cradlepoint NetCloud™

User Manual

cradlepoint.com

VERSION HISTORY

Version	Date	Description/Notes	Author
1.0	August 31, 2017	First full version	Pat Burroughs
2.0	October 30, 2017	Major changes driven by NetCloud Engine > NetCloud Perimeter; Addition of client analytics and content filtering	Pat Burroughs
2.1	November 16, 2017	Updated navigation scheme	Pat Burroughs

TABLE OF CONTENTS

INTRODUCTION 6

LOGIN 6
HELP 6
NAVIGATION 7

NETCLOUD MANAGER 8

NETCLOUD MANAGER TIERS 8

ADMINISTRATION PAGES 10

DASHBOARD 10
HOME 10
GEOVIEW 11
UPTIME 12
MODEM USAGE 13
CLIENTS 14
CLIENT ANALYTICS SETTINGS 15
TRAFFIC 16
DEVICES 17
ROUTERS 17
NETWORK INTERFACES 23
ROGUE AP 28
GROUPS 29
ADD 29
DELETE 29
CONFIGURATION 29
NETCLOUD OS 30
COMMANDS 30
SETTINGS 31
EXPORT 31
COLUMNS 31

APP STATUS 32
TOGGLE THE TREE VIEW 32
EDITING THE NAME FIELD 32
ALERTS AND LOGS 33
ALERT LOG 33
ACTIVITY LOG 35
REPORTS 37
DATA USAGE 37
SAVED REPORTS 37
REPORT TYPE 37
ALERT HISTORY 37
SIGNAL QUALITY 38
ACTIVITY LOG 38
DATE RANGE 39
DATA SOURCE 39
ROUTER 39
NETWORK INTERFACE 40
MODEM INFORMATION 40
SCHEDULER 41
TASKS 41
SCHEDULES 42
TOOLS 43
ROUTER APPS 43
APPLICATIONS 45
SERVICES 45
APPLICATIONS 45
BUTTONS 46
EXPIRATIONS 46
ACCOUNTS & USERS 47
ACCOUNT USERS 47
NCM PERMISSIONS 47
NETCLOUD PERIMETER PERMISSIONS 48

NETCLOUD PERIMETER 49

DEVICES 49

NAMESTATION 50

DEFAULT DNS NAMES 50

USING NAMESTATION 50

ADDING ALTERNATE NAMES TO SERVERS 51

ADCONNECT 51

HOW IT WORKS 51

USING ADCONNECT 51

GATEWAY 52

CONFIGURING YOUR ROUTER 52

CREATE NETCLOUD GATEWAY 53

ENABLE AND CONFIGURE NETCLOUD GATEWAY 53

MEMBERS 54

POLICY 54

SPECIFYING A RULE 55

SMARTZONES 55

USAGEMONITOR 56

MAIN CHART 56

TOP USERS 57

TOP DEVICES 57

SETTINGS 57

NETWORK INFO 57

NAMESTATION 57

ENTITLED SERVICES 57

APPENDIX 58

NETCLOUD PERIMETER CSV EXPORT 58

INTRODUCTION

Cradlepoint NetCloud is the integration of the company's NetCloud Manager (NCM) cloud management service and the NetCloud Perimeter cloud networking service. **NetCloud Manager** enables zero-touch deployment and remote management of Multi-WAN branch and in-vehicle routers and IoT gateways. **NetCloud Perimeter** enables virtual cloud networking that leverages cloud, Software-Defined Networking (SDN), and Network Function Virtualization (NFV) technologies.

LOGIN

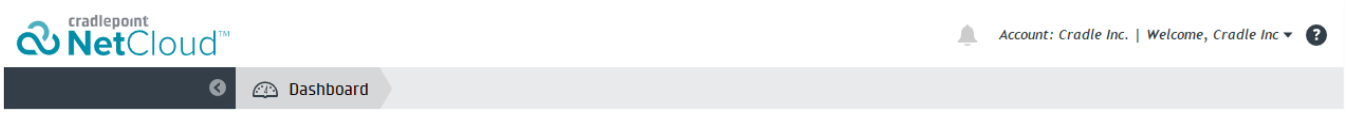
Depending on your ordering process, your devices may have already been bulk-loaded into NetCloud Manager. Simply log in at **cradlepointecm.com** using your NCM credentials and begin managing your devices seamlessly from the cloud.

If your device has not yet been loaded into your NCM account, you need to register. Follow these steps to register your device:

1. Connect to the router via Ethernet or WiFi. For WiFi, the default SSID is found on the product label on the bottom of the router.
2. Open a browser window and type "cp/" or "192.168.0.1" in the address bar and press return/enter.
3. When prompted for the Administrator password, type the default eight character password found on the product.
4. Navigate to **SYSTEM > Setup Wizards > NetCloud Registration**. Enter your NCM username and password, and click **Register**. Once you are logged into cradlepointecm.com, begin managing your devices individually or by group.

HELP

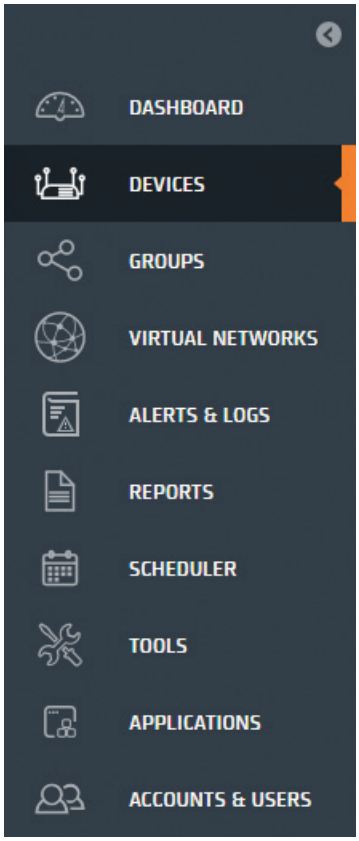
For contextual help, open the Help Panel by clicking on the question mark symbol (?) in the top right corner.



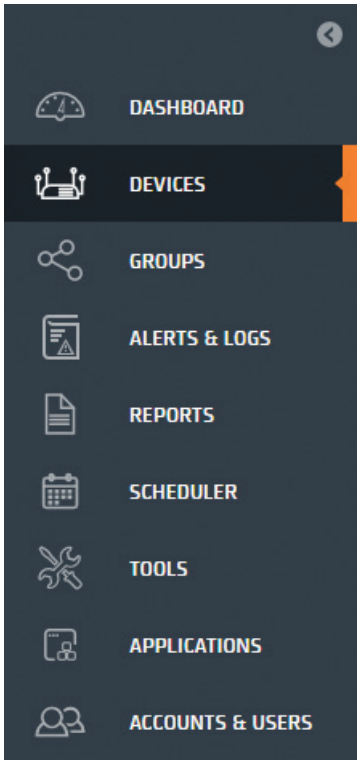
NAVIGATION

Depending on the service(s) you purchase, your navigation scheme will appear as shown:

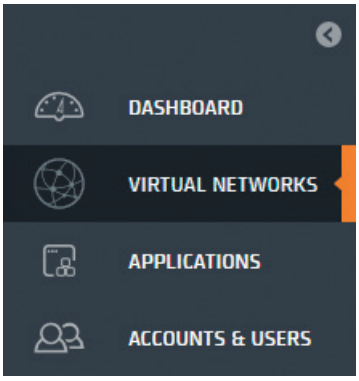
NetCloud Manager + NetCloud Perimeter



NetCloud Manager



NetCloud Perimeter



NETCLOUD MANAGER

NETCLOUD MANAGER TIERS

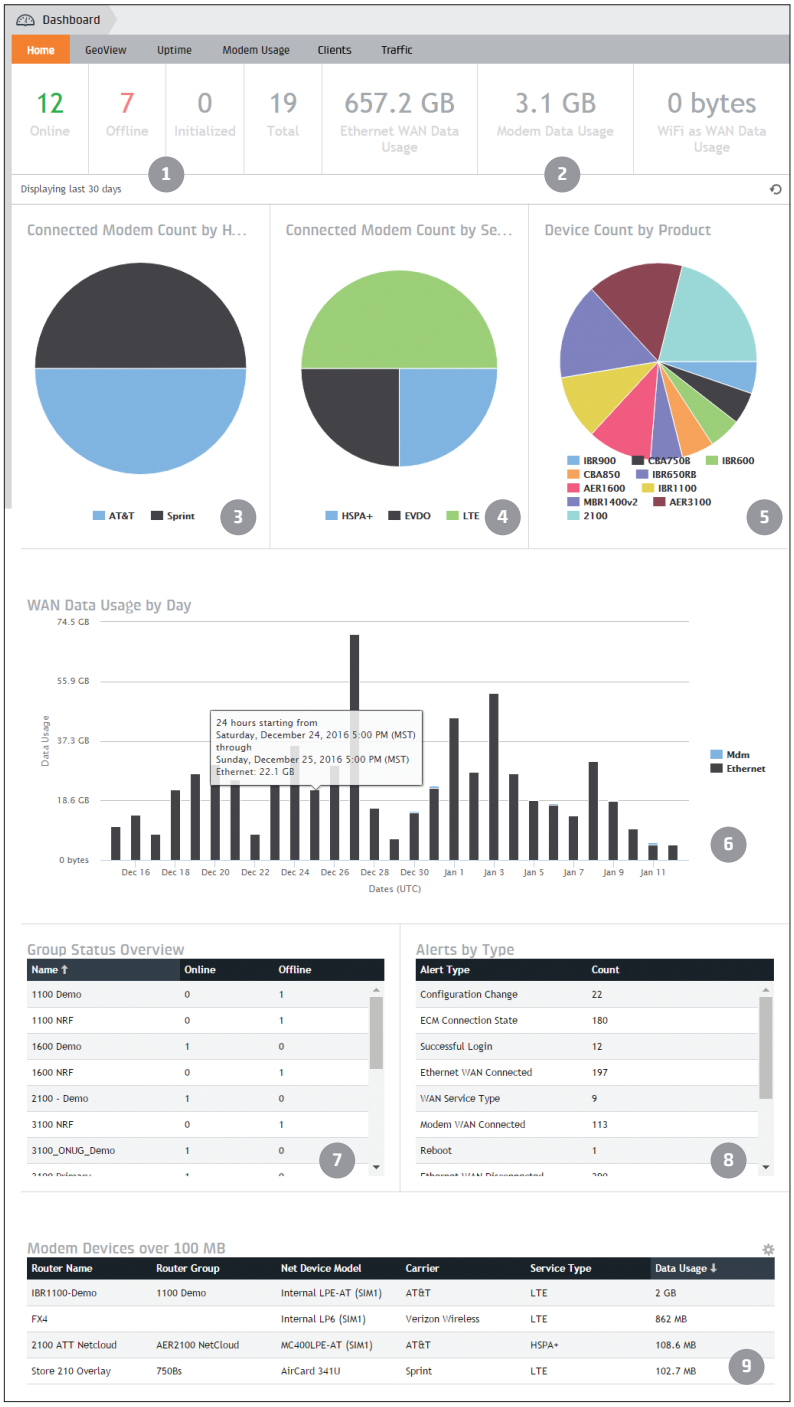
Functionality	STANDARD	PRIME	ENTERPRISE
	Basic Cloud management features	*Enhanced visibility, remote management, mapping/fencing & more*	*Integrated content filtering & traffic analytics*
Cloud Configuration			
Time-saving device management	✓	✓	✓
Zero-touch deployment	✓	✓	✓
NetCloud OS upgrades	✓	✓	✓
Security			
CP Secure Web Filter			✓
IPS/IDS with CP Secure Threat Management	✓	✓	✓
Zscaler Internet Security	✓	✓	✓
Visibility/Analytics			
Cellular data usage analytics		✓	✓
Client analytics		✓	✓
Application Analytics			✓
Uptime		✓	✓
Real-time Diagnostics/Troubleshooting			
On-demand real-time device diagnostics	✓	✓	✓
Speed test	✓	✓	✓
Ping	✓	✓	✓
Traceroute	✓	✓	✓
Reboot	✓	✓	✓
Alerts/Reports			
Alerts	✓	✓	✓
Activity logs	✓	✓	✓

Functionality	STANDARD	PRIME	ENTERPRISE
Reports	✓	✓	✓
Extensibility/Integration			
Fog computing at the network Edge	✓	✓	✓
RESTful open API	✓	✓	✓
Out-of-Band Management / Remote Connect			
Out-of-Band manager		✓	✓
Real-time on-demand device status		✓	✓
LAN manager		✓	✓
Console		✓	✓
Location Services			
GeoView		✓	✓
Geo-Fencing		✓	✓

ADMINISTRATION PAGES

DASHBOARD

HOME



Dashboard gives an analytics overview of your devices, particularly your WAN interfaces. Data is displayed for the last 30 days. **Dashboard** | **Home** information includes:

1. Device count including total devices, devices in Initialized status, and online/offline count
2. Ethernet and Modem WAN data usage
3. Connected Modem count by Home Carrier
4. Connected Modem Count by Service Type
5. Device Count by Product
6. WAN Data Usage by Day
7. Group Status Overview
8. Alerts by Type
9. Modem Devices over xGB

DASHBOARD | HOME TIPS

- Modems without an active connection (e.g., modems that are set for failover) may not always show the carrier or service type in the modem count charts.
- Click on a group name in **Group Status Overview** to link to a list of that group's devices displayed on the Devices page.
- Click on an alert type in **Alerts by Type** to link to a list of alerts of that type displayed on the Alerts page.

GEOVIEW

GeoView gives a geographical overview of your devices.

DEVICE LOCATIONS/LOCATION SERVICES

The GeoView Locations map displays the location of your devices. The location of routers can be set with GPS or by manually placing a pin using the map on the router's dashboard. Once a location has been set for the device, an icon will show up on the map for that device, indicating the general type of device, along with an icon indicating the router's current status. Clicking on the icon will give more information about the router (e.g. Name, Product, Approximate Location, Network Interfaces).

The location of NetCloud hosts is determined by GPS, Cell ID, WiFi SSID, and other techniques with increased accuracy. The icon represents the operating system of the network client.

Devices can be filtered by using the checkboxes to show or hide routers and NetCloud Perimeter clients. The network filter will allow you to filter devices based on a specific NetCloud Perimeter network.

MAP ICONS

ICON	DEFINITION
	A non-WiFi router
	A WiFi router
	A non-WiFi router with NetCloud Perimeter installed
	A WiFi router with a NetCloud Gateway installed

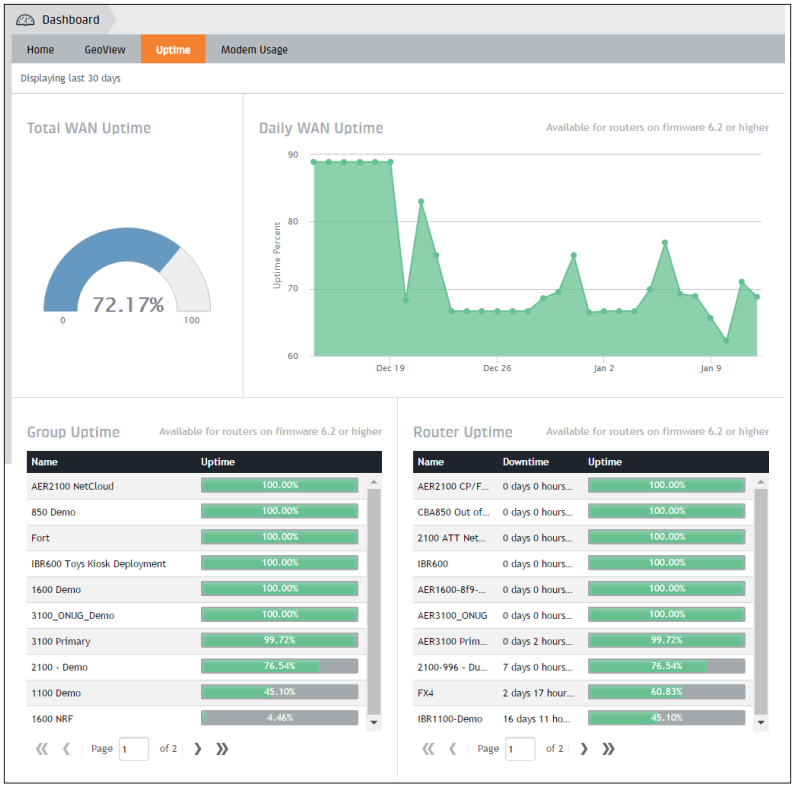
NOTE: NetCloud Perimeter clients are represented by an icon that matches the operating system of the device.

STATUS ICONS

ICON	DEFINITION
	Device in a working state
	Device not working as expected
	Device that is not yet ready, but not in an error state. This can happen because the device was recently turned on.

When there are many devices in a specific location, devices will be clustered together with a count of the number of devices affected. Hovering over a cluster will provide status information about those devices. Clicking on a cluster will zoom in on the map to provide greater location detail. If you have reached the maximum zoom level allowed for a particular location and devices are still clustered, clicking on the cluster will reveal additional information about all the devices in a list. Use the refresh button (⟲) to retrieve the most current device information.

UPTIME



The **Uptime** metric is an approximation of the router's Internet connection uptime percentage per day based on device WAN interface connectivity, and requires the device to be managed by NCM. The data can be analyzed to indicate the health or determine issues within the network. However, depending on the device's use, a high number of reconnects may not necessarily indicate an issue. For example, a mobile device frequently roaming outside normal coverage area will result in a high number of reconnects.

A "day" is defined by a 24-hour period beginning at midnight UTC (Coordinate Universal Time). Uptime is calculated at the end of each 24-hour period and displayed. Today's data will appear in the chart tomorrow. Any future changes to a device (i.e. removing a device from NCM or moving the device to a new group) will not affect the historically collected data.

DASHBOARD | UPTIME TIPS

- **Group Uptime** and **Router Uptime** lists are sortable. Click a column in the list to perform the sort. An arrow will indicate which column is currently being sorted on and the direction.
- Selecting the group name or router name will navigate to their specific dashboard.
- Only groups with Uptime analytical data gathered will be shown.
- Group uptime analytical data is historic. The history will not change if a router's group membership changes.

MODEM USAGE

Modem Usage is calculated at the end of each 24-hour period for the previous day.

A "day" is defined by a 24-hour period beginning at midnight UTC (Coordinate Universal Time).

All usage for the day is rolled into the current SIM. For example, a router has an AT&T SIM in modem 1 and uses 100 MB of data. The AT&T SIM is replaced with a Verizon SIM (same modem) and uses 200 MB of data. The application will then report 300 MB of data for Verizon.

Changes to a device (i.e. removing a device from NCM or moving the device to a new group) will not affect the historically collected data.

CONNECTED MODEM COUNT BY HOME CARRIER

The **Connected Modem Count by Home Carrier** chart displays the number of modems connected per home carrier. Clicking a carrier in the chart will filter the other widgets.

DATA USAGE BY CARRIER

The **Data Usage by Carrier** grid displays modem data usage per unique carrier. To set a data limit and billing cycle start date, click the Settings button in the toolbar.

Select desired carrier to filter the following charts:

CARRIER DATA USAGE BY DAY

The **Carrier Data Usage by Day** chart displays data for the last 30 days or since the last billing cycle start date set in the Data Usage by Carrier settings.

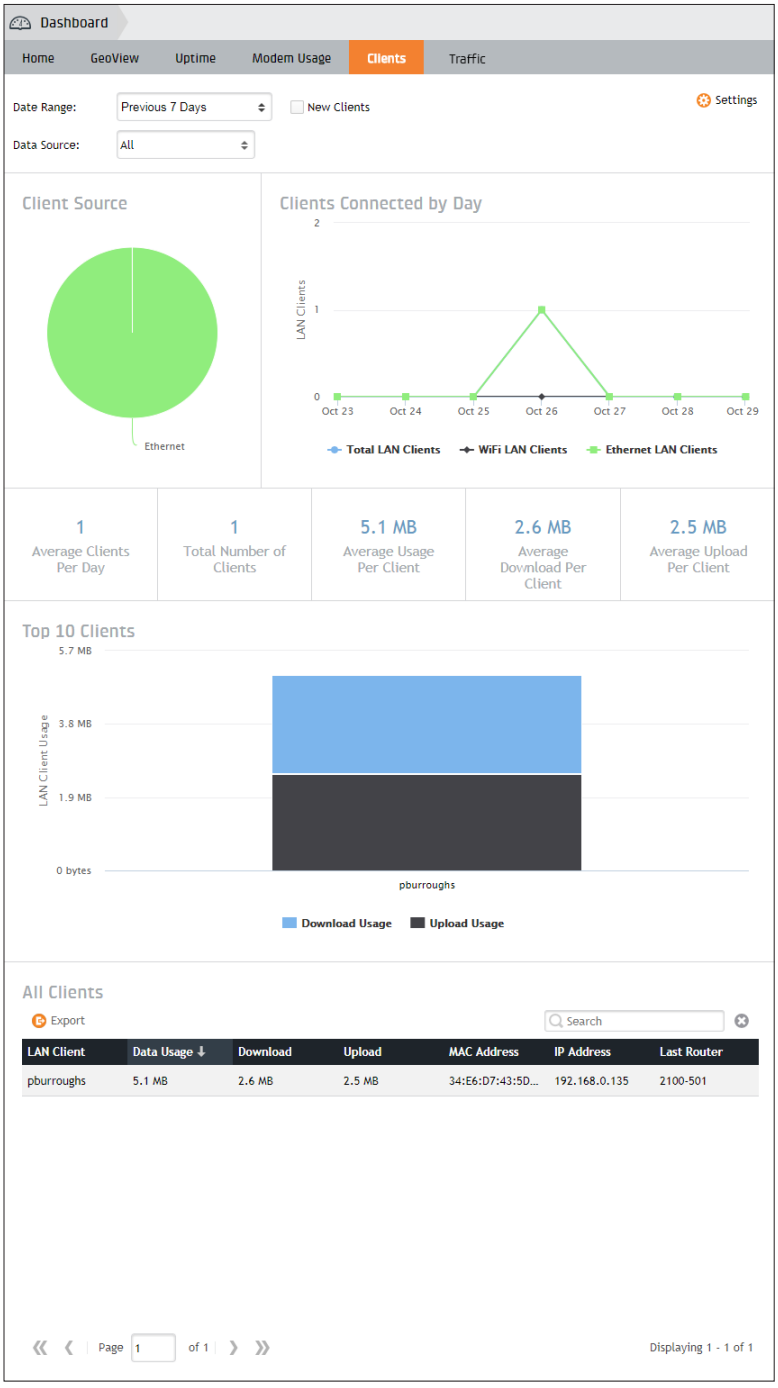
GROUP DATA USAGE BY CARRIER

The **Group Data Usage by Carrier** grid displays the portion of each group's data usage in relation to total usage across all modems for the selected carrier.

DEVICE DATA USAGE BY CARRIER

The **Device Data Usage by Carrier** grid displays the portion of each device's data usage in relation to total usage across all modems for the selected carrier.

CLIENTS



Client analytics data is calculated at the end of each 24-hour period for the previous day. A "day" is defined by a 24-hour period beginning at midnight UTC (Coordinate Universal Time). Data will be displayed 24 hours after enabling the feature on the router.

ENABLING CLIENT ANALYTICS

Client analytics data will not be collected until Client Analytics is enabled on a specific router and the router meets the minimum NetCloud OS version of 6.0.1. Click **Settings** in the upper right hand corner to enable and disable Client analytics on routers.

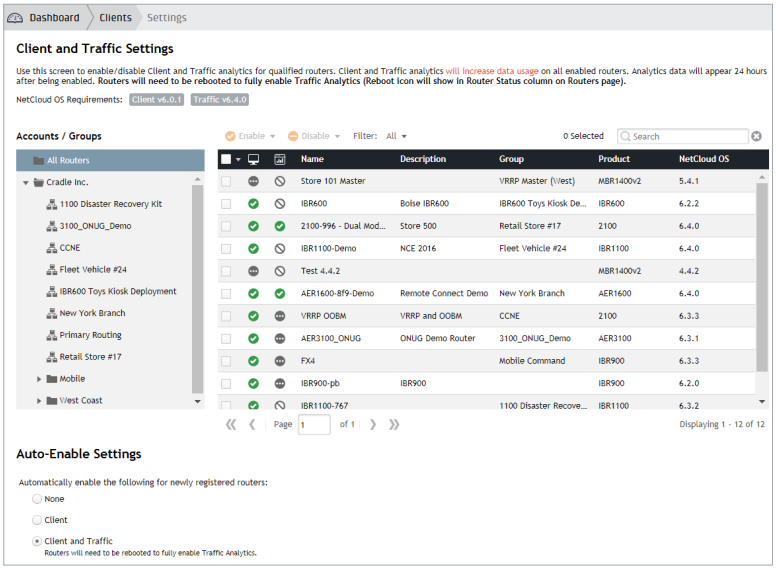
NEW CLIENTS

The **New Clients** checkbox shows clients that have connected to the router for the first time within the selected date range.

BLOCK/UNBLOCK CLIENTS

Blocking and unblocking clients is only available on the Clients tab on the Device Dashboard. Only Full Access and Admin users can use the block/unblock feature. Routers must be in blacklist mode before clients will be available to block or unblock. See this Knowledgebase **article** on how to put clients into blacklist mode.

CLIENT ANALYTICS SETTINGS



FILTERING

The gray tree on the left shows the accounts, groups and subaccounts that contain qualified routers. Routers in subaccounts will not show when the root level account is selected. Clicking “Show All” will clear the selection and show all routers in the account.

AUTO-ENABLE SETTINGS

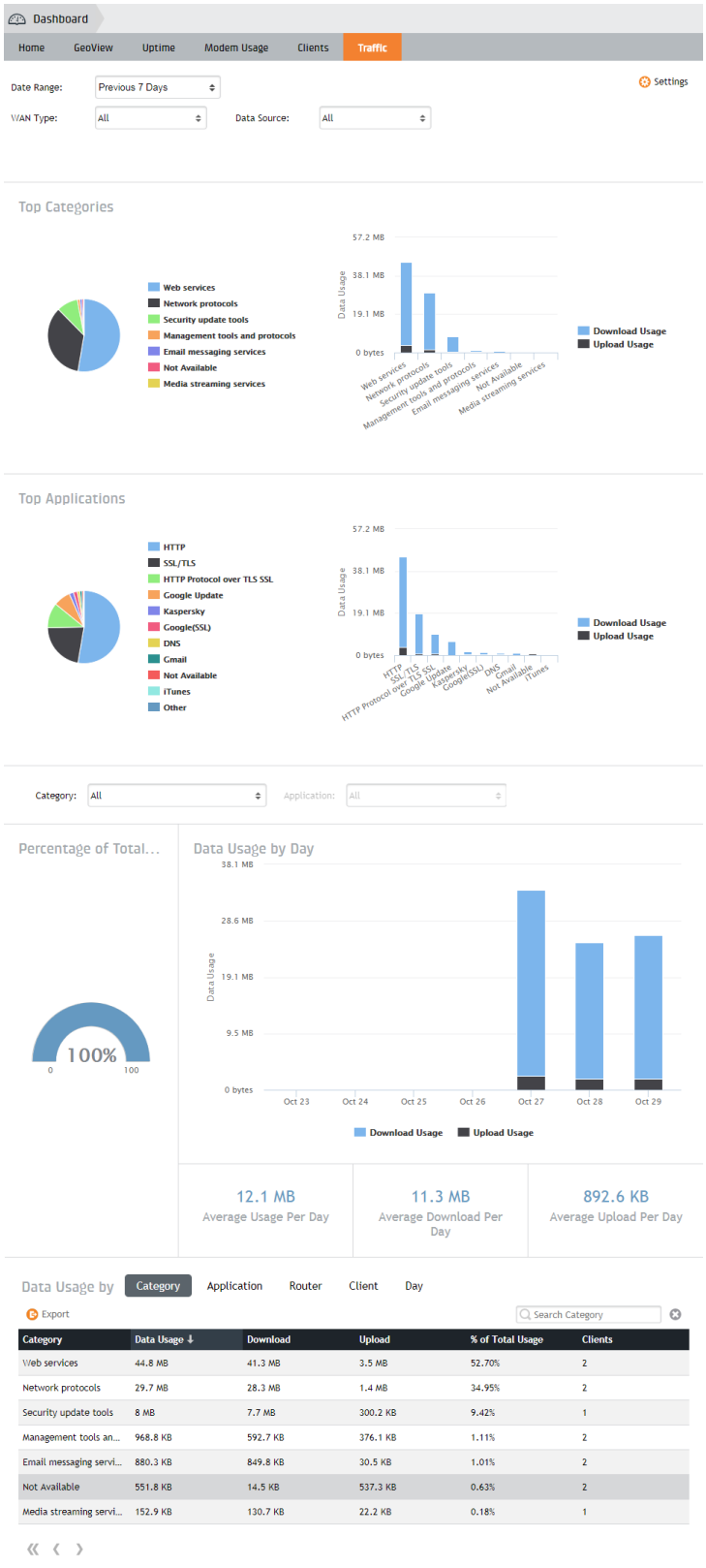
Turning on the auto-enable setting will automatically enable Client analytics for all newly registered routers. However, Client analytics data will not be collected until the router meets the minimum NetCloud OS version (6.0.1). Routers will automatically begin sending Client analytics data once they are upgraded past the minimum NetCloud OS version.

SUPPORTED PRODUCTS

The following products do not support Client analytics:

- Series 2 Devices
- CBA850
- CBA750B
- CBA400
- CBA450
- IBR350
- MBR1200B
- MBR1400

TRAFFIC



Category	Data Usage	Download	Upload	% of Total Usage	Clients
Web services	44.8 MB	41.3 MB	3.5 MB	52.70%	2
Network protocols	29.7 MB	28.3 MB	1.4 MB	34.95%	2
Security update tools	8 MB	7.7 MB	300.2 KB	9.42%	1
Management tools an...	968.8 KB	592.7 KB	376.1 KB	1.11%	2
Email messaging servi...	880.3 KB	849.8 KB	30.5 KB	1.01%	2
Not Available	551.8 KB	14.5 KB	537.3 KB	0.63%	2
Media streaming servi...	152.9 KB	130.7 KB	22.2 KB	0.18%	1

TRAFFIC DASHBOARD

Traffic analytics data is calculated at the end of each 24-hour period for the previous day. A "day" is defined by a 24-hour period beginning at midnight UTC (Coordinate Universal Time). Data will be displayed 24 hours after enabling the feature on the router.

ENABLING TRAFFIC ANALYTICS

Traffic analytics data will not be collected until it is enabled on a specific router which meets the minimum NetCloud OS requirement of 6.4.2. Click Settings in the upper right hand corner to enable and disable Traffic analytics on routers.

FILTERING DATA

Several filters can be applied to the data to drill down to specific data. Filters are applied by selecting items from the drop downs located at the top and middle of the page. **NOTE:** Drop downs only filter information below the drop down, e.g. filtering by Category will not filter information in Top filters section.

Top filters can filter by:

- Date Ranges
- WAN Types
- Data Sources
- WAN Interface
- Network Names
- SSIDs

Middle filters can be filtered by:

- Category
- Application

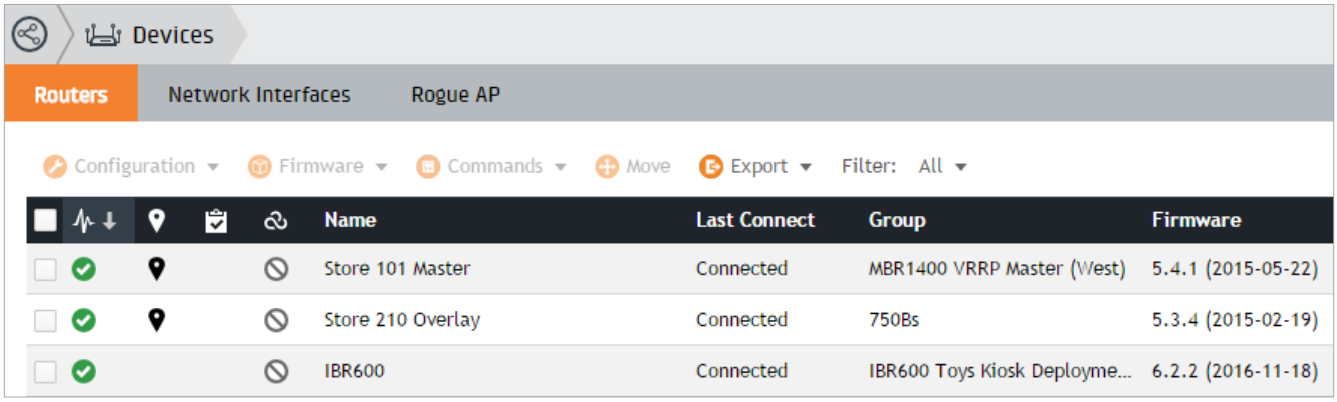
DEVICES

The Devices page has three main views: **Routers**, **Network Interfaces**, and **Rogue AP**. In the views menu at the top, next to Devices, select one of these views (default is Routers).

- Routers displays all the routers.
- Network Interfaces displays every network interface, including both LAN and WAN (e.g. modems, Ethernet connections, WiFi).
- Rogue AP displays a list of WiFi access points that your devices have seen so that you can search for rogue access points.

To view the network interfaces of a particular device (and other basic information) in the device dashboard, click on the device name in the Routers list.

ROUTERS



ONLINE STATUS

View whether a device is online.

ICON	DEFINITION
	Device is connected.
	Device is disconnected
	Device has been remotely activated but has not yet checked in with NCM. This process can take up to 24 hours.

ROUTER STATUS

The router status field shows an icon when there is an error or when NCM is in the process of updating something on the router (e.g. new NetCloud OS is downloading). Hover over the icon for details.

ICON	DEFINITION
	The “sync” icon displays when the device is syncing the configuration.
	The “download” icon displays when the device is downloading new NetCloud OS (NCOS).
	The “warning” icon displays when there has been an error, such as when NetCloud OS failed to download.
	The “reboot” icon indicates that the device must be rebooted to activate the functionality associated with new device licenses.
	The “schedule” icon indicates that the router is waiting for the assigned schedule window to take place before it will start updating.
	The “disabled” icon indicates that the router is in a group that has a disabled NetCloud OS upgrade scheduled task. This will block NCOS upgrades from running on this group until the schedule is enabled or deleted.

NETCLOUD GATEWAY STATUS

The NetCloud Gateway status field shows an icon when a router supports the client and what the status of the client is currently. Hover over the icon for details.

ICON	DEFINITION
	The “not supported” icon displays when the device does not support the Gateway function.
	The greyed out “add” icon displays when the device supports the Gateway function but something is preventing it from being added to the router.
	The “add” icon displays when the device supports the Gateway function but it has not been added to the router. Clicking on the “add” icon will allow you to configure this router as a NetCloud Gateway.
	The “downloading” icon displays when the NetCloud Gateway software is being downloaded to the router.
	The “installing” icon displays when the NetCloud Gateway software has been successfully downloaded to the router and is in the process of being installed.
	The “OK” icon displays when the NetCloud Gateway is functional.
	The “pending” icon indicates that the NetCloud Gateway is no longer connected to the virtual cloud network and intervention may be needed.
	The “error” icon indicates that the NetCloud Gateway has encountered an error or is offline and needs user intervention.

CONFIGURATION

There are three main ways to edit a device's configuration:

1. The **Groups** panel in NCM
2. The **Devices** panel in NCM
3. Locally, through the individual device administration pages

Configuration settings from all of these three sources are additive unless there is a conflict. The following table shows the configuration priority when there are conflicts:

CONFIGURATION PRIORITY LEVELS	
Highest	NCM Device
	Local
Lowest	NCM Group

Pending server changes will delete a pending local change. Local changes are only accepted if they are made after the device is synced. The exception is on registration, when local changes will be merged with the individual config.

In general, the preferred method for configuring devices is through the **Groups** panel in NCM. If you have more specific settings for individual devices, use the **Devices** panel (this page).

For example, you could make the administration password standard for an entire group and then create individual SSIDs for specific devices – both through NCM. If someone tried to log into the device administration pages to change either the administration password or SSID, those changes would be merged into the NCM Device configuration settings.

The **Configuration** menu in the top toolbar lets you Edit a device's configuration, display a configuration Summary, Clear the device configuration, Resume Updates after a configuration update stalled, and Copy To (save the settings from this device and apply them to a group of devices with the same type). To access this menu, you must first select at least one device.

- **Edit** – Opens a popup window with the same configuration options found in the administration pages of the individual devices. The configuration window includes dropdown menus for Network Settings, Internet, and System Settings. Refer to the product manual for more information about configuration options for each type of device.
- **Summary** – This is a diagnostic tool for experts. The output shows the Actual configuration currently on the device; the Individual configuration for the router; the Group configuration if the router is in a group; the Target configuration resulting from the individual being layered over the group config; and the Pending changes, the list of changes in NCM that have not yet been synced with the router (i.e., the difference between the Target and Actual configurations).
- **Clear** – Clear the NCM device configuration (including any local configuration); NCM group configuration remains.
- **Resume Updates** – It is possible for a device's configuration changes to be "suspended." This means that a configuration change was sent to the device through NetCloud Manager that disabled the connection to NCM. Whenever this happens the device rolls back to the previous configuration settings and it can no longer receive configuration updates. Select Resume Updates to restart configuration updates for the device.
  NOTE: You should first determine why the suspension occurred and correct the configuration.
- **Last Sync Error** – Opens a dialog showing details of the last configuration sync error for the selected router.
- **Copy To** – Saves the settings from this device and applies them to a group that you select. Only groups with the same product type and the same or newer NetCloud OS are available for you to select.
- **Location Services (Enable/Disable)** - Select one or more devices and then select Configuration in the top toolbar and Location Services in the dropdown menu, then choose Enable or Disable to turn Location Services on or off for the selected devices. When Location Services are enabled on a device, you will have

the option to turn on Automatic GPS Tracking as well. Automatic GPS Tracking allows the device's location to be updated and shown automatically using GPS. GPS will be enabled for the device if not already enabled. This will increase data usage for the selected device(s). When Location Services are disabled on a device, you will be prompted if you would like to disable GPS as well or leave it enabled.

NETCLOUD OS

When a device has a NetCloud OS error, select that device and click on **NetCloud OS** and then **Retry Upgrade** to attempt another NCOS upgrade. (An error may have taken place because of a modem disconnect, for example).

COMMANDS

- **Reboot** – Select one or more devices and then select **Commands** in the top toolbar and **Reboot** in the dropdown menu. Confirm that you want to reboot the selected device(s).
- **Restore to Defaults** – Select one or more devices and then select **Commands** in the top toolbar and **Restore to Defaults** in the dropdown menu to return the selected device(s) to factory defaults. You will be asked to confirm this action. Group and device configuration settings assigned through Cradlepoint NetCloud Manager will be reapplied once this operation is complete.
- **Unregister** – Select one or more devices and then select **Commands** in the top toolbar and **Unregister** in the dropdown menu to remove the selected device(s) from NCM. You will be asked to confirm this action.
- **WiFi Site Survey** – Select a device and then select **Commands** in the top toolbar and **WiFi Site Survey** in the dropdown menu to search for nearby wireless access points. Use this to refresh the **Devices > Rogue AP** list and find rogue access points.
- **Update IPS Signatures** – Select one or more devices and then select **Commands** in the top toolbar and **Update IPS Signatures** in the dropdown menu to send a request for a new IPS signature version. The current signature version is displayed in the IPS Version column (the column does not display by default). Signatures can also have regularly scheduled updates: click on **Configuration > Edit** to open a configuration window, and then select **Network Settings > Threat Management** to view Threat Management configuration options (including scheduled signature updates).

  NOTE: Update IPS Signatures is only available for devices with a CP Secure Threat Management entitlement. Purchase or trial Threat Management in the Applications section (available to account administrators only).
- **Ping** – Select a device and then select **Commands** in the top toolbar and **Ping** in the dropdown menu to open a popup window for a simple ping test, which measures round-trip message times.
- **Traceroute** – Select a device and then select **Commands** in the top toolbar and **Traceroute** in the dropdown menu to use the traceroute utility, which outputs the times and IP addresses for each hop along a route.
- **Speed Test** - Select a device and then select **Commands** in the top toolbar and **Speed Test** in the dropdown menu to open a popup window for a speed test, which measures connection speed and outputs metrics such as Latency, Jitter, Loss, Throughput, etc.
- **Console** – Select a device and then select **Commands** in the top toolbar and **Console** in the dropdown menu to open a console session to the selected device.
- **Create NetCloud Gateway** - Select a router and then select **Commands** in the top toolbar and **Create NetCloud Gateway** in the dropdown menu to create a secure cloud gateway.
- **Edit NetCloud Gateway** - Select a router and then select **Commands** in the top toolbar and **Edit NetCloud Gateway** in the dropdown menu to edit the existing NetCloud Gateway. This is only visible if the NetCloud Gateway has been previously configured.
- **View NetCloud Configuration** - Select a router and then select **Commands** in the top toolbar and **View NetCloud Configuration** in the dropdown menu to view an existing NetCloud Gateway configuration. Only visible if the account is Read-Only.
- **Remove NetCloud Gateway** - Select one or more routers and then select **Commands** in the top toolbar and **Remove NetCloud Gateway** in the dropdown menu to remove the NetCloud Gateway functionality.

MOVE

To move one or more devices to a different group or account, select the device(s) and then click **Move**. In the popup window, select the group or account and click **OK** to save the change. (Only groups with the same product type are displayed in the popup window. To move multiple devices, they all must have the same product type.)

EXPORT

Export device information as a CSV file. Choose from Filtered List, All Routers, Router Logs, and Activity Logs.

- **Filtered List** – exports information for the devices displayed in the grid, which may have been filtered (e.g. by using the search tool or by selecting by product type)
- **All Routers** – exports information for all routers, regardless of how the display in the grid has been filtered
- **Router Logs** – exports the logs of the selected router
- **Activity Logs** - exports activity log information for the selected router

COLUMNS

To edit the columns displayed, click on the columns selection icon in the top right corner. This opens a complete list of the available columns. To customize your grid, select or deselect column titles.

The following columns are available:

- **Online Status**
- **Router Status**
- **Individually Configured** - Displayed if the router has configuration settings that override or extend the group configuration.
- **NetCloud Gateway Status**
- **Linked Router** - This icon is displayed if the router is linked to another router. To enable this feature, both routers must have the LLDP configuration option enabled and NetCloud OS version 6.1.0 or above. Clicking the link icon loads the linked router's Device Dashboard.
  NOTE: If the LLDP link is broken, a broken link icon is displayed. If both routers are offline, their last linked status is displayed.
- **Location Services** - This icon is displayed if Location Services are turned on for the router.
- **Name** – User-editable name; by default this is of the form "IBR900-f76"; click on the pencil icon within this column to edit the name for the device
- **Description** – User-defined description; click on the pencil icon within this column to edit the description for the device
- **Asset Identifier** – User-defined identifier that is often used for asset tracking and inventory management; click on the pencil icon within this column to edit the asset identifier for the device
- **Product** – product type, e.g. "IBR900"
- **MAC Address** – Device media access control address
- **IP Address** – Device Internet Protocol address
- **Group** – Name of the group the device is in
- **NetCloud OS** – NetCloud OS version number and date
- **Configuration**
  - **Synched** – Device has adopted all configuration changes sent through NCM
  - **Pending** – Device has not yet adopted configuration changes sent through NCM
  - **Suspended** – A configuration change was sent to the device through NetCloud Manager that disabled the connection to NCM; whenever this happens the device rolls back to the previous configuration settings and it can no longer receive configuration updates
- **NCOS Status** – When a NetCloud OS upgrade is sent to a device, this shows the status of that upgrade
  - **Flashing** – NetCloud OS is being written to the device; this shows the percent complete

  - **Installing** – Shows the time, in minutes and seconds, of the install process
  - **Complete** – NetCloud OS has been upgraded
  - **Pending** – A NetCloud OS upgrade was sent to the router but did not complete (probably due to a modem disconnect); it will try again when the connection is restored
  - **Retry** – Initial NetCloud OS upgrade failed, but it will now try to upgrade again
  - **Error** – NetCloud OS upgrade failed after retry; select **NetCloud OS** on the top bar and then **Retry Upgrade** to attempt another NCOS upgrade
- **Account** – Name of the account the device is in
- **Full Product** – More detailed product type; distinguishes between cellular technologies (e.g. IBR600LE, IBR600P)
- **ID** – Each device in NCM has a unique number for identification
- **Custom 1 and Custom 2** – Editable fields for individualized needs
- **Last Connect** – Displays "Connected" if the device is currently connected to NCM; displays the time since the last connection if not connected to NCM (e.g. "23 minutes ago"); hover over this field to see a more detailed time listing:
  - Disconnected devices show the last time the device was connected
  - Connected devices show the time from the last activity over this connection
- **Serial Number** – Router serial number; this field might not be populated for some routers
- **IPS Version** – Signature version number for CP Secure Threat Management

  NOTE: IPS Version information is only available for devices with a CP Secure Threat Management entitlement. Purchase or trial Threat Management in the Applications section (available to account administrators only).

By default, all the above columns display except **Full Product, ID, Custom 1, Custom 2, Last Connect, Serial Number, and IPS Version**.

HOW TO FILTER THE GRID

To filter the display to show a subset of devices, you have two main options:

1. Some of the fields in the grid are hyperlinks for filtering the grid (e.g. "Product"). From within the grid, click on a hyperlinked field and the grid will be filtered to display only the devices of that type. For example, click on "MBR1400v2" to display only MBR1400v2 devices. The hyperlinked fields for filtering are:
   - Product
   - Group
   - Account
   - Full Product (not displayed by default)
2. Input a string of characters into the search box (top right) to filter by devices that have that string in one of their fields. You can use partial strings, and the field does not have to start with the partial string. For example, "600" will display devices that have "IBR600" in the Product field. This searches all of the following fields:
   - Name
   - Description
   - MAC Address
   - IP Address
   - Product
   - Group
   - Account
   - ID (not displayed by default)

- Full Product (not displayed by default)

TOGGLE THE TREE VIEW

Click on the Toggle Tree icon in the views menu at the top left to display a tree view of your accounts and groups. Use this to drill down to a particular account or group: only the devices within that account or group display in the grid.

Click on (the "Clear Tree Selection" icon) at the top of the tree panel to clear the selection.

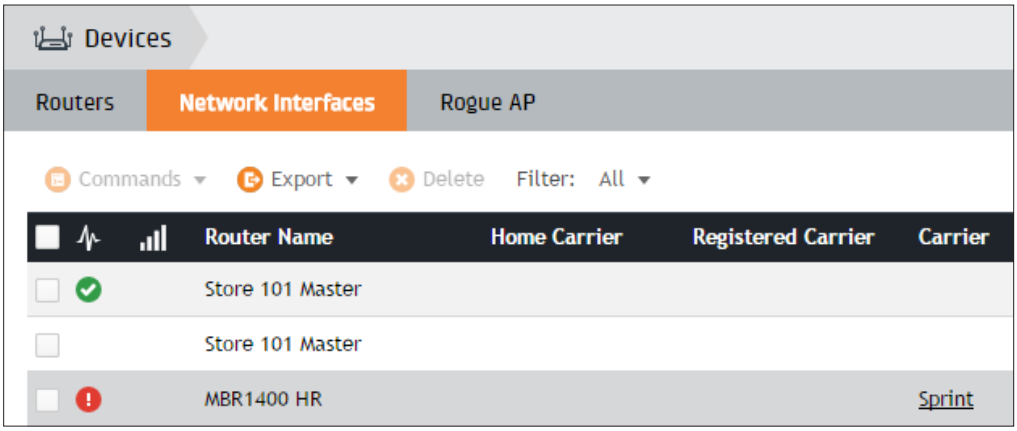
EDITING THE "NAME" AND "DESCRIPTION" FIELDS

The **Name**, **Description**, **Asset Identifier**, and **Custom** fields are editable. Click within the row you want to edit: the pencil icon appears in these columns. Click on this icon to edit these fields.

NOTE: It's possible to use = or " symbols in these editable fields, but those symbols are not searchable.

NETWORK INTERFACES

View information about individual network interfaces (e.g. modems, Ethernet connections, WiFi).



Filter the Network Interfaces display by selecting one of the following buttons from the menu bar at the top:

- All (default)
- Modems
- WiFi
- WiFi as WAN
- WiFi Bridge
- Ethernet
- VLAN

COMMANDS

The commands available on the Network Interfaces page are all related to updating modem firmware. Select a modem to access these options – the **Commands** menu is greyed out for other interfaces. Click on **Commands** in the top toolbar to open a dropdown menu with the following options:

- **Manage Modem Firmware** – Manage the Modem firmware. Allows for checking, upgrading and switching firmware as applicable to the modem model.
- **PUK Unlock** - This will become enabled if the selected modem's SIM has been locked and therefore requires a PUK Code to be unlocked. The PUK unlock will not work if the modem is the only connection to the internet. There needs to be an alternative connection, such as a WAN ethernet port or dual modems.

The status for each of these selections appears in the Modem FW Status column. Possible statuses include the following:

Check for New Modem Firmware

- Checking
- Upgrade Available (version)
- Up to date
- Retrying (2nd Retry)
- Error Checking Firmware: reason

Upgrade Modem Firmware

- Checking (%)
- Downloading (%)
- Validating (%)
- Valid
- Flashing (%)
- Applying
- Upgrade Successful
- Retrying (x Retry)
- Upgrade Error: reason

Switch Carrier

- Starting
- Downloading (%)
- Valid
- Flashing (%)
- Applying
- Complete
- Upgrade Successful
- Upgrade Error: reason

Possible reasons for an error include the following:

- WAN disconnect or poor connection
- A router NetCloud OS upgrade is already in process
- The modem is not attached
- No upgrade is available
- There is a problem with the modem itself

EXPORT

Export network interface information as a CSV file. Choose from Filtered List and All Network Interfaces.

- **Filtered List** – Export information for the network interfaces displayed in the grid, which may have been filtered (e.g. by using the search tool or by selecting by product type).

- **All Network Interfaces** – Export information for all network interfaces, regardless of how the display in the grid has been filtered.

DELETE ✖

To delete a network interface, select one or more unused network interface(s) from the grid and click on **Delete** in the top toolbar. **WARNING:** This action will permanently remove all statistics and history associated with these network interfaces. If the network interface(s) are later rediscovered, they will be treated as new entries within NetCloud Manager and all history will be reset.

COLUMNS

To edit the columns displayed, click on the columns selection icon in the top right corner. This opens a complete list of the available columns. To customize your grid, select or deselect column titles. Drag the column headers to reorder or resize columns. Click on a column header to order the rows by the information in that column.

The following columns are displayed by default:

- **Online Status** – Shows the connection state for WAN interfaces. LAN interfaces are left blank.

ICON	DEFINITION
	Interface is connected
	Interface is connecting
	Interface is available or in standby (i.e., for failover)
	Interface is disconnected
	Interface is unconfigured
	Interface is unplugged

- **Signal Strength** – Relative percentage indicating the signal strength based on signal quality metrics.

ICON	DEFINITION
	Unavailable or not applicable
	0%
	1–24%

ICON	DEFINITION
	25–49%
	50–74%
	75–100%

- **Name** – ethernet-lan, ethernet-wan, wlan-wireless0, etc. Cellular modems include an identifier (e.g. lte-cec5ffa7).
- **Cellular RSSI** – This is the signal strength, or **RSSI** (received signal strength indicator) measured in dBm. For most modems, the minimum acceptable value is dBm > -85 (values closer to 0 are better). WiFi devices report RSSI under the WiFi RSSI column.
- **SINR** – **Signal to Interference plus Noise Ratio**. This is a measure of the quality of the signal, taking into account interference and noise. SINR is positive, and higher numbers are better. (Minimum acceptable value: dB > 7)
- **ECIO** – **Ec/Io** is a measure of the signal quality used with multiple technologies including HSPA+ and EVDO. It is the ratio of the received energy of the carrier to the overall interference, expressed as a logarithm (i.e. Ec/Io = $\log_{10}$[Effect energy / (total energy + noise)]). This value will be negative: numbers closer to 0 are better quality signals. (Minimum acceptable value: dB > -10)
- **Service Type** – The service or technology type of the network interface (e.g. LTE, Ethernet, WiFi).
- **Carrier** – The connected carrier if available. Otherwise, the carrier the modem is configured to connect to.
- **Registered Carrier** – The carrier the modem is currently registered with.
- **IPv4 Address** – The IPv4 (Internet Protocol version 4) address of the network interface. Example: 10.143.127.234.
- **Model** – Detailed network interface type (e.g. Internal LTE/EVDO, 10/100/1000 Ethernet Switch).
- **Router Full Product** – The router product type (e.g. IBR600LE).
- **Bytes In** – Amount of data input transferred since the last reboot.
- **Bytes Out** – Amount of data output transferred since the last reboot.
- **MDN** – Mobile Directory Number. This is the phone number associated with the modem.
- **Modem FW Status** – Shows the status of a change to the modem firmware settings. See the Commands section (above) for more details.

The following columns are not displayed by default but are available to be shown:

- **Account** – The account the device is in.
- **Asset** – Specifies if an interface and its historical data will persist when moved between routers in an account.
- **BSID** – The WiMAX Base Station Identifier.
- **Cell ID** – The ID of the cell tower you are currently connected to.
- **CINR** – **Carrier to Interference plus Noise Ratio**. This is a measure of the quality of the signal, taking into account interference and noise. CINR is specific to WiMAX. CINR is positive, and higher numbers are better. (Minimum acceptable value: dB > 9)
- **Connection State** – Connection to the carrier network.
- **Device Type** – The type of device. (e.g. Ethernet, VLAN, LTE, Modem, etc.)

- **ESN** – **Electronic Serial Number** – older identification number for CDMA, replaced in newer devices by MEID. "Pseudo" ESNs (pESN) that are not necessarily unique can be generated from the MEID when an ESN is needed.
- **Gateway** – The default gateway of the network interface's internet connection.
- **Home Carrier** – The carrier of the modem's service provider account. This value is associated with either the modem itself, or the modem's SIM card if applicable.
- **ICCID** – **Integrated Circuit Card Identifier** – unique international identifier for a physical SIM card. Not all devices using a SIM will report an ICCID.
- **ID** – The ID of the network interface. Each network interface in NCM has a unique number for identification.
- **IMEI** – **International Mobile Station Equipment Identity** – unique identifier for LTE, HSPA+, and GSM technologies.
- **IMSI** – **International Mobile Subscriber Identity** – unique identifier for a subscriber. This is typically displayed as a 15-digit number composed of the mobile country code (MCC), mobile network code (MNC), and mobile subscription identification number (MSIN).
- **Last Update** – The time of the last update received from the device.
- **Manufacturer** – The manufacturer of the device.
- **MEID** – **Mobile Equipment Identifier** – unique identifier for certain carrier devices. An MEID is comprised of hexadecimal digits and is 56 bits long (14 hex digits).
- **Family** – The type of network the interface is currently operating in (e.g. WAN or LAN).
- **Modem FW** – The modem's firmware carrier as determined from the modem's firmware package string.
- **Modem FW Version** – The modem's firmware version.
- **Modem Serial Number** – The GSN number (ESN/IMEI).
- **MTU** – The **Maximum Transmission Unit** is the size of the largest packet that the layer can pass onwards.
- **NAI** – The **Network Access Identifier** is the user identity submitted by the client during network access authentication.
- **Netmask** – The netmask of the network interface's internet connection. A netmask is used to define a range of IP addresses.
- **Port** – The physical port on the device that the modem is plugged into.
- **Primary DNS** – Primary Domain Name System server address.
- **Product** – The product name of the modem.
- **Router Group** – The name of the group the router is in.
- **Router ID** – The ID of the router. Each device in NCM has a unique number for identification.
- **Router MAC** – The MAC (Media Access Control) address of the router.
- **Router Name** – The name of the router. By default, this is of the form: MBR1400-f76 or IBR600-52b (the last three characters are the last three characters of the MAC address). You can change these names in the Devices section.
- **Router Product** – The router product type (e.g. IBR600).
- **RSRP** – Reference Signal Receive Power is an LTE-specific measure of signal strength, similar to RSSI. RSRP measures lower than RSSI due to the way it is calculated.
- **RSRQ** – Reference Signal Receive Quality is an LTE-specific measure of signal quality that works in conjunction with RSRP. It is a ratio of the RSRP to the total received power, including unwanted noise.
- **Secondary DNS** – Secondary Domain Name System server address.
- **Serial Number** – The modem's serial number. This is selected by the router from the first available field (CGSN, ESN, GSN).
- **SSID** – The "Service Set Identifier" or "network name" for WiFi interfaces.
- **UID** – The unique identifier the router uses to identify the modem.

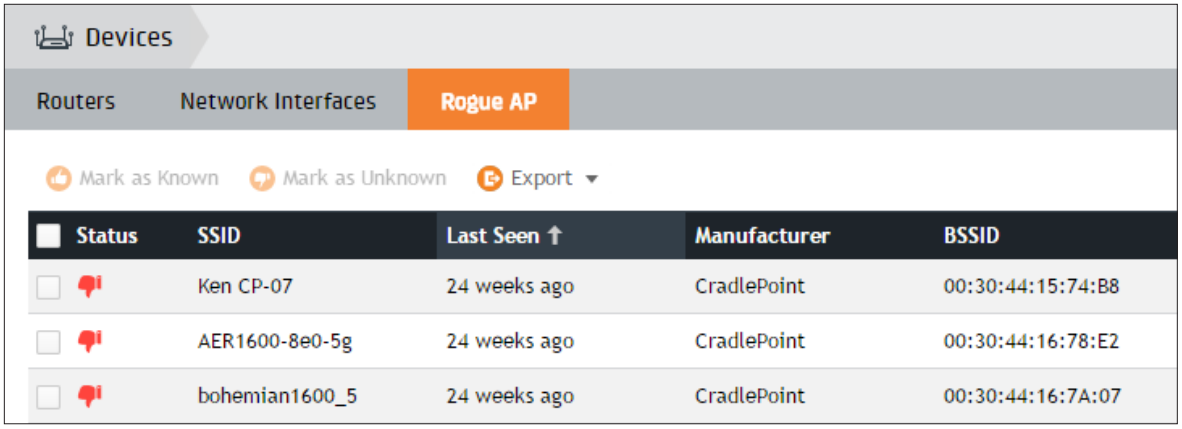
- **Uptime** – The time in seconds since the network interface was restarted.
- **WiFi Channel** – The WiFi channel currently in use. Only for WWAN devices.
- **WiFi RSSI** – **Received Signal Strength Indicator** is a measurement of the power present in a received radio signal. WiFi as WAN and WiFi bridged connections report RSSI values. Modems report RSSI under the Cellular RSSI column.
- **WiMAX Realm** – Used to attach and authenticate with a WiMAX service. This value is only used by WiMAX-capable devices.

To learn more about signal strength, quality and values, refer to the following Cradlepoint Knowledge Base articles:

- **Modem Signal Strength and Signal Quality**
- **Minimum Mobile Broadband Data Connection Signal Values**

ROGUE AP

View a list of wireless access points that your devices have seen. Mark these as **Known** or **Unknown**. Use this list to search for rogue access points that could threaten your networks.



EXPORT

Export this list as a CSV file. Choose from Filtered List and All Access Points.

- **Filtered List** – Exports information for the access points displayed in the grid, which may have been filtered (e.g. by using the search tool or by selecting by one of the fields)
- **All Access Points** – Exports information for all access points, regardless of how the display in the grid has been filtered

COLUMNS

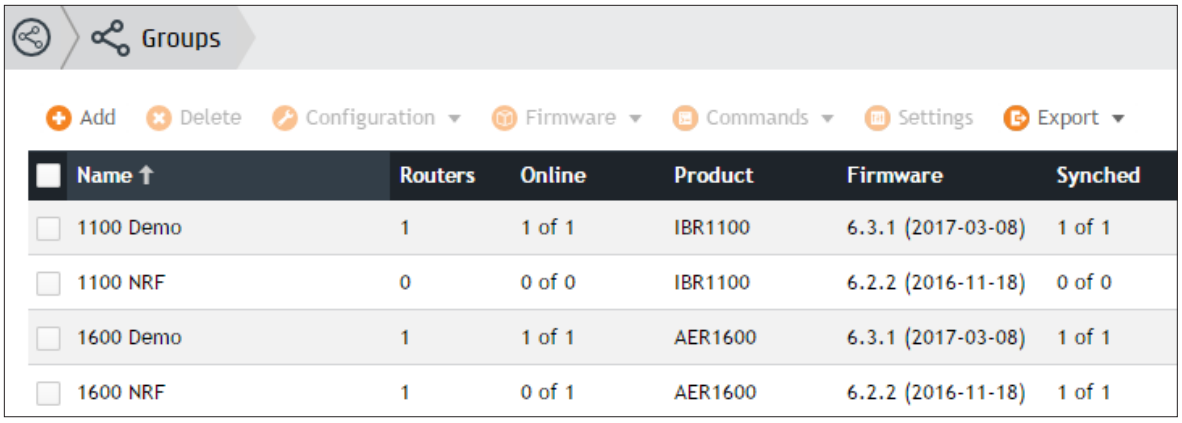
To edit the columns displayed, click on the columns selection icon in the top right corner. This opens a complete list of the available columns. To customize your grid, select or deselect column titles.

GROUPS

Manage groups of devices. Categorize your devices into groups of the same type. NetCloud OS and configuration updates are applied to the whole group.

To make configuration changes, update NetCloud OS, etc., first select the group by clicking on the checkbox next to the group or clicking within the row of the group.

Click on the name of a group to open the **Group Dashboard**, which shows basic information about the group and the device list information for devices in the group.



Name	Routers	Online	Product	Firmware	Synched
1100 Demo	1	1 of 1	IBR1100	6.3.1 (2017-03-08)	1 of 1
1100 NRF	0	0 of 0	IBR1100	6.2.2 (2016-11-18)	0 of 0
1600 Demo	1	1 of 1	AER1600	6.3.1 (2017-03-08)	1 of 1
1600 NRF	1	0 of 1	AER1600	6.2.2 (2016-11-18)	1 of 1

ADD

Click Add at the top left to create a new group. This opens a popup Add Group window. Complete the following fields:

- **Group Name** – Choose a name meaningful to you.
- **Subaccount** – This defaults to your main account. Click "Change" to select one of your subaccounts.
- **Product** – Select from the dropdown list (e.g., IBR600B or AER3100).
- **NetCloud OS** – Select a NetCloud OS version from the dropdown list. This NCOS version will be pushed to devices when you add them to the group.

DELETE

Select one or more groups and click Delete to delete the group(s). If there are devices in the group(s), the devices will still be listed in the Devices page, but unattached to a group.

CONFIGURATION

There are three main ways to edit a device's configuration:

1. The **Groups** panel in NCM
2. The **Devices** panel in NCM
3. Locally, through the individual device administration pages

Configuration settings from all of these three sources are additive unless there is a conflict. The following table shows the configuration priority when there are conflicts:

CONFIGURATION PRIORITY LEVELS	
Highest	NCM Device
	Local
Lowest	NCM Group

Pending server changes will delete a pending local change. Local changes are only accepted if they are made after the device is synced. The exception is on registration, when local changes will be merged with the individual config.

In general, the preferred method for configuring devices is through the **Groups** panel in NCM. If you have more specific settings for individual devices, use the **Devices** panel (this page).

For example, you could make the administration password standard for an entire group and then create individual SSIDs for specific devices – both through NCM. If someone tried to log into the device administration pages to change either the administration password or SSID, those changes would be merged into the NCM Device configuration settings.

The **Configuration** menu in the top toolbar lets you Edit a device's configuration, display a configuration Summary, Clear the device configuration, Resume Updates after a configuration update stalled, and Copy To (save the settings from this device and apply them to a group of devices with the same type). To access this menu, you must first select at least one device.

- **Edit** – Opens a popup window with the same configuration options found in the administration pages of the individual devices. The configuration window includes dropdown menus for Network Settings, Internet, and System Settings. Refer to the product manual for more information about configuration options for each type of device.
- **Summary** – This is a diagnostic tool for experts. The output shows the Actual configuration currently on the device; the Individual configuration for the router; the Group configuration if the router is in a group; the Target configuration resulting from the individual being layered over the group config; and the Pending changes, the list of changes in NCM that have not yet been synced with the router (i.e., the difference between the Target and Actual configurations).
- **Clear** – Clear the NCM device configuration (including any local configuration); NCM group configuration remains.
- **Copy To** – Saves the settings from this device and applies them to a group that you select. Only groups with the same product type and the same or newer NetCloud OS are available for you to select.

NETCLOUD OS

To upgrade NetCloud OS, select a group and click on **NetCloud OS** in the top toolbar.

Select a NetCloud OS version number from the dropdown list. A popup will appear with some options. If a scheduled NCOS upgrade task is not assigned to that group the popup will ask if the NCOS upgrade should be run immediately or if it should be scheduled for later. Scheduling the upgrade for later will make another popup appear where a schedule can be selected. This will create a new scheduled task for that group which can be viewed in **Scheduler**.

If an NCOS upgrade task is already scheduled for this group then the popup will ask if the upgrade should be run immediately (ignoring the schedule), run with the current schedule, or if a new schedule should be chosen. A popup window will ask you to confirm that you want to upgrade the NCOS. *Note: NetCloud OS upgrades cause a device reboot.*

COMMANDS

- **Reboot** – Select one or more groups and then select Commands in the top toolbar and Reboot in the dropdown menu. Confirm that you want to reboot all the devices in the group(s).
- **Restore to Defaults** – Select one or more groups and then select Commands in the top toolbar and Restore to Defaults in the dropdown menu to return all the devices in the group(s) to factory defaults. You will be asked to confirm this action. Group and device configuration settings assigned through Cradlepoint NetCloud Manager will be reapplied once this operation is complete.
- **Update IPS Signatures** – Select one or more groups and then select Commands in the top toolbar and Update IPS Signatures in the dropdown menu to send a request for a new IPS signature version. Signatures can also

have regularly scheduled updates: click on **Configuration > Edit** to open a configuration window, and then select **Network Settings > Threat Management** to view Threat Management configuration options (including scheduled signature updates). *NOTE: Update IPS Signatures is only available for devices with a CP Secure Threat Management entitlement. Purchase or trial Threat Management in the Applications section (available to account administrators only).*

- **Manage Router Apps** - Select a group and then select Commands in the top toolbar and Manage Router Apps in the dropdown menu to open a dialog that will show a list of all router apps installed on that group. Apps can also be removed and new apps installed from this dialog.

SETTINGS

The default group Settings are sufficient in most cases. You have the ability to control which information is regularly sent from the router to Cradlepoint NetCloud Manager: edit the usage reporting frequency and the connection pulse interval.

EXPORT

Export group information as a CSV file. Choose from Filtered List and All Groups.

- **Filtered List** – exports information for the groups displayed in the grid, which may have been filtered (e.g. by using the search tool or by selecting by product type)
- **All Groups** – exports information for all groups, regardless of how the display in the grid has been filtered
- **Activity Logs** - exports activity log information for the selected group

COLUMNS

To edit the columns displayed, click on the columns selection icon in the top right corner. This opens a complete list of the available columns. To customize your grid, select or deselect column titles.

The following columns are available:

- **Name** – User-editable group name. This is initially defined when you create a group.
- **Individually Configured** - Displayed if there is a router in the group that has configuration settings that override or extend the group configuration.
- **Online** – Shows the number of devices in the group with an active WAN connection.
- **Offline** – Shows the number of devices in the group with no active WAN connection.
- **Product** – The product type, e.g. “IBR600”.
- **NetCloud OS** – Shows the NetCloud OS version number and the date of its release. If an NCOS update task is scheduled for this Group, the Schedule icon ( ) will appear next to the NCOS version. Hovering over the icon will display the next time the schedule will run in a tooltip.
- **Synched** – Shows the number of devices in the group for which all configuration settings assigned within NetCloud Manager have already been updated on the device.
- **Suspended** – It is possible for a device’s configuration changes to be “suspended.” This means that a configuration change was sent to the device through NetCloud Manager that disabled the connection to NCM. Whenever this happens the device rolls back to the previous configuration settings and it can no longer receive configuration updates. To resume configuration updates for a device (so that it is no longer suspended), go to the Devices page and select the device. Select Configuration from the top bar and then “Resume Updates”. Note: You should first determine why the suspension occurred and correct the configuration.
- **FW Pending** – Shows the number of devices that have been sent a new NetCloud OS version through NCM but have not yet updated.
- **FW Errors** – Shows the number of devices that have NetCloud OS errors (i.e., a device was unable to load an NCOS version sent through NCM). Typically, NCOS errors are caused by a poor WAN connection.
- **Account** – The name of the account the group is a part of.

- **Routers** – The total number of routers in the group.
- **App Status**

APP STATUS

ICON	DEFINITION
	**Installing** - One or more apps are pending installation on one or more routers in the group.
	**Running** - All apps are installed and running on all routers in the group.
	**Notify** - All apps are installed but one or more apps are in a transitory state.
	**Error** - At least one app is in an error state, even though all apps may not yet be installed. Manual intervention is required to fix the error

HOW TO FILTER THE GRID

To filter the display to show a subset of devices, you have two main options:

1. A couple of the fields in the grid are hyperlinks for filtering the grid (e.g. "Product"). From within the grid, click on a hyperlinked field and the grid will be filtered to display only the groups of that type. For example, click on "MBR1400v2" to display only MBR1400v2 devices. The hyperlinked fields for filtering are:
   - Product
   - Account
2. Input a string of characters into the search box (top right) to filter by groups that have that string in one of their fields. You can use partial strings, and the field does not have to start with the partial string. For example, "600" will display groups that have "IBR600" in the Product field. This searches all of the following fields:
   - Name
   - Product
   - Account

TOGGLE THE TREE VIEW

Click on the Toggle Tree icon in the views menu at the top left to display a tree view of your accounts. Use this to drill down to a particular account: only the groups within that account display in the grid.

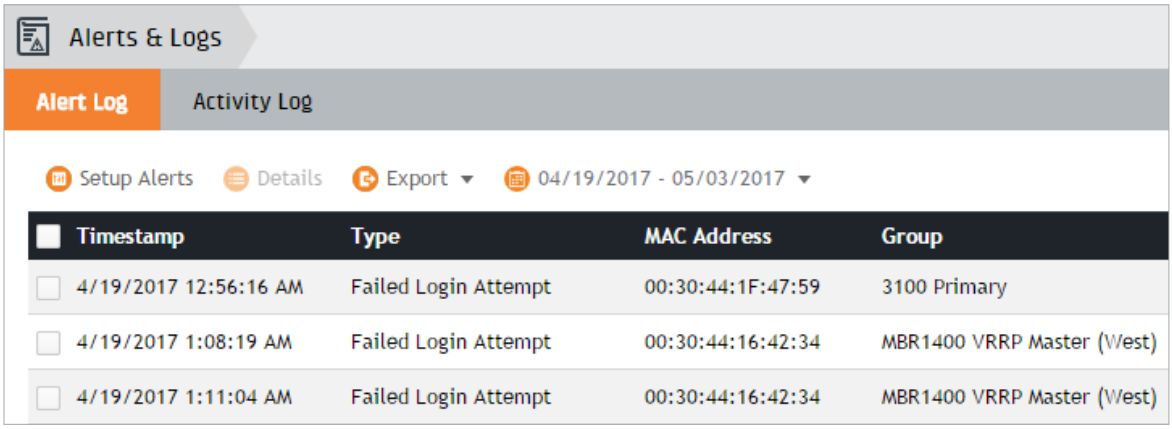
Click on the ✖ icon (the "Clear Tree Selection" icon) at the top of the tree panel to clear the selection.

EDITING THE NAME FIELD

The group "Name" field is editable. Click within the row you want to edit: the pencil icon appears next to the "Name" field. Click on this icon to edit the group name.

NOTE: It's possible to use = or " symbols in an editable field, but those symbols are not searchable.

ALERTS AND LOGS



ALERT LOG

View a list of alerts of the following types:

- **Account Locked** – If Advanced Security Mode is turned on for a device, the account will lock for 30 minutes after six failed attempts to log into the device. To enable this setting, open the configuration pages in **Groups** or **Devices** and go to **System Settings** > **Administration**. Open the **Router Security** tab and select **Advanced Security Mode**.
- **Configuration Change** – This displays when there has been a local configuration change. *Sample alert: The device configuration has changed.*
- **Configuration Rejected** – A configuration change that was sent to the device has been rejected.
- **Configuration Unacknowledged** – A configuration change that was sent to the device was not acknowledged by the device.
- **Data Cap Threshold** – If you have a data cap threshold set, this sends an alert when the threshold is reached. A data cap threshold must be configured under **Internet** > **Data Usage**. *Sample alert: The (Internal LTE/EVDO Port:int1) rule exceeded 100 percent of its 150 MB daily cycle.*
- **Device Location Unknown** - Displays when no location has been reported for 24 hours if the device has GPS enabled. If a manual location is being used the alert will not be generated.
- **NCM Connection State** – Displays when the device loses or regains its connection to NCM. Sample alert: The device entered the "online" state.
- **Ethernet WAN Connected** – An Ethernet WAN device is now active.
- **Ethernet WAN Disconnected** – An Ethernet WAN device is no longer active.
- **Ethernet WAN Plugged In** – An Ethernet WAN device is now attached.
- **Ethernet WAN Unplugged** – An Ethernet WAN device has been removed.
- **Failed Login Attempt** – Someone attempted to log into the device administration pages locally and failed. *Sample alert: An attempt to log in as the admin user from 192.168.0.142 has failed.*
- **NetCloud OS Upgrade** – The device NetCloud OS has been upgraded.
- **Geo-fence Proximity Change** - Displays whenever the device enters or exits the specified geo-fence.
- **GPIO State Change** - A device GPIO pin has changed state. To update the GPIO configuration, open the configuration pages in **Groups** or **Devices**, select the **System** > **GPIO Configuration** tab. Requires at least NetCloud OS 6.0.2.
- **Intrusion Activity** – This is only relevant for devices with CP Secure Threat Management. Whenever the Threat Management deep packet inspection engine detects an intrusion, the event is recorded in the logs. These events are grouped together for 15 minutes and then reported in NCM, so even if you select "Immediately" in the Interval field below, an emailed alert might not arrive for approximately 15 minutes

after an intrusion. Intrusion Activity alerts include the intrusion details and the action taken by the engine (e.g., "Blocked"). To edit Threat Management settings, open the configuration pages in **Groups** or **Devices** and select **Network Settings > Threat Management**. For more information about Threat Management, visit the **Knowledge Base article**.

- **IP Address Banned** – If the Ban IP Address setting is turned on for a device and someone from a particular IP address attempts and fails to log into the device administration pages six times, that IP address will be banned for 30 minutes. To enable this setting, open the configuration pages in **Groups** or **Devices** and go to **System Settings > Administration**. Open the **Router Security** tab and click on **Advanced Security Mode**. Select the Ban IP Address option.
- **IPS Engine Failure** – This is only relevant for devices with CP Secure Threat Management. In the unlikely event that the Threat Management engine fails, an alert is logged. You can set the router to either allow or deny traffic with a failed engine; to edit this setting, open the configuration pages in **Groups** or **Devices** and select **Network Settings > Threat Management**. For more information about Threat Management, visit the **Knowledge Base article**.
- **Modem WAN Connected** – A modem WAN device is now active.
- **Modem WAN Device Plugged In** – A modem WAN device is now attached.
- **Modem WAN Device Unplugged** – A modem WAN device has been removed.
- **Modem WAN Disconnected** – A modem WAN device is no longer active.
- **Modem WAN Standby** – A modem WAN device is now in standby. This means the modem is connected to the carrier, but is not sending any data. A modem in standby will failover faster than a modem not in standby. Standby can be turned on in the router's configuration in the **Connection Manager** grid.
- **Reboot** – Displays when the device has been rebooted. *Sample alert: The device has been rebooted*.
- **Rogue Access Point Detected** - Displays after running a WiFi site survey when a rogue access point not marked as known is detected broadcasting the same SSID as the device running the site survey. This helps identify potential access point hijacking, evil twin, and man-in-the-middle WiFi attacks.
- **Router App Custom Alert** - A custom alert that is generated by the custom code inside a router app.
- **Router App Execution State Changed** - A router app that is running on a group goes into a different execution state (start, stop, error, etc.).
- **Unexpected Router App Installed** - An unexpected router app is found installed, an expected router app is unexpectedly uninstalled, or a router app unknown to the system is found installed.
- **Successful Login** – A user has logged into the router locally (requires at least NetCloud OS 5.0.1).
- **Temperature Limit Exceeded** – For products with an internal temperature sensor (COR IBR1100 and IBR1150) and configured temperature limits, this alert displays when one of those limits is reached. To set these temperature limits for the COR IBR1100 Series, open the configuration pages in **Groups** or **Devices**, select **System Settings > Administration**, and click on the **Temperature** tab.
- **Unrecognized Client** – A client with an unrecognized MAC address has attempted to connect to the device. MAC logging must be enabled for this alert to display. In the configuration pages, go to: **Network Settings > MAC Filter/Logging** to enable MAC logging.
- **WAN Service Type** – A WAN device has changed its service type, such as switching from 3G to 4G. Possible service types include: DHCP, LTE, HSPA+, etc. *Sample alert: The lte-2ae6ec8e service type has changed to LTE*.
- **WiFi as WAN Connected** – WiFi as WAN is now active.
- **WiFi as WAN Disconnected** – WiFi as WAN is no longer active.
- **WiFi as WAN Network Available** – A WiFi as WAN network is now attached.
- **WiFi as WAN Network Unavailable** – A WiFi as WAN network has been removed.

For alerts to appear in this log, they must be assigned under **Settings**.

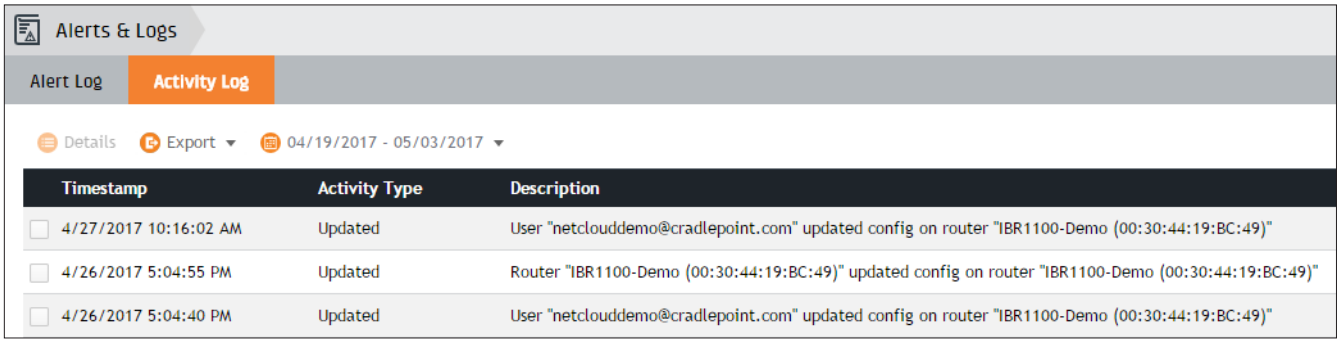
To drill down into a subset of this list, select a date filter or click on a particular Device name, Product type, Group name, or Account name: only alerts from that subset of devices display.

COLUMNS

To edit the columns displayed, click on the columns selection icon in the top right corner. This opens a complete list of the available columns. To customize your grid, select or deselect column titles.

ACTIVITY LOG

Activities consist of initiators, activities, and targets. Activity Log entries are stored for 30 days. *NOTE: Initiators and targets are also known as actors and objects respectively. References to actors and objects can be found in the activity details and csv exports.*



Activity entries are descriptions of the form “initiator_type initiator activity target_type object”.

For instance, the activity entry for creating a user would be: User “Mike” created user “Bill”.

The initiator types are:

- **System** - The NCM system
- **User** - A User in the NCM system
- **API Key** - A request using an API key
- **Router** - A router that has been registered with NCM

The activity types (with examples) are:

- **Created** - User “Mike” created group “Group 1”
- **Deleted** - User “Mike” deleted group “Group 1”
- **Updated** - User “Mike” updated fields “name” on group “group 1”
- **Requested** - User “Mike” requested control.ping.stop on router “2100-14d” (00:11:22:33:44:55)
- **Reported** - Router “2100-14d” (00:11:22:33:44:55) reported NetCloud OS change to 6.1.0
- **Logged In** - User “Mike” logged in
- **Logged Out** - User “Mike” logged out
- **Register** - Router “2100-14d” (00:11:22:33:44:55) registered with NCM
- **Unregister** - Router “2100-14d” (00:11:22:33:44:55) unregistered with NCM

The target types (with examples) are:

- **Account** - User “Mike” created account “Subaccount 1”
- **User** - User “Mike” deleted user “Bill”
- **Group** - User “Mike” updated fields “name” on group “Group 1”
- **Router** - User “Mike” updated fields “name” on router “Router 1” (00:11:22:33:44:55)
- **Schedule** - User “Mike” created schedule “Schedule 1”
- **Task** - User “Mike” created task
- **API Key** - User “Mike” created API key “API key 1”

- **Network Interface** - 'Router "Router 1" (00:11:22:33:44:55) updated fields "modem_fw" on network interface "lte-a22f73cd"'
- **Alert Notification** - User "Mike" updated fields "users" on alert notification
- **Feature** - User "Mike" created feature "ANALYTICS" for account "Account 1"
- **Authorization** - User "Mike" created authorization "admin" for api key "API key 1"

To drill down into a subset of this list, select a date filter or click on a particular Initiator Type, Initiator, Activity Type, Target Type, or Target.

EXPORT

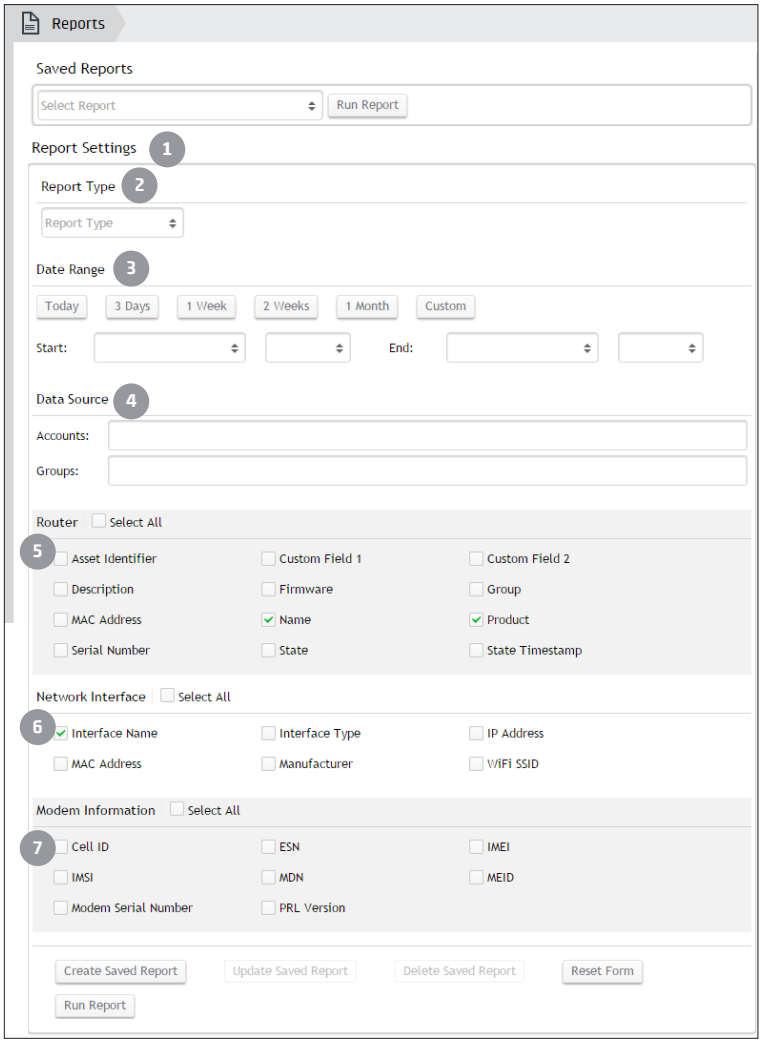
Custom Report - Export activity log information as a CSV file from the reports page.

COLUMNS

To edit the columns displayed, click on the columns selection icon in the top right corner. This opens a complete list of the available columns. To customize your grid, select or deselect column titles.

REPORTS

Reports allow you to create a summary of information (CSV file) about one or more groups of devices. Customize your reports by selecting the type of report you want, the range of dates, the group(s), and additional fields for identification and then click **Run Report** to view the report. You also have the option to save the settings of a report for future use.



Configure reports using the following parameters:

1. **Report Settings**
2. **Report Type**
3. **Date Range**
4. **Data Source**
5. **Router**
6. **Network Interface**
7. **Modem Information**

SAVED REPORTS

If you have saved report settings, select from the dropdown list. This will automatically populate the report settings based on your saved report. Click **Run Report** to view the report. You can make changes to these settings before running the report.

REPORT TYPE

Select from the following report types: Alert History, Data Usage and Signal Quality.

ALERT HISTORY

Includes the type of alert and the date the alert was created.

Allows any date range within the last 90 days.

The following fields are included in Alert History reports:

- created_ts – The timestamp when the row's information was created; includes date and time.
- alert_type – The type of alert (e.g. login_failure, login_success, config_change).

DATA USAGE

- Includes bytes in, bytes out, the date, and the number of samples.
- Allows any date range within the last 90 days.
- The following fields are included in Data Usage reports:
  - **bytes_in** – Amount of data input transferred during the time interval for the network interface.
  - **bytes_out** – Amount of data output transferred during the time interval for the network interface.

- **day** – The UTC date. One line in a data usage report represents one 24-hour period beginning at midnight UTC. Depending on the device's time zone, a "day" might begin at, e.g., 8:00 p.m. local time. (Compare your local time to the **current UTC**.)
- **sample_count** – The number of samples taken over that 24-hour period. By default these samples are taken every hour, but heavy data usage can cause more frequent reports. You can edit the default sample frequency in **Groups** under the **Settings** tab (see Enable Usage Reporting).

SIGNAL QUALITY

The modem connection statistics we report are specific to different technologies (e.g. LTE) and carriers (e.g. Verizon), so not all modems will display information for all of the available fields. The measure of a connection depends on multiple values that measure signal strength and quality. See this **Cradlepoint Knowledge Base** article for more information about RSSI, CINR, SINR, and ECIO.

- Includes signal strength both as a percentage and in dBm (RSSI), SINR, CINR, ECIO, RSRQ, RSRP, and the timestamp.
- Allows date ranges of 1-7 days within the last 90 days.
- The following fields are included in Signal Quality reports:
  - **net_device__service_type** – The service or technology type of the network interface (e.g. LTE).
  - **signal_strength** – This is a percentage that gives an overall evaluation of the signal received by the modem. This number is mapped to the number of bars displayed on the device LEDs and in the device administration pages (e.g., if the percentage is 100, the device will show four bars – see **this article** for more details). This value depends on the technology and carrier, as different modems provide different signal strength/quality information, and the percentage values are defined by the carrier.
  - **dbm** – This is the signal strength, or **RSSI** (received signal strength indicator) measured in dBm. For most modems, the minimum acceptable value is dBm > -85 (values closer to 0 are better).
  - **sinr** – **Signal to Interference plus Noise Ratio**. This is a measure of the quality of the signal, taking into account interference and noise. SINR is specific to LTE. SINR is positive, and higher numbers are better. (Minimum acceptable value: dB > 7)
  - **cinr** – **Carrier to Interference plus Noise Ratio**. This is a measure of the quality of the signal, taking into account interference and noise. CINR is specific to WiMAX. CINR is positive, and higher numbers are better. (Minimum acceptable value: dB > 9)
  - **ecio** – **Ec/Io** is a measure of the signal quality used with multiple technologies including HSPA+ and EVDO. It is the ratio of the received energy of the carrier to the overall interference, expressed as a logarithm (i.e. Ec/Io = $\log_{10}$[Effect energy / (total energy + noise)]). This value will be negative: numbers closer to 0 are stronger signals. (Minimum acceptable value: dB > -10)
  - **rsrp** – Reference Signal Receive Power is an LTE-specific measure of signal strength, similar to RSSI. Because of the way it is calculated, it measures lower than RSSI.
  - **rsrq** – Reference Signal Receive Quality is an LTE-specific measure of signal quality that works in conjunction with RSRP. It is a ratio of the RSRP to the total received power, including unwanted noise.
  - **created_ts** – The timestamp when the row's information was created; includes date and time.

ACTIVITY LOG

- Includes the type of activity and the date the activity was created.
- Allows any date range within the last 30 days.
- The following fields are included in Activity Log reports:
  - **created_at** – The timestamp when the row's information was created; includes date and time.
  - **actor_type_name** – The type of actor (e.g. "user", "api_key", "system").
  - **actor_name** – The actor name (e.g. an NCM user's login, a device's name, an api key label).

- **activity_type_name** – The type of activity (e.g. “created”, “deleted”, “updated”).
- **object_type_name** – The type of object (e.g. “account”, “user”, “group”).
- **object_name** – The object name (e.g. an NCM user’s login, a device’s name, an api key label).
- **actor_type** – The actor type identifier (e.g. “system”, “user”, “api_key”).
- **actor_id** – The actor identifier.
- **activity_type** – The activity type identifier.
- **object_type** – The object type identifier.
- **object_id** – The object identifier.
- **attributes** – Extra information in JSON format.

DATE RANGE

Every report will have a starting and ending date and time. You can manually set these, or select one of the buttons to auto-fill the date range:

- Today
- 3 Days
- 1 Week
- 2 Weeks
- 1 Month

For each of these auto-fill buttons, the end time is midnight at the end of today (UTC), and the start time is calculated in 24 hour increments from that time.

You can use the auto-fill buttons as a starting place and then edit the dates or times as desired.

DATA SOURCE

Every report is mapped to one or more accounts or groups of devices. Select the account(s) and/or group(s) by clicking in one of the input boxes (or on the words “Accounts” or “Groups”). This will open up a window with a list of accounts and groups. Check the box next to each account/group you want included in the report. You do not have to select accounts and groups separately; they will automatically fill the appropriate box.

Select from the following device identifier fields. Use these selections to keep track of which data is associated with which device (router, network interface, or modem) in the CSV file. A few fields – **Name, Product**, and **Interface Name** – are included by default. Deselect any of these fields to keep them out of a report.

Click the box next to the category title to toggle between selecting all or none of the fields in that category.

ROUTER

- **Asset Identifier** – Optional field that is often used for asset tracking and inventory management. You can change this identifier in the **Devices** section.
- **Custom Field 1, Custom Field 2** – Customize these fields in the **Devices** section.
- **Description** – This is a user-defined description of the device, editable in the **Devices** section.
- **NetCloud OS** – The NetCloud OS version.
- **Group** – The name of the group the device is in.
- **MAC Address** – The MAC (media access control) address uniquely identifies a device. *Example: 00:30:44:15:ff:76*.
- **Name** – By default, this is of the form: MBR1400-f76 or IBR600-52b (the last three characters are the last three characters of the MAC address). You can change these names in the **Devices** section. This is included by default.
- **Product** – Product type (e.g. IBR600). This is included by default.

- **Serial Number** – The router serial number. This field might not be populated for some routers.
- **State** – A recent status for the device (e.g. "online").
- **State Timestamp** – The timestamp when the state was evaluated.

NETWORK INTERFACE

NOTE: The network interface selections are only available for certain types of reports.

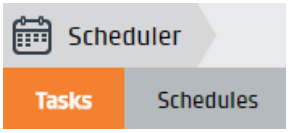
- **Interface Name** – ethernet-lan, ethernet-wan, wlan-wireless0, etc. Cellular modems include an identifier (e.g. lte-cec5ffa7). This is included by default.
- **Interface Type** – Ethernet, WLAN, LTE, WiMax, etc.
- **IP Address** – The IP (Internet Protocol) address of the network interface. *Example: 10.143.127.234*.
- **MAC Address** – The MAC address of the network interface. *Example: 00:30:44:15:ff:76*.
- **Manufacturer** – The modem manufacturer (e.g. Pantech; Cradlepoint for integrated modems).
- **WiFi SSID** – The "service set identifier," or "network name," for a local WiFi network.

MODEM INFORMATION

NOTE: The modem information selections are only available for certain types of reports.

- **Cell ID** – The **Cell ID** is a number used to identify the base transceiver station.
- **ESN** – **Electronic serial number** – older identification number for CDMA, replaced in newer devices by MEID. "Pseudo" ESNs (pESN) that are not necessarily unique can be generated from the MEID when an ESN is needed.
- **IMEI** – **International Mobile station Equipment Identity** – unique identifier for LTE, HSPA+, and GSM technologies.
- **IMSI** – **International Mobile Subscriber Identity** – unique identifier for SIM cards. This is typically displayed as a 15-digit number composed of the mobile country code (MCC), mobile network code (MNC), and mobile subscription identification number (MSIN).
- **MDN** – Mobile Directory Number. This is the phone number associated with the modem.
- **MEID** – **Mobile equipment identifier** – unique identifier for CDMA technologies. An MEID allows hexadecimal digits and is 56 bits long (14 hex digits).
- **PRL Version** – **Preferred Roaming List** version number.
- **Modem Serial Number** – This is a modem identifier that pulls from the other identifiers (it usually matches the IMEI or ESN). In the CSV report this is labeled net_device_gsn. The advantage of this identifier is that it is always populated for cellular modems.

SCHEDULER



TASKS

Add, edit and delete scheduled tasks. Set up schedules on the Schedules page that can then be assigned to a scheduled task.

ADD

Click Add at the top left to create a new scheduled task. This opens another screen where the following options will need to be chosen:

- **Task Type** - Select the type of task to be completed during the scheduled time. Options include: Update Group NetCloud OS.
- **Group** - Select the Group(s) to run the task on. *NOTE: More than one Group can be selected but a separate task will be created for each Group selected.*
- **NetCloud OS Version** - Select the version of NetCloud OS you would like the group to upgrade to when the scheduled task runs. If multiple groups for multiple products are selected then the list will populate with NCOS versions common to all products selected. If there are no common NCOS versions an error will appear and fewer groups will need to be selected.
- **Schedule** - Select the Schedule the task should run on. A new Schedule can also be created on this screen.

EDIT

Select one Task from the grid and click Edit to edit the Schedule of the currently selected Task. There are two options to choose from:

1. **Run as scheduled** - Do not make any changes and run the scheduled task with the schedule already assigned.
2. **Use a different schedule** - Select a different schedule to use for the task. This will open another dialog where another schedule can be selected.

DELETE

Select one or more Tasks from the grid and click **Delete** to delete the task(s).

COLUMNS

To edit the columns displayed, click on the columns selection icon in the top right corner. This opens a complete list of the available columns. To customize your grid, select or deselect column titles.

The following columns are available:

- **Task** - The task type.
- **Schedule** - The schedule assigned to the task.
- **Start On** - The date and time the task will run.
- **Group** - The group the task will run on.

SCHEDULES

Add, edit and delete scheduled tasks. The Schedules page is where you can manage schedules that can be used for scheduled Tasks.

ADD

Click Add at the top left to create a new Schedule. This opens a dialog where Name, Description, and Start On can be set.

EDIT

Select one Schedule from the grid and click Edit to edit that Schedule. The same fields are available as adding a new Schedule.

DELETE

Select one or more Schedules from the grid and click Delete to delete the schedule(s). Warning: This will also delete any scheduled Tasks that were using the selected Schedule(s).

COLUMNS

To edit the columns displayed, click on the columns selection icon in the top right corner. This opens a complete list of the available columns. To customize your grid, select or deselect column titles.

The following columns are available:

- **Name** - Name of the schedule.
- **Description** - Description of the schedule if added by the user.
- **Start On** - The first time the schedule will run.
- **Last Run** - The last time the schedule ran.
- **Created** - When the schedule was created.

TOOLS

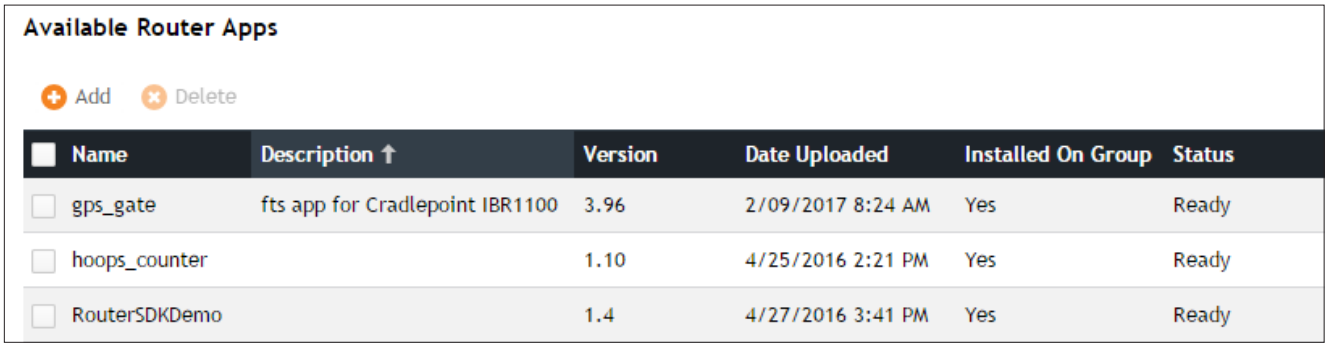
ROUTER APPS

Cradlepoint Router Apps allow developers to add custom functionality to groups of routers. Testing application code can be done on a router that is in Developer Mode. Developer Mode routers cannot be in a group.

WARNING: Router apps can introduce security and other potential issues when not carefully engineered. Test your code thoroughly before deploying it to production routers.

AVAILABLE ROUTER APPS

A list of Router App files uploaded to the account.



- **Add** ⊕
  Click the Add button to upload a new app. This opens the Add Router App dialog where a .tar.gz file can be selected and uploaded. The file must be less than 2 MB in size. Also, make sure that the .tar.gz file includes a manifest file that has a unique App Name and Version. Otherwise, the app will most likely fail the validation process.
- **Delete** ✖
  Select an app and click the Delete button to delete an app. Apps with an Error status will not be automatically deleted, they will remain in the list until manually deleted.
- **Columns** ⁞⁞⁞
  To edit the columns displayed, click on the columns selection icon in the top right corner. This opens a complete list of the available columns. To customize your grid, select or deselect column titles. The following columns are available:
  - **Name** – The name of the app. This is pulled from the manifest file.
  - **Description** – The description of the app. This is pulled from the manifest file.
  - **Version** – The version of the app. This is pulled from the manifest file.
  - **Date Uploaded** – The date the app was uploaded to NetCloud Manager using the **Add** button on this screen.
  - **Assigned To Group** – This column displays whether or not the app has been deployed to a group of routers or not. Apps must be deployed to groups from the **Groups** page.
  - **Status** – The app upload status. Possible statuses include:
    - **Uploading** – This appears when the app is still being uploaded.
    - **Validating** – The app has been successfully uploaded and is now going through the validation process. This can take anywhere from 2 to 30 seconds.
    - **Ready** – The app has passed the validation process and is ready to be deployed to a group of routers.
    - **Error** – There was an issue when trying to upload or validate the app. If the status says "Error" then clicking the text will open a dialog with more details as to why the upload failed.

DEVELOPER MODE ROUTERS

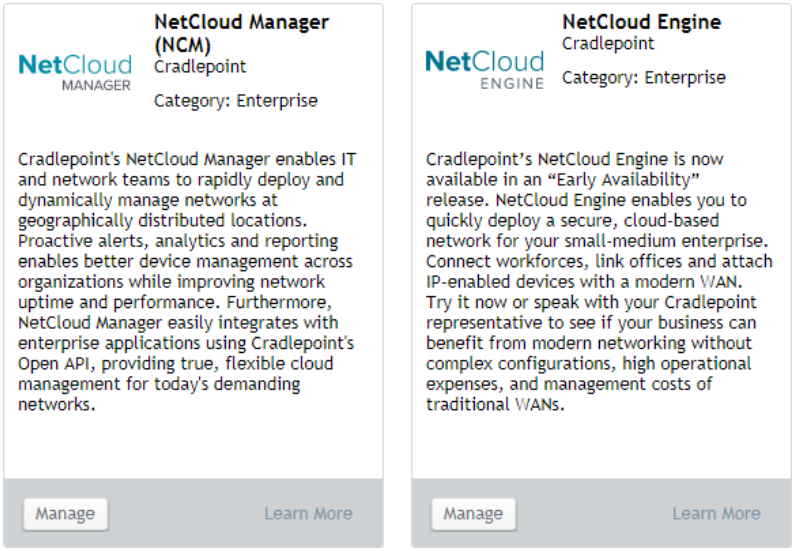
A list of routers that are currently in Developer Mode. Testing application code can be done on a router that is in Developer Mode. Developer Mode routers cannot be in a group.

- **Add** ⊕
  Click the **Add** button to select a router to turn on Developer Mode. Routers must not be assigned to a group in order to be eligible to have Developer Mode turned on.
- **Remove** ✖
  Select a router and click the **Remove** button to turn off Developer Mode for that router.

APPLICATIONS

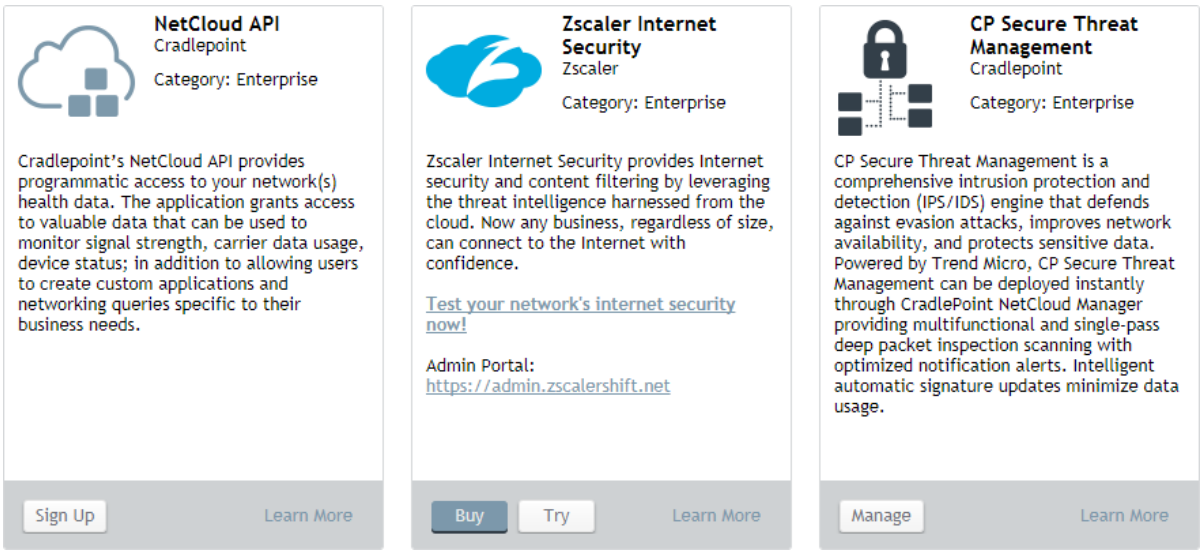
SERVICES

Services represent core functionality of the NetCloud platform. Services can be used independently or combined to fit business needs. Services are offered in two tiers; Standard or Prime, with Prime offering additional features and capabilities. Services can be evaluated free for 30 days.



APPLICATIONS

Applications extend the capabilities of NetCloud Services by delivering purpose-driven features for security, software development and more. Applications are add-ons to NetCloud Services and cannot be tried or purchased until the dependent NetCloud Service is tried or purchased.



BUTTONS

Try – The Try button steps through the process of starting a 30-day trial. If an Application is an add-on to a Service, the Try button will be disabled until the dependent Service is triad or purchased.

Buy – The Buy button starts the process of buying the selected Service or Application. If an Application is an add-on to a Service, the Buy button will be disabled until the dependent Service is purchased.

Manage – The Manage button directs users to the appropriate page within the NetCloud platform to manage the Service or Application.

Buy More – The Buy More button starts the process of buying more licenses for the selected Service or Application.

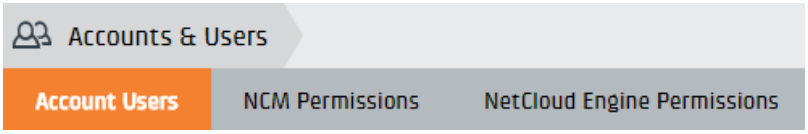
Learn More – The Learn More button shows information about the Service or Application, including key features, requirements and supported products.

EXPIRATIONS

When a Service or Application expires, access and visibility to it will end. Upon Service expiration, you'll see changes to the main navigation, the Service tile will display an expiration notice, and Application tiles may display notices that the dependent Service has expired. Upon Application expiration, the Application tile will display an expiration notice. To resume your Service and/or Application, click the **Buy** button.

NOTE: Services and Applications can only be tried by a primary account administrator.

ACCOUNTS & USERS



ACCOUNT USERS

Add and edit account users. User Administrator privileges are required to create additional users. A User role only has access to the account with which it is associated.

ADD A USER

To add a user to the current account, click (**Add**, upper-left corner). Choose from **User** or **User Administrator** in the dropdown menu, then press **Save**.

EDIT A USER

Once a user has been selected, user-specific account attributes can be modified by selecting (**Edit**).

USER PERMISSION LEVELS

There are two levels for user permissions:

- **User:** Users have full access to the account they are in.
- **User Administrator:** Same access as users except they can create/edit other users.

Accounts can be filtered by selecting either **All, Enabled** or **Disabled** from the **Filter** dropdown menu.

NCM PERMISSIONS

Add, edit, and delete NCM accounts and users. The top-level account is simply the name of your designated account with Cradlepoint (typically the name of your organization). Administrators create any additional subaccounts.

Users are associated with a particular account. Users have access to the account they are associated with as well as any nested subaccounts.

ADD A SUBACCOUNT OR USER

Every subaccount and user must be inside a specific account. First select an account and then click (**Add**, upper-left corner). Choose from **Subaccount, User**, or **Collaborator** in the dropdown menu.

ADDING A COLLABORATOR

After adding a collaborator they will show up in the grid but the First Name, Last Name and Email will be starred out until the user accepts the request to be a collaborator. Before the collaborator accepts the request, the collaborator's role may still be changed by selecting the collaborator and clicking **Edit**. The collaborator may also be removed by selecting the collaborator and clicking **Delete**. This does not delete the user's root account but simply removes collaborator access from the currently logged in account.

USER PERMISSION LEVELS

There are four levels for user permissions:

- **Administrator:** Administrators have full access to the account they are in, along with all subaccounts within that account.
- **Full Access User:** Full access users have the same access as administrators except they cannot create/edit other users or subaccounts. The Accounts & Users tab is not visible for these users.
- **Diagnostic User:** Cannot make any configuration changes or change settings; can only view information within NCM, run reports, and perform the diagnostics activities of rebooting routers, performing pings or traceroutes, and running speedtest. The **Accounts & Users** tab is not visible for these users.
- **Read Only User:** Cannot make any configuration changes or change settings; can only view information within NCM and run reports. The **Accounts & Users** tab is not visible for these users.

EXPORT

Export activity log information as a CSV file. Choose from **Changes initiated by user** and **Changes on user**.

Changes initiated by user will export activity log entries where the user is the activity initiator. **Changes on user** will export activity log entries where the user is the target of the activity.

NETCLOUD PERIMETER PERMISSIONS

USER PERMISSION LEVELS

There are two levels of user permissions:

- **Administrator:** Administrators have full access to manage the NetCloud Perimeter Services. Their credentials can be used to login to the web UI, and can be used to authenticate NetCloud Clients, and connect to the overlay network.
- **Member:** Can use their credentials to authenticate NetCloud Clients and connect to the overlay network. They can login to the web UI, but will be unable to administrate the NetCloud Perimeter services until they are promoted as NetCloud Perimeter Admins on this screen.

NETCLOUD PERIMETER

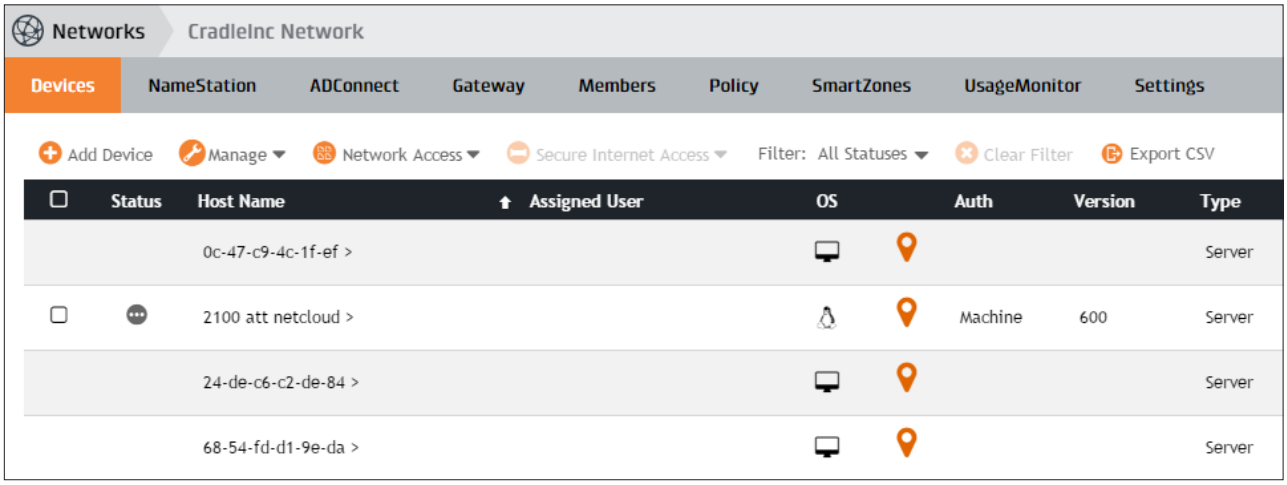
NetCloud Perimeter (NCP) is a software-defined, identity-based security perimeter to connect M2M and IoT devices to your network. NetCloud Perimeter (NCP) is a software-defined, identity-based security perimeter to connect M2M and IoT devices to your network. NCP allows you to connect a wide range of devices — Windows, Mac, Linux, iOS, Android, and IoT — regardless of location. Standing up an overlay network is now a matter of minutes, rather than hours or days. NCP also works across any carrier and transport (MPLS, broadband, wireless).

DEVICES

The **Devices** pane displays status information about the devices on your Cradlepoint NetCloud Perimeter network. Devices can be either end-user devices used to connect to the Cradlepoint NetCloud Perimeter network or servers in your branch, data center, or cloud.

Columns provide information pertaining to **Status, Host Name, Assigned User, OS, Authentication, Version, Type, IPv4 Address, IPv6 Address**, and **Subnet**. If **Secure Internet Access** is entitled, you will also see status information on whether Secure Internet Access VPN connectivity is enabled for each device.

To add a device, click the ⊕ (**Add**) button.



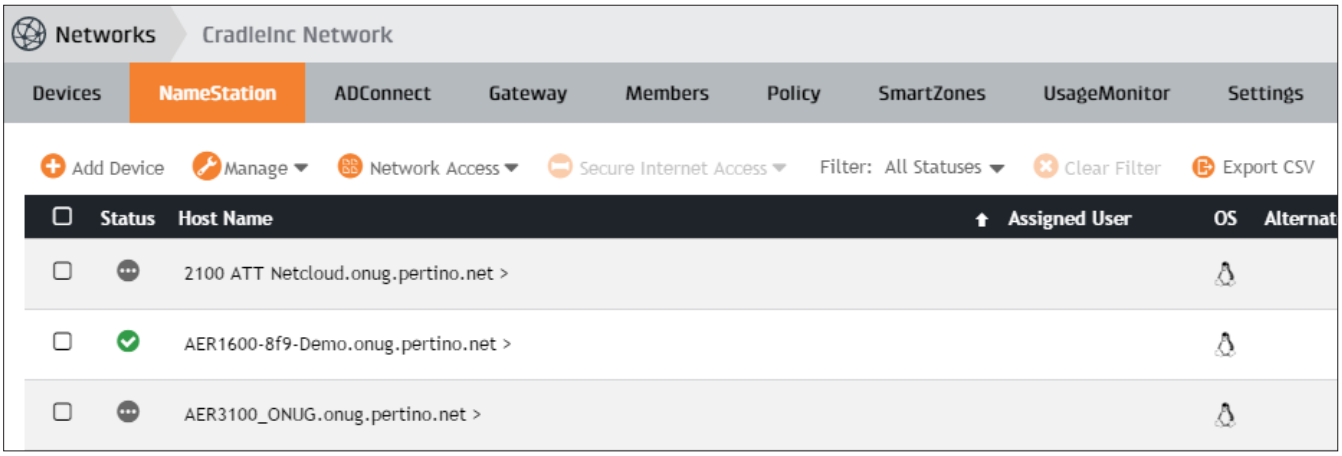
Selecting a device allows you to perform the following operations:

ICON	DEFINITION
	Remove Device
	Assign Device
	Convert
	Reauthenticate
	Approve

ICON	DEFINITION
	Reject
	Toggle Secure Internet Access
	Clear Filter
	Show Duplicates
	Export CSV (see Appendix for more information)

NAMESTATION

Every device on a Cradlepoint NetCloud Perimeter network receives a default DNS name so that other members of the network can access it using the fully qualified domain name (FQDN). NameStation allows the network administrator to choose a custom subdomain and assign aliases to network resources.

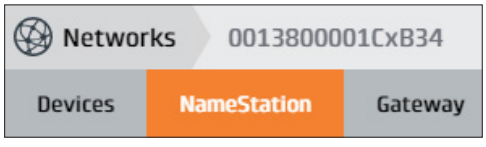


DEFAULT DNS NAMES

- Each NetCloud virtual cloud network is assigned a short subdomain such as *2q1k5f*.
- Each device's fully qualified domain name is in the form of *hostname.subdomain.pertino.net*, so a computer named "Katie-pc" would be *katie-pc.2q1k5f.pertino.net*.

USING NAMESTATION

1. Select the **NameStation** tab.



2. Select the check box of device(s) for which you want to create alternate names.

3. Click the ✎ (**Edit**) icon to add as many as three alternate names.
4. Click **Save**.
5. Once you have added a custom name, devices on your network can be accessed at the new DNS names.

ADDING ALTERNATE NAMES TO SERVERS

For servers, you have the option of adding additional DNS names or aliases. For example, you may have a server that is used for both an intranet site and as file server on your network.

- If its hostname is *server3*, it would be accessible at *server3.acmecorp.pertino.net*.
- You could add two alternate names of files and intranet to make access easier for your users. Now, *files.acmecorp.pertino.net* and *intranet.acmecorp.pertino.net* both point to your server.

ADCONNECT

With ADConnect, you can easily make Active Directory services available to remote users. This app lets you specify which AD Name Servers to use over Cradlepoint NetCloud Perimeter so that your remote devices know how to reach your domain controllers. In just three steps, you can provide domain access for remote devices without policy updates, DNS changes, or firewall configuration.

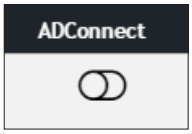
DNS is the key to making Active Directory services available to remote clients. When remote clients can use the same DNS servers as computers on your local network, they are able to fully participate in all Active Directory functions including authentication and file access.

HOW IT WORKS

- When ADConnect is enabled, client computers connecting to the NetCloud virtual cloud network are instructed to use the specified DNS servers for name resolution.
- Active Directory takes care of all name resolution and replication. Once clients are using AD servers for name resolution, they will get any updates you make to your Active Directory in real time.
- Active Directory DNS servers will ensure clients get the right name resolution depending on their location.
- Local clients (on your private IP address space) will be instructed to connect locally.
- Remote Cradlepoint NetCloud Perimeter clients will be instructed to connect using Cradlepoint NetCloud Perimeter IP address space.

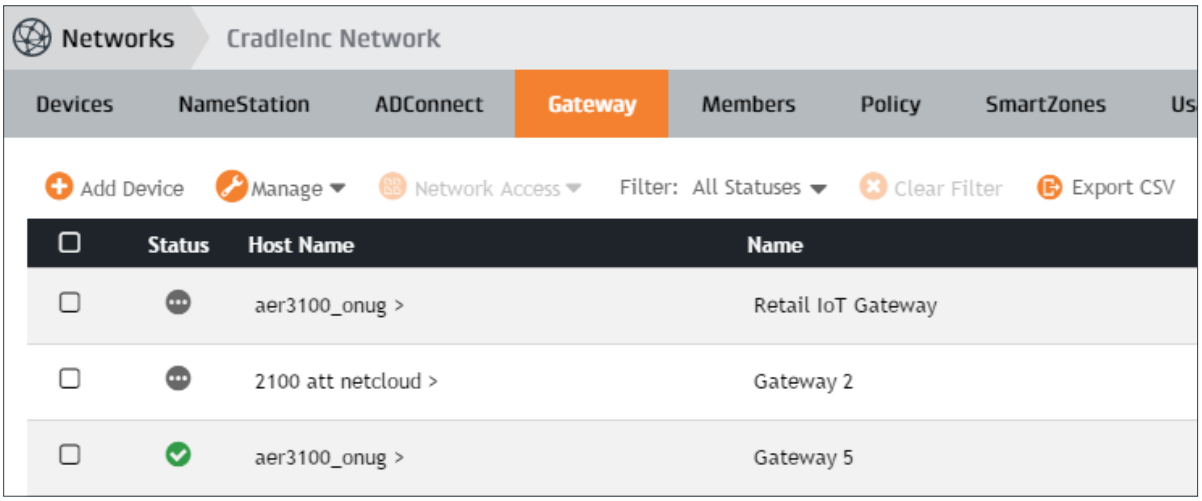
USING ADCONNECT

1. Install the NetCloud Client on your Active Directory member servers, including both DNS and application servers.
2. Activate the ADConnect app by changing the **ADConnect** toggle on the right-hand side of the screen.



GATEWAY

For systems and machines (such as printers and servers) that do not support the Cradlepoint NetCloud Client, Cradlepoint has developed the Gateway feature.



NOTE: The Cradlepoint NetCloud Gateway can be deployed locally or in AWS. For specific instructions on deploying in AWS, please consult http://www.cradlepoint.com/support.

The Gateway enables deployments including:

- Customers who have specific policies that prohibit 3rd-party clients to be installed on devices such as servers.
- Products that do not support the installation of the Cradlepoint NetCloud Client such as printers, security cameras, or time-card machines.
- Remote users located in remote physical networks needing access to IT devices (such as databases or applications).
- Local users on the same or different subnets requiring access to similar devices where the Cradlepoint NetCloud Client cannot be installed.

NOTE: The Cradlepoint NetCloud Gateway is a Linux-only release. The following are the supported system requirements:

- Linux Ubuntu Server 12.04
- 64-bit
- 4 cores
- 4 GB RAM

WARNING: To enable Gateway, Cradlepoint NetCloud Perimeter modifies entries in the `/proc/sys/net/` file system. These changes remain in place but will not persist across a reboot. Administrators should be aware that these modifications may occur at any time when a Cradlepoint NetCloud Client has been installed. Please consult **http://www.cradlepoint.com/support** for more information.

CONFIGURING YOUR ROUTER

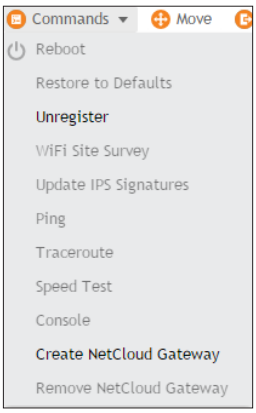
To enable communication between your network and the NetCloud Gateway, add a route. This usually involves command-line or web access to a router's configuration. A typical CLI command might look like this:

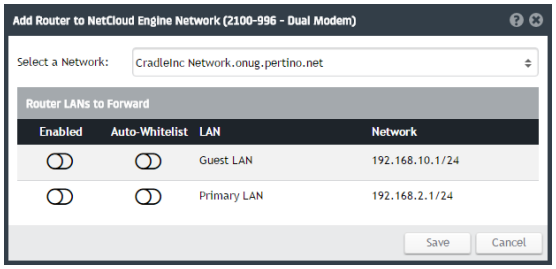
```
$ ip route 50.203.224.0 /24 10.10.130.10
```

where 10.10.130.10 is the IPv4 address of the Cradlepoint NetCloud Gateway. To enable connectivity to the Cradlepoint NetCloud Gateway, add this static route to the site router configuration or to an Amazon VPC route table.

CREATE NETCLOUD GATEWAY

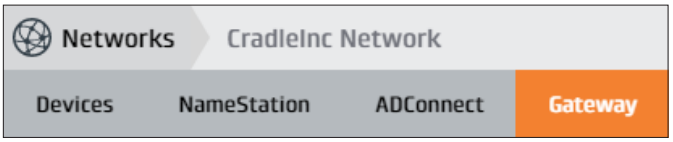
1. Select the **DEVICES** panel in NCM.
2. Select a device and then select **Commands** in the top toolbar and **Create NetCloud Gateway** in the dropdown menu to add the device to the NetCloud Perimeter Network.
3. Select which LAN(s) to forward, then select **Save**.



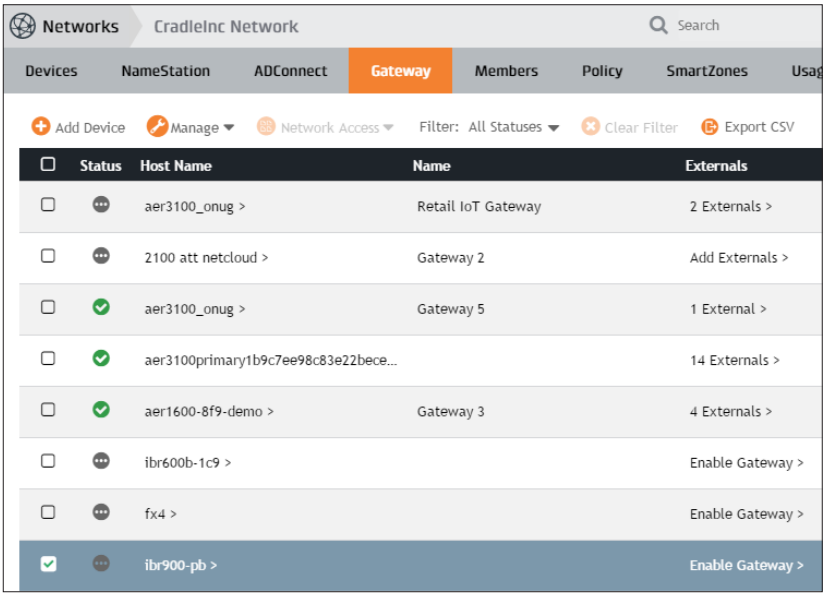


ENABLE AND CONFIGURE NETCLOUD GATEWAY

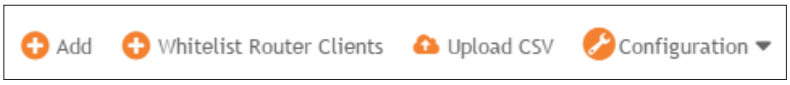
1. Select **NETCLOUD PERIMETER** panel in NCM.
2. Select the **Gateway** panel from top menu.



3. Click **Enable Gateway** from the **Externals** column.

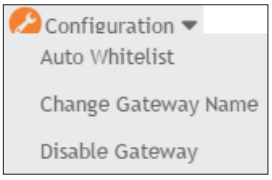


4. To add an external, click **Add**.



5. Enter **Hostname**, **Name**, and **External IPv4**.

6. To whitelist all router clients, click **Whitelist Router Clients**.
7. To add multiple externals, click **Upload CSV**. Ensure CSV file contains the following information, in order: Hostname, Name, and External IPv4.
8. To **Auto Whitelist**, **Change Gateway Name**, or **Disable Gateway**, click **Configuration**.



MEMBERS

The **Members** tab allows you to view member information. Information includes:

- **Username**
- **Email**
- **Number of devices**
- **Status**
- **Role**

Additionally, you can click on the username to view data usage.

POLICY

The security policy feature allows you to segment your network using rules and policies, further increasing security. These rules are similar to network Access Control Lists (ACLs) or firewall rules, where access is allowed or denied between a source and destination devices.

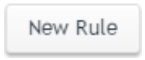
NOTE: All rules are analyzed in order, e.g. rule 1, then rule 2, then rule 3, etc. For example, if your first rule is to allow access to "ANY" device and your second rule is to deny access to a device, the second rule will not be "hit". Changing the order of the rules will ensure the correct policy is applied.

Cradlepoint adds an additional layer of segmentation through the Services feature, allowing you to specify a specific service via well-known port/protocol combinations or via a list of nearly 1,500 applications.

NOTE: This feature offers "type-ahead", where applications and services are selected via characters that you enter in the selection panes.

SPECIFYING A RULE

1. To create a rule, click the **New Rule** button. An empty rule appears with a rule number automatically supplied.

2. Enter a name for the rule. The rule name you enter should be descriptive so that it enables you and other administrators to understand what the rule is intended to do.
3. Select a **Source** and a **Destination**. Multiple entries for each may be specified. The drop-down box allows for selection of displayed entries, but you may also enter specific values.
4. Select a **Service**. You may select from well-known services that are displayed by default, or you may use type-ahead to specify your own.
5. You may also choose to specify a custom service using the + icon immediately to the right of the **Service** menu.

   - Enter a **Service Name**, a **Description**, the **Protocol**, **Start Port**, and **End Port** in the **Custom Services** dialog box.
   - You may specify more than one service by clicking on **New Service**.
   - When finished, click **Add Services**.
6. Choose whether to **Allow** or **Deny** traffic between the **Source** and **Destination**.
7. Select the **Enable** toggle to enable the rule.
8. Click **Apply Policy**. Alternately, you may add additional rules before applying multiple policies.

You may delete the rule by clicking the × next to the Policy.

After you have added security rules and finalized your security policy, you can change the default **Allow** rule to a **Deny** rule, ensuring that only the traffic you have specified will be permitted.

NOTE: The default rule cannot be deleted. Its order cannot be changed—it will always be the last rule in the policy list.

SMARTZONES

A SmartZone enables a client on a virtual cloud network to achieve optimal traffic paths through a local network if a local network is available to communicate with other devices. In other words, SmartZones are designed for remote users who occasionally come into central or branch offices from time to time and don't want network traffic to traverse the overlay network when there is a local—and possibly better performing—network. Only network administrators can configure SmartZones.

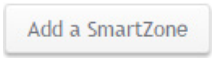
NOTE: Once you add a SmartZone and then save it, clients will be provisioned with their SmartZone membership immediately.

Once configured, devices located in the same SmartZone will always use the local network path while communicating with each other. Devices outside the SmartZone will use the Cradlepoint network to connect.

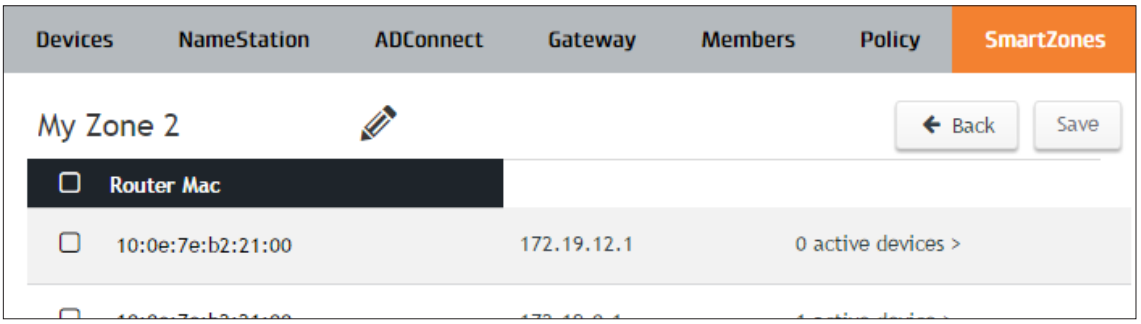
If you have enabled ADConnect, you should configure SmartZones for all networks where local devices and remote devices may connect. This way, when your remote users come into the office, their connection will automatically know to use the LAN rather than the Cradlepoint NetCloud Perimeter network.

To add a SmartZone, follow these steps:

1. Click the **Add a SmartZone** button at the upper-right.



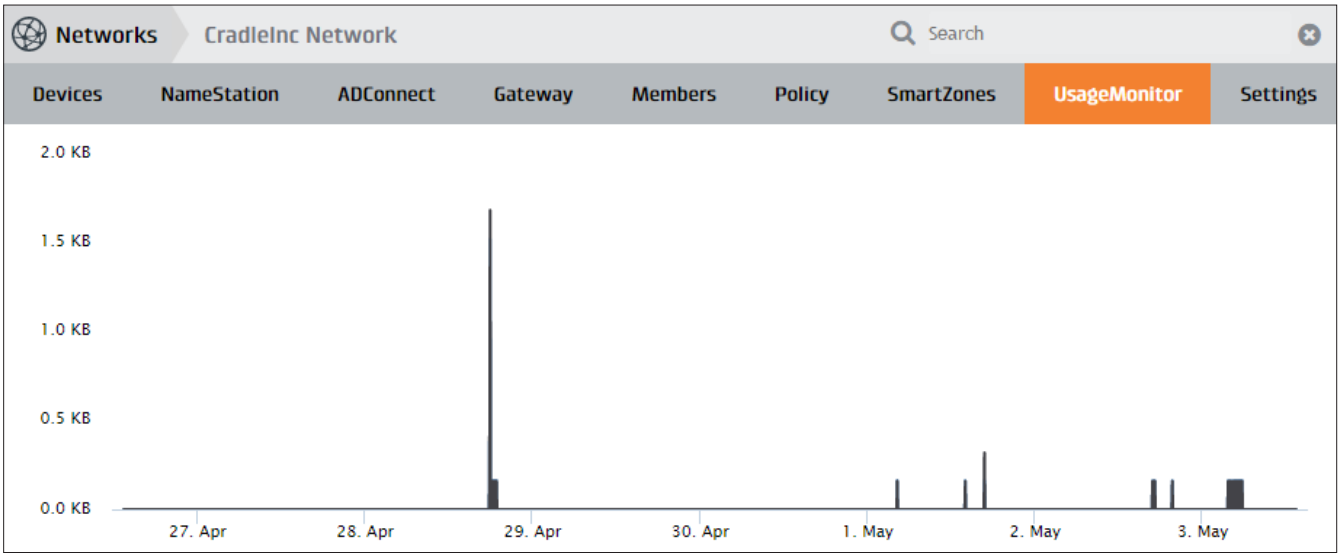
2. Click the (**Edit**) icon to name your SmartZone.



3. Select device(s) you wish to add. *NOTE: Devices may belong to only one SmartZone.*
4. Click **Save** to add the SmartZone.

USAGEMONITOR

The UsageMonitor lets you see how much data is flowing across your entire virtual cloud network. You can view the whole network at once, or drill down into individual members or devices.



MAIN CHART

The main chart shows the total volume of traffic across the entire network. Click on a point in the chart to display the top devices at that time. If you see a spike in data usage in the main chart, you can click on the peak to see what device or devices were most active during the spike.

TOP USERS

The Top Users section shows the top five users and the amount of data they have transferred. Click on a user to drill down and get detailed information about their data usage and which devices they are using.

TOP DEVICES

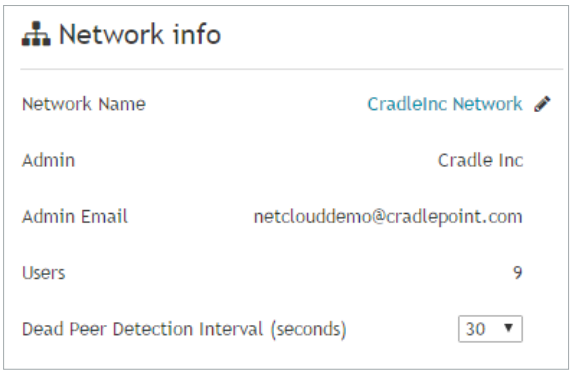
Like Top People, the Top Devices section shows the top five devices and the amount of data they have transferred across the virtual cloud network. Click on a device to drill down.

SETTINGS

List of your account settings, including Network Info, NameStation, and Entitled Services.

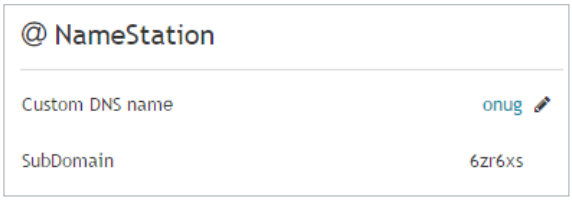
NETWORK INFO

- **Network Name** - Click (**Edit**) to change Network Name
- **Admin**
- **Admin Email**
- **Users**
- **Dead Peer Detection Interval (seconds)** - Select from 30, 60, or 300 seconds



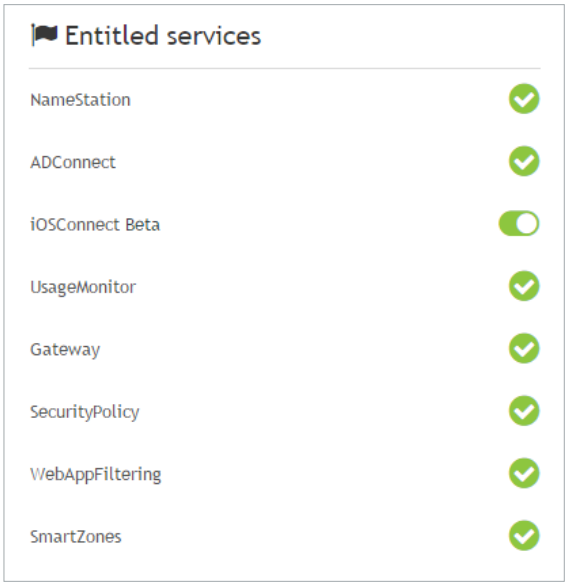
NAMESTATION @

- **Custom DNS name** - Click (**Edit**) to change Custom DNS name
- **SubDomain**



ENTITLED SERVICES

- **NameStation**
- **ADConnect**
- **iOSConnect Beta**
- **UsageMonitor**
- **Gateway**
- **SecurityPolicy**
- **WebAppFiltering**
- **SmartZones**
- **NAC**
- **Secure Internet Access**

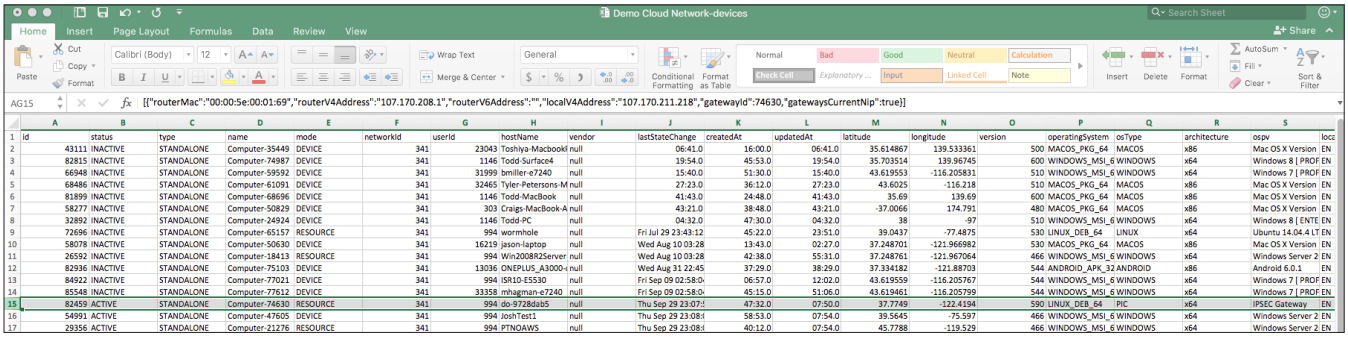


APPENDIX

NETCLOUD PERIMETER CSV EXPORT

The Devices tab in NetCloud Perimeter provides information on each of the devices in your virtual cloud network. Information such as host name, assigned user, OS, and other data about each device is available. However, should you wish to export that information in CSV (comma separated value) format for use in a spreadsheet or database, simply click the (**Export CSV**) button in the top right of the pane.

An example of an exported CSV file is shown below. Please note that this is only a partial view as there are approximately 50 fields.



FIELD	INFORMATION
id	The **id** field is an identification numeral used by the NetCloud Perimeter to uniquely identify the client.
status	The **status** field shows `ACTIVE` if the device is actively participating on the network, or `INACTIVE` if not. A device may also be in a `PENDING` state if the end user has not yet accepted an invitation to join a network.
type	The **type** field indicates the type of device.
name	The **name** field indicates the internal name used by the NetCloud Perimeter to uniquely identify the client.
mode	The **mode** field indicates if the device is a `DEVICE` (e.g., a laptop or an end-user device such as a mobile phone) or a `RESOURCE`, such as a server (e.g., an Active Directory server).
networkId	The **networkId** field is specified by NetCloud Perimeter to uniquely identify the network used by each of the devices.
userID	The **userId** field indicates the user associated with the device. If more than one **userId** is the same, it may be that the device is part of a VPC or similar.
hostName	The **hostName** field gives the name associated with the device. This name is obtained from the Client itself.

FIELD	INFORMATION
vendor	The **vendor** field provides the name of the vendor associated with the device. This field is reserved for future use.
lastStateChange	The **lastStateChange** field provides the timestamp of the most recent state change. A state change may be considered when a device re-connects to the NetCloud Perimeter, such as after a device is activated after being in sleep mode.
createdAt	The **createdAt** field illustrates the time that the device entry was created.
updatedAt	The **updatedAt** field provides a timestamp of when the device's state was last updated.
latitude	The **latitude** field provides the last known latitude for the device.
longitude	The **longitude** field provides the last known longitude for the device.
version	The **version** field indicates the version of the client device.
operatingSystem	The **operatingSystem** field shows the operating system of the client device. Examples include `MACOS_PKG_64` and `WINDOWS_MSI_64`.
osType	The **osType** field provides the known operating system type of the client device.
architecture	The **architecture** field shows the architecture type of the operating system of the client device.
ospv	The **ospv** field provides a detailed view of the operating system of the client device.
locale	The **locale** field shows a basic identifier of the device's known geography.
userEmail	The **userEmail** field gives the email address of each of the devices on the network.
userFullName	The **userFullName** gives the name of the owner or user of the device on the network.
assignedDevice	The **assignedDevice** field indicates that the device is assigned by the administrator. There are two identifiers: • `FALSE` identifier means that the device was not assigned by the administrator, but was an invited device associated with a user. • `TRUE` identifier means that the device was assigned by the administrator, most likely through a network automation deployment tool such as Puppet or Chef.

FIELD	INFORMATION
assignedUserId	The **assignedUserID** field indicates a non-zero numeral assigned by NetCloud Perimeter internally to identify a device assigned by the administrator.
assignedUserName	The **assignedUserName** field shows the name assigned by the administrator if the device is an **assignedDevice**.
assignedUserEmail	The **assignedUserEmail** address is the email address defined by the administrator if the device is an **assignedDevice**.
ipv4Address	The **ipv4Address** field shows the IPv4 address assigned by NetCloud Perimeter to the device.
ipv6Address	The **ipv6Address** field shows the IPv6 address assigned by NetCloud Perimeter to the device.
vanityFQDN	The **vanityFqdn** field is the custom name (or vanity name) assigned by the administrator to the specific device. This often helps in identifying similar types of devices.
alternateNames	The **alternateNames** field shows any alternate names assigned by the administrator to the device, if any.
authMode	The **authMode** field indicates what type of authentication is associated with the device. • `USER_AUTH` indicates that the device is authenticated with user credentials • `MACHINE_AUTH` indicates that the device is authenticated through machine-generated credentials
registeredByUserId	The **registeredByUserId** field is a non-zero numeral assigned by NetCloud Perimeter to identify devices on the network.
nipGroupId	The **nipGroupId** (network info fingerprint) field associates the device with a SmartZone. If the numeral is non-zero, the device is part of the specified SmartZone. If the numeral is zero, the device is not part of a SmartZone.
gatewaySupportEnabled	The **gatewaySupportEnabled** field indicates if the device has Gateway functionality enabled. • `TRUE` indicates that the device is currently functioning as a Gateway • `FALSE` indicates that the device is currently not functioning as a Gateway
displayName	The **displayName** field indicates the Gateway name as displayed in the management view.
clientId	The **clientId** field is assigned by NetCloud Perimeter to identify the device and its relationship to a Gateway.

FIELD	INFORMATION
external	The **external** field indicates whether the device is associated with a Gateway. • `TRUE` indicates that the device is currently associated with a Gateway • `FALSE` indicates that the device is currently not associated with a Gateway
externalIpv4Address	The **externalIpv4Address** is an address assigned by NetCloud Perimeter for use by the Gateway feature.
activeDirectoryServer	The **activeDirectoryServer** field indicates whether the device is an Active Directory server. • `TRUE` indicates that the device is currently part of an Active Directory server • `FALSE` indicates that the device is currently not part of an Active Directory server
ipAddress	The **ipAddress** field is the client's WAN IP address that is visible to NetCloud Perimeter. This address is typically assigned to the Internet-facing WAN device.
lastActiveTimeStamp	The **lastActiveTimeStamp** field provides the timestamp of the most recent transition to the **ACTIVE** state.
nacStatus	The **nacStatus** field indicates whether the device has been accepted or rejected on to the network via the Network Access Control feature.
hostNameConflict	The **hostNameConflict** field indicates whether the device has a conflict with a hostname of a device already part of the network.
currentNetworkId	The **currentNetworkId** field is deprecated.
networkName	The **networkName** field indicates the network the device is associated with.
isOwner	The **isOwner** field indicates if the device is owned by the user. A value of `TRUE` means that the device itself is owned by the user.
appEntitlements	A series of sub-fields, the **appEntitlements** column indicates the application entitlements, such as **Content Filtering** and **GeoView**, that are associated with each device.