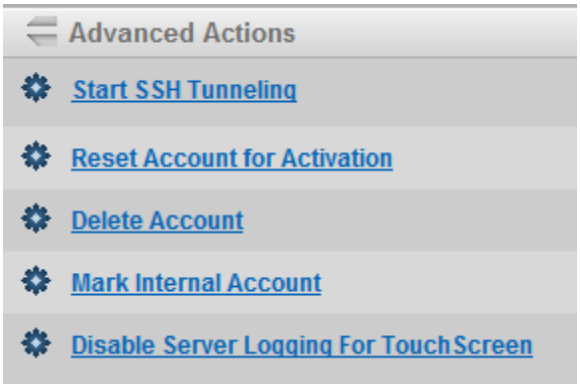
Refer to *Converge System Architecture Guide* or *Touchstone System Architecture Guide* for more information about server logging.

To turn on/off logging to the server:

1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

2. Open the Advanced Actions menu in the Account Management tools.



3. Click **Enable Server Logging For touchscreen** to begin logging or **Disable Server Logging For touchscreen** to turn off logging. When you click the link, the text changes accordingly.

9.15 Enabling/Disabling Debug Logging on a CPE

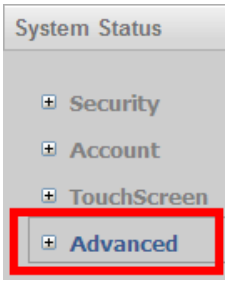
You can set a CPE to log every action between it and the system servers.

To turn on/off debug logging on a CPE:

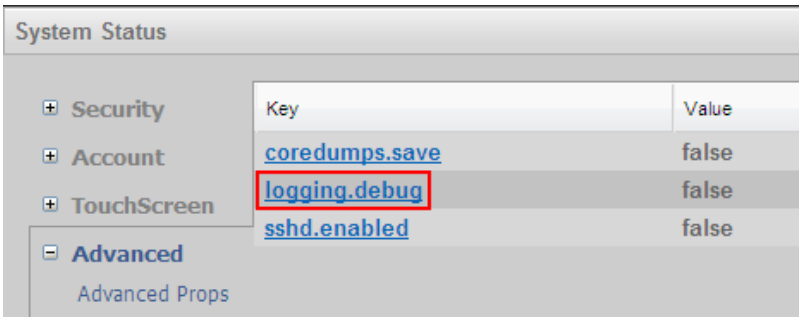
1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

   The Account Information screen is displayed.

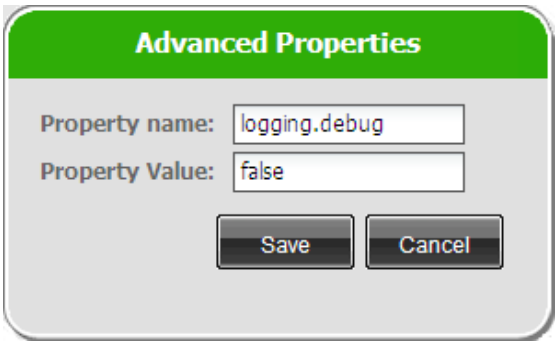
2. In the System Status reports, select the Advanced group to display the Advanced Properties report.



3. Click **logging.debug**.



The Advanced Properties dialog for logging.debug property is displayed.



4. In the Property Value field, type `true` to turn on debug logging.
   Type false to turn off debug logging.
5. Click **Save**.

   The debug logging state is changed.

9.16 Enabling/Disabling Saving Core Dumps on a CPE

You can set a touchscreen to save a recorded state of its working memory in the event of a crash or freeze.

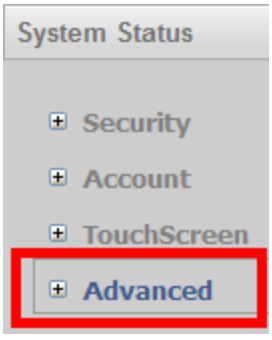
Before activation, core dumps are saved on the touchscreen at `/opt/ucontrol/activationDumps/`.

After activation, core dumps are saved on the system servers in the directory configured in the `custom.properties` file.

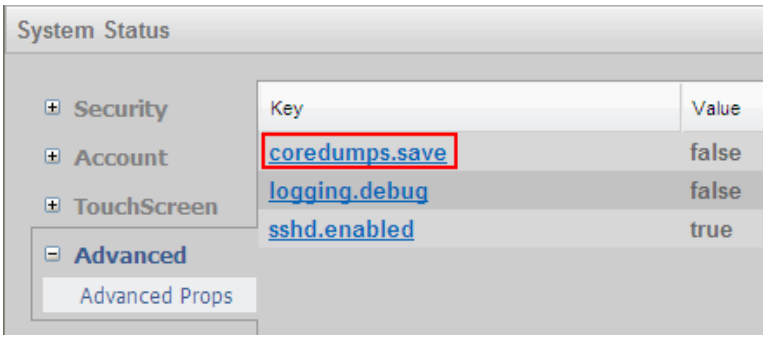
To turn on/off core dump saving on a touchscreen:

1. Query for an Activated account as described in "Monitoring the Status of an Account" on page 100.

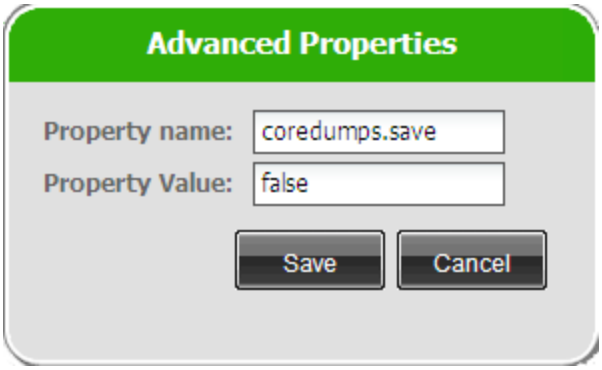
   The Account Information screen is displayed.
2. In the System Status reports, select the Advanced group to display the Advanced Properties report.



3. Click **coredumps.save**.



The Advanced Properties dialog for coredumps.save property is displayed.



4. In the Property Value field, type `true` to turn on core dump saving.
   Type `false` to turn off core dump saving.
5. Click **Save**.

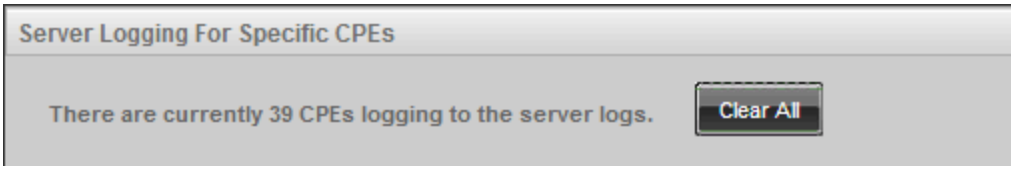
   The core dump save state is changed.

10 Managing Log Levels

The Log Level management portion of this screen is no longer accessible from the Management Portal main menu. Instead, that portion of the screen and its functions are accessible from the following URL:

`https://<host>/ICHealthCheck/manageLogLevel`

The Server Logging for Specific CPEs section is still accessible from the Main Menu by selecting **Advanced > Manage CPE Logging**. It still lists the number of devices that are currently writing to the server log. Click the **Clear All** button to turn off logging for all CPEs.



11 Monitoring Tools

The system provides several tools for monitoring the status of the server and its processes.

11.1 ICHealthCheck Service

The ICHealthCheck summary page provides a set of queries that determine the status of the server, database, accounts and other aspects of the Icontrol common architecture.

You must have a login created and managed through the Management Portal with a systemMonitor role to access this tool.

Use the following URL to access the summary page:

```
https://<host>/mp/ICHealthCheckService?method=ichealthcheck.getSummaryPage
```

See the *System Operations Guide* for more information about the ICHealthCheck service.

11.2 Server Status Check List

The Server Status Check List page provides a summary of key components of the server, including server IP, build number, firmware versions, whitelist URLs, groups, server properties, and more.

You must have a login created and managed through the Management Portal with the admin role to access this tool.

Use the following URL to acccess this page:

```
https://<host>/mp/getServerStatus.action
```