



Digi aView

User Guide

Revision history—90002319

Date	Description
January 2019	Initial release of Digi-branded version of the <i>Digi aView User Guide</i> .
May 2019	Updated for Digi aView version 3.16.1.
April 2020	Updated for Digi firmware release 20.2. ■ With firmware release 20.2, Active Recovery has been renamed to Digi SureLink™. ■ After upgrading to firmware release 20.2, if a configuration erase is performed, the router will default to Digi Remote Manager rather than to aView.

Trademarks and copyright

Digi, Digi International, and the Digi logo are trademarks or registered trademarks in the United States and other countries worldwide. All other trademarks mentioned in this document are the property of their respective owners.

© 2018 Digi International Inc. All rights reserved.

Disclaimers

Information in this document is subject to change without notice and does not represent a commitment on the part of Digi International. Digi provides this document “as is,” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose. Digi may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time.

Warranty

To view product warranty information, go to the following website:

www.digi.com/howtobuy/terms

Customer support

Gather support information: Before contacting Digi technical support for help, gather the following information:

- ✓ Product name and model
- ✓ Product serial number (s)
- ✓ Firmware version
- ✓ Operating system/browser (if applicable)

- ✓ Logs (from time of reported issue)
- ✓ Trace (if possible)
- ✓ Description of issue
- ✓ Steps to reproduce

Contact Digi technical support: Digi offers multiple technical support plans and service packages. Contact us at +1 952.912.3444 or visit us at www.digi.com/support.

Feedback

To provide feedback on this document, email your comments to

techcomm@digi.com

Include the document title and part number (Digi aView User Guide, 90002319 A) in the subject line of your email.

Contents

Introduction

About aView	11
Login page	11
Reset password	11

Site navigation

Navigation panel	13
Account Settings menu	13
Search bar	13
Organization Filter	14
Filter bar	14
Pagination	15
Dashboard	16
Deployment chart	16
Connectivity chart	17
Cellular Network Type chart	18
Signal Strength chart	18
Export a chart	19
Print a chart	19
Maps	20
Devices	21
Device details page	22
Device events	25
Tunnel servers	27
Configurations	28
Reports	29
Report history	29
Notifications	30
Organizations	31
Create a new sub-organization	31
Optional service name	33
Optional logo and footer	34
Roles	34
Permissions	36
Device settings	36
Data plans	37
SNMP probes	37
New User	38
Subscribe to device notifications	38

Sites	39
Users	40
Create a new user	40
Edit a user	41
Manage users	41

Monitoring devices

About monitoring devices	44
Color indicators	44
Deploy a device	44

Cellular devices

About cellular devices	46
Cellular device details	46
Cellular device Configuration tab	47
Cellular device Settings tab	47
Cellular device Associated Devices tab	47
Cellular device Cellular Details tab	47
Cellular utilization chart	49
Cellular device Tunnels tab	49
Cellular device Network tab	49
Cellular device remote commands	50
Cellular device emergency SMS commands	51
Cellular configuration requirements for aView	51
View Cellular configuration profiles	52
Create a new Cellular device configuration profile	52
Apply a Cellular configuration profile	53
Individual device configuration settings	53
Delete a Cellular device configuration profile	54

Dial-to-IP devices

About dial-to-IP devices	56
Dial-to-IP device details	56
Dial-to-IP device Configuration tab	56
Dial-to-IP device Associated Devices tab	56
Dial-to-IP device Tunnels tab	57
Dial-to-IP device Network tab	57
Dial-to-IP device remote commands	58
Dial-to-IP configuration requirements for aView	59
View Dial-to-IP configuration profiles	59
Create a new Dial-to-IP device configuration profile	60
Apply a Dial-to-IP configuration profile	60
Individual device configuration settings	61
Delete a Dial-to-IP device configuration profile	61

Legacy cellular devices

About legacy cellular devices	63
Legacy cellular device details	63
Legacy Cellular device Settings tab	64

Legacy Cellular device Configuration tab	64
Legacy Cellular Associated device tab	64
Legacy Cellular device Cellular details tab	65
Cellular utilization chart	66
Legacy Cellular device Tunnels tab	66
Remote commands	66
Legacy Cellular device emergency SMS commands	67
Remote power commands	67
Legacy Cellular configuration requirements for aView	67
Create a new Legacy Cellular configuration profile	68
Apply a cellular configuration profile	69
Delete a configuration profile	69

VPN Gateway devices

About VPN Gateway devices	71
Configure down status for VPN gateway devices	71
VPN Gateway device details	72
VPN Gateway WAN utilization	73
VPN Gateway device Settings tab	73
VPN Gateway devices Associated Devices tab	73
VPN Gateway devices Cellular Details tab	74
VPN Gateway device Cellular Utilization chart	75
VPN Gateway device Tunnels tab	75
VPN Gateway device Location tab	76
VPN Gateway device Intelliflow tab	76
VPN Gateway Connectivity Tests tab	76
VPN Gateway IDS tab	77
VPN Gateway Remote commands	77
VPN Gateway configuration requirements for aView	78

Remote Manager devices

About Remote Manager devices	80
Remote Manager device details	80
Remote Manager Configuration tab	81
Remote Manager device Settings tab	81
Remote Manager Associated devices tab	81
Remote Manager Cellular Details tab	81
Cellular utilization chart	82
Remote Manager Tunnels tab	83
Remote Manager Network tab	83
Remote Manager device remote commands	84
Remote Manager device emergency SMS commands	85
Remote Manager configuration requirements for aView	85
View Remote Manager configuration profiles	86
Create a new Remote Manager device configuration profile	86
Apply a Remote Manager configuration profile	87
Individual device configuration settings	87
Delete a Remote Manager configuration profile	88

WiFi devices

About WiFi devices	90
WiFi device details	90
Associated devices tab	90
Rogue access points tab	91
Configuration	91
WiFi configuration requirements for aView	91

uCPE devices

About uCPE devices	93
uCPE device details	93
Configuration tab	93
uCPE device Settings tab	93
Associated devices	94
uCPE device Cellular Details tab	94
Cellular utilization chart	95
uCPE device Tunnels tab	96
uCPE device Network tab	96
uCPE device remote commands	96
uCPE device emergency SMS commands	97
uCPE configuration requirements for aView	98
View list of uCPE configuration profiles	98
Create a new uCPE device configuration profile	99
Apply a uCPE configuration profile	99
Individual uCPE device configuration settings	100
Delete a uCPE configuration profile	100

Adding devices to aView

Add a gateway device	102
Add devices	102

Generating reports

Availability report	105
Create an availability report	105
Cellular network type report	106
Create a cellular network type report	106
Cellular signal strength report	107
Create a cellular signal strength report	107
VIG report	108
Create a VIG report	108

Controlling device down status

About device down status in aView	111
Configure down status options for devices	111
Grace Period Interval option	112
Heartbeat Interval option	112
Examples: Adjusting device down status	112

Configure down status for VPN gateway devices	113
---	-----

Manage User Preferences

Changing your password	114
Managing Notifications	114
Notification subscriptions	115
Notification profiles	115

Managing User Access

Workflows

Staging for initial connectivity	125
Goal	125
Setup	125
Staging via WAN Port	125
Local Staging	126
Subscribing to alerts	128
Goal	128
Setup	128
Notification Profiles	129
Cellular Notifications	129
Notification Subscriptions	130
Adjusting alerts for downed devices	130
Goal	130
Setup	131
Adjusting the Grace Period	131
Creating new organizations	132
Goal	132
Setup	132
Add a new Sub Organization	133
Grant admin permissions	135
Populate the new organization	137
Duplicating device configurations	139
Permissions between organizations	141
Goal	141
Setup	141
Overview	142
Roles with Limited Abilities	142
Permissions for Other Organizations	143
Assigning Permissions to Users	145
Offline cellular connectivity test	146
Background	146
Config Setup	146
Scheduled testing of inactive SIM slot	148
Design	148
Config Setup	149
aView tunnel alternatives	150
Overview	150
Cellular signal strength threshold test	160
Goal	160
Background	160

Config Setup	160
--------------------	-----

API

Managing your token	163
Limitations	163

Release notes

Version 3.16.1	165
Version 3.14.1	165
Version 3.12.1	166
Version 3.12.0	167
Version 3.10.0	167
Version 3.9.2	168
Version 3.9.1	168
Version 3.9.0	169
Version 3.7.8	170
Version 3.7.1	171
Version 3.6.12	172

Introduction

About aView	11
Login page	11
Reset password	11

About aView

aView is a sophisticated, but intuitive cloud-based portal that monitors remote data network devices across Tier 1 carriers and service providers. In today's environment the configuration, installation, and central management of complex distributed networks is a challenge for businesses. The challenge increases for businesses with multiple locations, which now may span multiple time zones and countries. To complicate matters further many locations may not have any support staff on-site.

aView provides a company with one system to monitor and remotely control VPN Gateways, Cellular Extenders, WiFi Extenders, and Dial-to-IP devices. The system has a powerful user interface that allows sorting and searching in order to improve productivity and identify problem patterns. In addition to standard reports, online views can be exported to create ad hoc reports. Data is provided on over 50 items regarding the availability, performance, configuration and location of your devices. Remote devices can be configured in groups or individually, and the firmware easily updated from a central operations center. Based on user criteria the portal can also send real-time alerts to defined e-mail addresses.

The system's mapping functions provide a visual picture of a customer's network status at any given time. The maps can be zoomed in and out to display finer levels of granularity all the way to a single site. The device can then be selected from the map for further analysis and control. Mapping is also used for site location information, along with the physical address and contact information.

Managing large enterprises, distributed enterprises, and mid-market networks alike is simple with aView. As long as a site has a connection to the Internet, you are ready to remotely manage its devices. aView lives in the cloud and utilizes up to date secure technology. This is especially important in large distributed enterprises, where there could be thousands of locations. Your infrastructure can be monitored and controlled by multiple administrators who are geographically dispersed, each with appropriate permissions.

Login page

To login:

1. Go to <https://aview.accns.com>.
2. Enter in the email address associated with your login and your password.

Login credentials are assigned and managed by your account administrator. If you do not have a login setup, please contact your administrator.

The footer, which appears throughout the aView site, includes a copyright along with the version of aView that is currently running. A link to the aView Terms of Service is also provided.

Reset password

To reset your password:

1. Go to <https://aview.accns.com>.
2. Enter the email address associated with your account.
3. Click **Forgot your password?**
4. Confirm your email address and click **Send**.

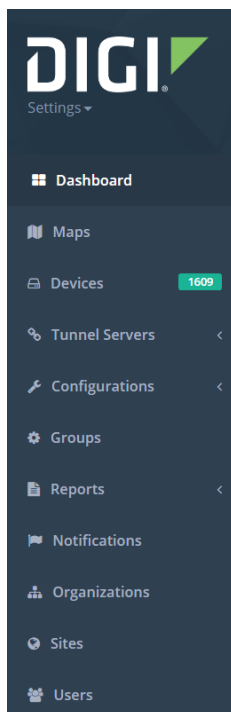
You will receive an email with instructions on how to reset your password. If you do not reset your password within 72 hours of receiving the email, you must reset your password again using the **Forgot your password** link.

Site navigation

Navigation panel	13
Search bar	13
Organization Filter	14
Filter bar	14
Pagination	15
Dashboard	16
Maps	20
Devices	21
Tunnel servers	27
Configurations	28
Reports	29
Notifications	30
Organizations	31
Sites	39
Users	40

Navigation panel

The navigation panel, which is found on the left side of every page, provides access to the main menu with links to sections of the aView application. Several of the items have sub-menus that allow the user to further narrow the selection.



Account Settings menu

The first menu item in the navigation panel is the user account's **Settings** menu.

Account

The **Settings** menu at the top of the Navigation panel includes the **Account** item, where a user can access manage their user profile, change their password, and log out from the system. See [Manage User Preferences](#) for information about your user profile.

Logging out of the aView application

The **Settings** drop-down at the top of the Navigation panel includes a **Logout** button. Clicking on this will log you out of aView.

Search bar

In the toolbar at the top of each page of the aView site is a **Search** box that can be used to locate specific devices or sites. Type the desired value, press Enter, and the selected entries will be displayed. The search tool will match on the following fields:

- MAC address
- Serial Number

- Modem ICCID
- Site ID

The **Advanced Search** link can be used to search for a device or site by more specific details; including location, IP address, phone number, site ID, and cellular modem details.

Organization Filter

aView makes extensive use of the structure called the **organization**. An organization is a term used to associate devices, sites, users, and configurations together. A sub-organization is a term that describes an organization that is accessible under a higher level organization.

By default, the aView application displays information related to all organizations that you have access to. To limit the organizations that are displayed:

1. On the tool bar, click the Filter button (▼).
2. Click **Search for organization....**
3. Type at least the first three letters of the organization. A list of organizations that match the string is displayed.
4. Select the organization from the list.
5. Click **Apply**.

All displays throughout the aView application will now be limited to the selected organization and any of its sub-organizations. To return to viewing information for all devices, click the Filter button again and click **Clear**.

Filter bar

Many pages in the aView application have a filter bar at the top of the page that allows you to narrow the list of items displayed on the page.

The type of filters changes depending on the type of detail being displayed. The items that can be filtered are listed when you click on the filter bar. Multiple filters can be applied at once. Once a filter is selected, the results on the page will automatically be filtered and refreshed.

You can remove the applied filters by clicking the **x** on the filter bar. The applied filters only apply to the current page; if the user goes to a different page and comes back, the filters will be reset.

Some filters require the user to type in a value to be filtered on, such as the MAC address filter for devices.

- Device-related filters:
 - **Categories:** The category of devices (such as gateway, cellular, or WiFi).
 - **Deployment:** What state the device is in (deployed or undeployed).
 - **Firmware:** The firmware version of the device.
 - **Hostname:** The network hostname of the device.
 - **MAC:** The MAC address of the device.
 - **Model:** The device model type (such as 8200 or 6200-FX)
 - **Organization:** Filters based on the organization name.
 - **Site:** The site name associated with the device.

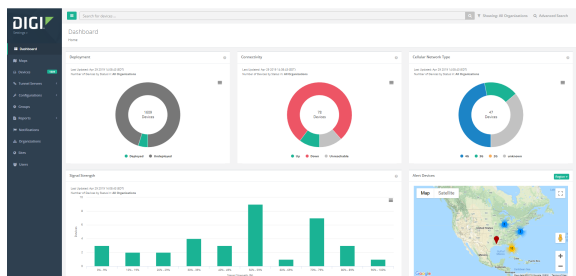
- **Status:** What status the device is in (such as up or down). Note, the status only applies to deployed devices.
- Event related filters:
 - **Level:** The severity level of the event. Each event is tagged with a certain severity level to indicate the importance of the event (such as notice or alert). Severity levels are listed in the filter from lowest severity to highest severity.
 - **Range:** The time range of events to display. The default is to display the events for the past 30 days.
 - **Type:** All events are tagged with a certain type, making it easy to associate similar events together (such as DHCP, tunnel, or reboot).
- User-related filters (available only to users with sufficient privileges to view the **Users** page):
 - **Email:** The email address of the user.
 - **Name:** The name of the user.
 - **Organization:** Filters based on the organization name.
 - **Status:** The status of the user's account in aView. Active indicates that the user has logged in within the past 30 days. If a user has not logged in within the past 30 days, their account is set to inactive. A Pending account indicates the user has never logged in to aView.
 - **Timezone:** The timezone selected by the user for displaying timestamps in aView.

Pagination

Several pages throughout the aView application have pagination, where only a certain number of entries are listed on each page. The number of entries can be controlled by the **Show *n* entries** pagination drop-down, which is always listed at the top-right of the table on the page.

Dashboard

The **Dashboard** page displays several charts and other widgets to provide at-a-glance details for your devices.



Within each chart, clicking on a displayed category will open a table of devices included in that category. The following charts are provided:

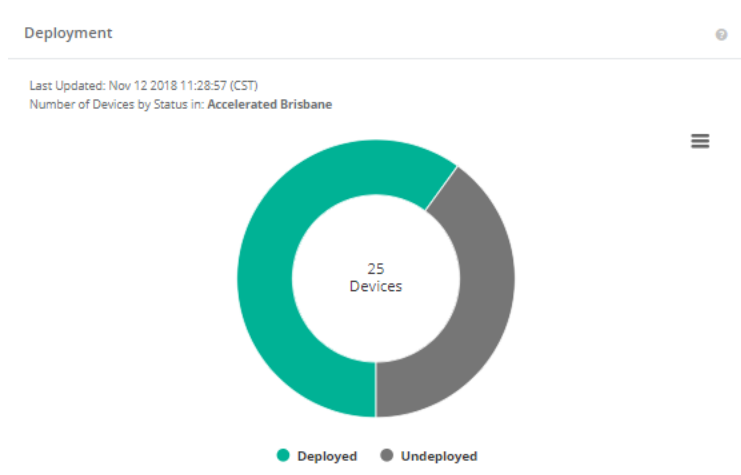
- [Deployment chart](#)
- [Connectivity chart](#)
- [Cellular Network Type chart](#)
- [Signal Strength chart](#)

The **Dashboard** page also provides an **Alert Devices** map widget that displays devices in an alert status. You can zoom in and out within the map, and select different regions to display. Click on a status indicator to open a window containing detailed information on the device. From within the window, you can click on the Organization name, the device's MAC address, or the Site ID to open associated pages. Devices in an alert state are also listed in tabular form at the bottom of the **Dashboard** page.

Note The dashboard page does not automatically refresh, so the devices listed in on the dashboard page were in alert status at the time of when the page loaded. If the page is left alone for an extended period of time, the listed devices in alert state may become outdated.

Deployment chart

The Dashboard **Deployment** widget displays a donut-style chart that provides a breakdown of deployed and undeployed devices in the organization. A device's deployment status indicates whether or not aView should provide active monitoring and alerts for the router.

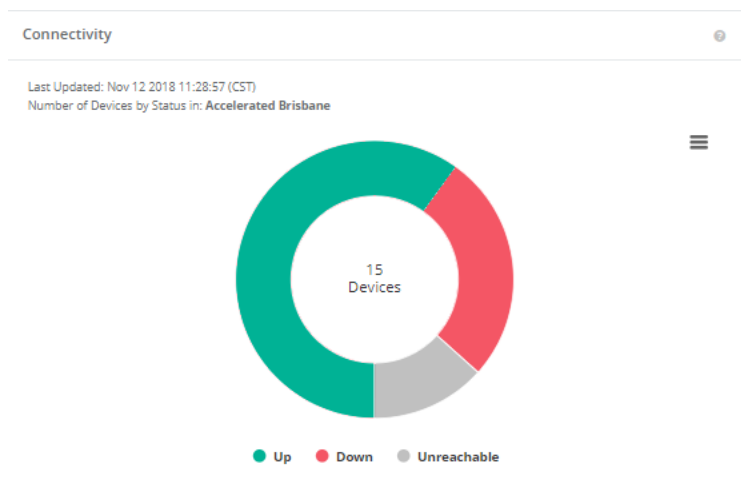


Click on an area in the chart to open the **Devices** page listing all of the organization's devices with this deployment status.

- **Deployed:** Indicates the number of devices that have been deployed, which means that they will be monitored based on the events that are sent by the device, and will also generate notification alerts based on the events received and your access to the device. In the **Devices** page, devices that have been deployed will be listed with a particular deployment status (for example, Up, Down, or Inactive). Further dashboard information is provided for deployed devices in the [Connectivity chart](#) and [Cellular Network Type chart](#).
- **Undeployed:** Indicates the number of devices that have not been deployed, which means that they should not be monitored. aView will list details and events for undeployed devices, but these events will not generate any notification alerts. Undeployed devices will be listed in the **Devices** page with a pause icon (⏸) as their status.

Connectivity chart

The Dashboard **Connectivity** widget displays a donut-style chart that provides a breakdown of the connectivity status of deployed devices in the organization. The chart only reports on the main statuses of **Up**, **Down**, and **Unreachable**.



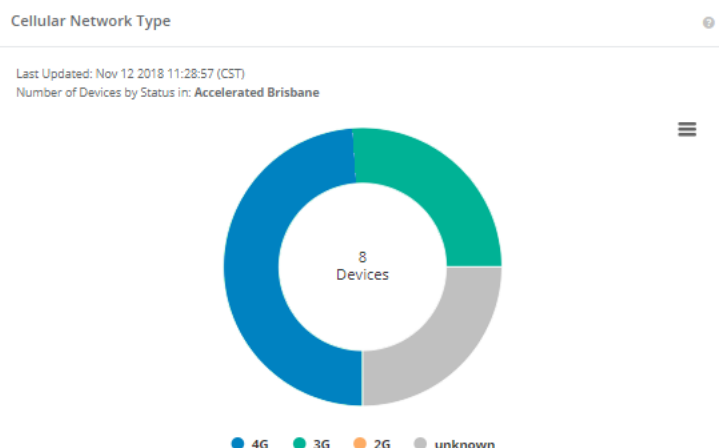
Click on an area in the chart to open the **Devices** page listing all of the organization's deployed devices with this connectivity status.

- **Up:** The device is online and is reachable through aView.
- **Down:** The device is not reachable through aView.
- **Unreachable:** The device has never checked into aView even though it is in a Deployed state.

Note The **Grace Period Duration** and **Heartbeat Interval** device configuration options control the amount of time that aView should wait before reporting a device as Down. For example, the default **Grace Period Duration** for cellular devices is 109 minutes, and the default **Heartbeat Interval** is 30 minutes. When combined, this means that by default, aView will consider a cellular device to be down if it has not heard from the device in 139 minutes. See [Configure down status options for devices](#) for more information about the **Grace Period Duration** and **Heartbeat Interval** options.

Cellular Network Type chart

The Dashboard **Cellular Network Type** widget displays a donut-style chart that provides a breakdown of the cellular connectivity type for deployed cellular-enabled devices. The type of cellular connection can vary depending on availability of service, quality of connection, and device configuration. You should verify the anticipated connection type and the APN associated with the cellular data plan before troubleshooting a device's type of cellular connectivity.

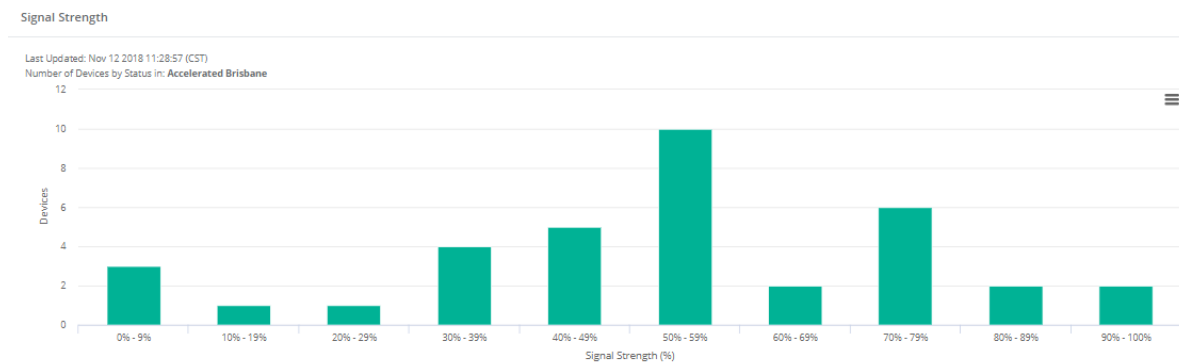


Click on an area in the chart to open the **Devices** page listing all of the organization's devices with this cellular connectivity type .

LTE status indicators on your device displays the device's cellular network type using the same color codes used in **Cellular Network Type** chart. A blue light (solid or blinking) indicates a 4G connection, a green light (solid or blinking) shows the router is on 3G, and so forth.

Signal Strength chart

The Dashboard **Signal Strength** widget displays a bar graph representing the reported signal strength percentage of deployed devices in the organization.



Click on one of the bars in the graph to open the **Devices** page listing all of the organization's devices with this reported signal strength.

Export a chart

Dashboard widget charts can be exported to the following formats:

- PNG image
- JPEG image
- PDF document
- SVG vector image

To export a dashboard widget chart:

1. When a chart is displayed, click ≡ (Chart menu).
2. Select the appropriate **Download** type from the menu.

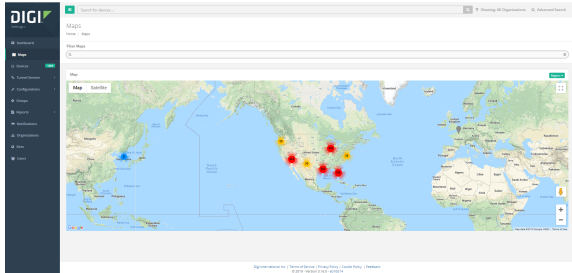
Print a chart

To print a chart:

1. When a chart is displayed, click ≡ (Chart menu).
2. Select **Print chart**.
3. Fill in print options and click **Print**.

Maps

The **Maps** page displays the graphical view of monitored devices on a world map. The maps allows a user to drill down on specific units and their current status. When global devices are being managed, a specific country or region can be selected.



The **Maps** page displays the status of the various devices visually on a map of the organization's home country. The map can be zoomed in and out to display finer levels of granularity all the way to a single site. The map can be filtered by organization, device category, device type, status, and country/region. Changes can be made to any filter criteria before filtering the map. A user can also toggle the map between a street view and geographical view.

Once the desired devices are displayed a user can obtain more detailed information on a particular site by clicking on the status indicator display. This will display an information bubble with the device type, site ID, and device information. Clicking on the Organization will direct the user to a page that lists all the devices associated with that organization. Clicking on the site ID will direct the user to a page that lists all the devices associated with that site ID in that particular organization.



Devices

The **Devices** page displays the status of all devices that you have access to. Clicking on the **Devices** page menu option in the navigation bar displays a drop-down to specify the type of device. You can also select **All** to display all devices without regard to the device type.

Status	MAC	Primary IP	Category	Model	Organization	Site	Firmware	City	Country	Last Heartbeat (EDT)	Carrier	dBm	Signal	Network	Phone Number
●	00270423988E	97.97.245.255	VPN Gateway	8300	USARMT	NATE HOME TEST	7.0.200		US	Apr 29 2019 14:29:58 (EDT)					
●	002704302587	10.251.3.4	Cellular	6300-MX	Nate Test	Nate Home MX	19.1.134.81	Tampa	US	Apr 29 2019 14:29:57 (EDT)	Novistar	-47	40%	lte (4G)	+18132555311
●	00270420917E	10.120.40.242	Cellular	6300-CX	Zacant		16.7.49		US	Apr 29 2019 14:29:13 (EDT)	ATT	-76	50%	LTE (4G)	18132304720
●	00270420C50A	100.132.8.187	Cellular	6300-SR	Accelerated Test Environment	Jos SR	17.11.125	Toronto	CA	Apr 29 2019 14:15:22 (EDT)	T-Mobile	-99	20%	LTE (4G)	unknown
●	002704269590	10.75.33.194	VPN Gateway	8300	USARMT	WESTCOH AWWOB STAGING UNIT2	7.0.200	KATY	US	Apr 29 2019 13:55:58 (EDT)					
●	00270424A490	192.168.10.120	VPN Gateway	8300	USARMT	NCR AWWOB STAGING UNIT	7.0.200	RENO	US	Apr 29 2019 13:42:51 (EDT)					
●	002704375967	47.206.66.228	VPN Gateway	U115	USARMT	U115 HQ	7.0.200	Tampa	US	Apr 29 2019 13:30:06 (EDT)					
●	00C0CA48D344	10.23.199.229	WIFI	4200-AX	Accelerated Demo		1.621.81	New York	US	Apr 29 2019 12:20:54 (EDT)					
●	00270420C8F2	10.250.1.85	Cellular	6300-SR	Accelerated_Test_Environment	Default	19.8.14.12-DIRTY		US	Mar 13 2019 13:53:59 (EDT)	Verizon	-58	87%	LTE (4G)	+18134600748
●	00270438FD69	192.168.86.147	VPN Gateway	U115	USARMT	JOS WORK FROM HOME U115	7.0.130	Palm Harbor	US	Feb 26 2019 03:19:03 (EST)					
●	00270427C395	10.0.62.200	Cellular	6300-CX	Segethes		19.8.14.124		US	Jan 09 2019 10:50:18 (EST)	YVW	-47	72%	LTE (4G)	918202823
●	00270427AF46		Cellular	6300-CX	Zacant	Default	17.5.108.6		US	Nov 02 2018 16:37:52 (EDT)					
●	002704308096		Cellular	6300-MX	Zacant	Default	17.5.108.6	Greenville	US	Nov 02 2018 16:37:52 (EDT)					
●	00270430C628		Cellular	6300-MX	Zacant	Default	17.5.108.6	Orlando	US	Nov 02 2018 16:37:52 (EDT)					
●	00270427AF42		Cellular	6300-CX	Zacant	Default	17.5.108.6	Bloomington	US	Nov 02 2018 16:37:52 (EDT)					
●	00270427B4C3		Cellular	6300-CX	Zacant	Default	17.5.108.6			Nov 02 2018 16:37:52 (EDT)					
●	00270427B4C0		Cellular	6300-CX	Zacant	Default	17.5.108.6			Nov 02 2018 16:37:52 (EDT)					
●	00270427B4BF		Cellular	6300-CX	Zacant	Default	17.5.108.6			Nov 02 2018 16:37:52 (EDT)					
●	00270427B510		Cellular	6300-CX	Zacant	Default	17.5.108.6			Nov 02 2018 16:37:52 (EDT)					
●	00270427B4C0		Cellular	6300-CX	Zacant	Default	17.5.108.6			Nov 02 2018 16:37:52 (EDT)					
●	00270427B4C3		Cellular	6300-CX	Zacant	Default	17.5.108.6			Nov 02 2018 16:37:52 (EDT)					
●	0027042965CA	10.0.40.65	Cellular	6300-CX	Accelerated Test Environment	P06 customer CX	19.8.14.124		US	Nov 01 2018 18:16:49 (EDT)	VZW	-57	88%	LTE (4G)	9183450036
●	00270427AF46	100.129.187.54	Cellular	6300-CX	Zacant		17.8.128.63	Wimauna	US	Nov 01 2018 17:48:25 (EDT)	T-Mobile	-79	53%	LTE (4G)	unknown

The **Devices** page allows you to display the current status of all devices managed by their organization. The filter bar also allows you to select only a certain category of devices (for example, VPN, WiFi, Cellular).

Once you have selected a category of devices, aView displays a tabular tab of the devices and their current statuses. The filter bar can be used to filter the results, so that only the relevant devices are shown. You can select the organization that should be displayed and then further narrow the results down by filtering on the device type or status.

Devices are listed in the table can include the following details. Display additional details, or hide details, by selecting the wrench icon (🔧) at the top-right of the table.

- **Status:** The status displayed is a color coded indicator. See [Color indicators](#) for details on each status color.
- **MAC:** The MAC address of the device generating the event. The MAC address field is selectable. Clicking this link will direct the user to the device's details page. For additional information about the device's details page, refer to the section of this guide that details the specific device category that is being viewed.
- **Comment:** Provides a bubble icon. Mouse-over the bubble icon to view a comment associated with the device, or click the bubble icon to open a dialog that you can use to enter or edit a comment.
- **Primary IP:** The device's primary IP address.
- **Management IP:** IP address used by aView to manage the device.
- **Hostname:** The WAN IP address of the device. Clicking the link provided in the field will open a new URL with the host as the URL. For example if the host is 172.16.3.2, the URL will be <https://172.16.3.2>

- **Category:** The category of the device.
- **Model:** The model of the device.
- **Organization:** The organization that the device is associated with. A device is assigned to an organization when it is entered into aView. In most cases the organization will be the company or one of its sub-organizations. This field is selectable. Clicking the link in this field will display all the devices associated with that organization and any sub-organizations under it.
- **Site:** The site ID that the device is associated with. Clicking the link in this field will display all the devices associated with that site ID in the same organization.
- **Firmware:** The firmware version the device is currently running on.
- **City:** The city where the device is located.
- **Country:** The country where the device is located.
- **Activation Date:** The timestamp of when the device first reported in to the aView site.
- **Last Heartbeat:** The last time the device has checked in with aView.

Device details page

Clicking on the Device ID (MAC address) of a device will display the device's **Device Details** page. This includes detailed information about the specific device. The following sections describe the details that are found on the **Device Details** page that apply to all categories of devices.

MAC: 0027042DC63A / Site ID: Jos SR

Home / Devices / Cellular / 6350-SR / 0027042DC63A

Cellular 6350-SR

Reports ▾ Actions ▾ Commands ▾ SMS ▾ Pages ▾

Device Details
Configuration
Settings
Associated Devices
Cellular Details
Tunnels
Networks
Location
Contacts
Intelliflow

Organization:	Accelerated Test Environment
Site ID:	Jos SR
MAC Address:	0027042DC63A
Serial Number:	6350010178181755
Status:	Device is up
Model:	6350-SR
Management IP:	172.33.198.58
Uplink IP Address:	100.78.247.210
Terminal:	Terminal on Unit
Firmware Version:	17.11.125
Primary Interface:	wwan1
Activated At:	Jan 11 2018 12:49:22 (CST)
Last Heartbeat:	Nov 12 2018 15:20:19 (CST)
Last Restart:	Jul 30 2018 09:59:30 (CDT)
Data Plan:	Jos' Dataplan 0816
Data Plan Individual Limit:	10.00 MB
Data Plan Usage:	650.14 MB
Comment	This is a second comment.

Settings tab

The **Settings** tab contains attributes that can only be updated if you have the appropriate permissions. If you do not have permissions to edit these settings, this tab will not be listed. If you do have the ability to edit these settings for the device, then the options will be listed in an edit mode, with drop-downs and input text boxes listed. Multiple options can be edited at the same time. Once any desired updates have been made, click **Update Settings**.

Options available in the **Settings** tab vary depending on the device. Common options for all devices include:

- **Organization:** The organization that the device is currently associated with. If the user has the ability to change the device's organization, a button labeled Change will be displayed that, when clicked, will allow a user to move the device to a new organization. When moving the device to a new organization, the user can also optionally copy the device's site and/or data plan (if any).
- **Site ID:** The site ID that the device is associated with. Clicking the link in this field will display all the devices associated with that site ID in the same organization.

Details tab

The **Details** tab contains specific information that identifies the device. The following is a list of details that apply to all devices:

- **Status:** The current status of the device when this page was loaded.
- **MAC Address:** The MAC address of the device.
- **Device Details:** The serial number of the device.
- **Model:** The model of the device.
- **Firmware Version:** The firmware version the device is currently running on.
- **Activated At:** The timestamp of when the device first reported in to the aView site.
- **Last Heartbeat:** The last time the device has checked in with aView.
- **Last Restart:** The last time the device rebooted.

Location tab

The **Location** tab displays the location of the device on a geographical map based on the device's address details. Depending on your permissions, the location details may be listed in a view-only mode, or there will be editable text boxes and drop-downs to update the location if desired.

To add or update a device's location, enter in a valid address into the location details. Once all desired address details have been typed in, click **Update**. The aView application will send the address details to GoogleMaps to validate the address, and the map will be updated.

If Google does not return a valid address, aView will save the address details as entered. However, the aView application will not display a map of the address details since Google did not return valid latitude/longitude coordinates.

Clicking **Clear** will remove the location details for the device and remove the map from the page.

Cellular location

If aView has valid GSM location details for a device with cellular capabilities, a second pin, colored orange, will appear on the map to indicate the location determined using these GSM details.



Cellular location reported by device modem

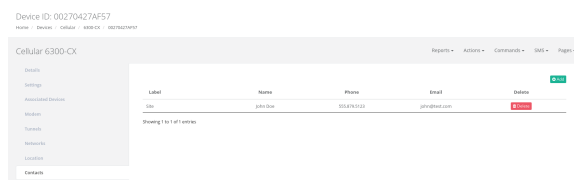
Location entered in form below

Address 1

Address 2

Contacts tab

The **Contacts** tab displays any contacts that are associated with the device. A contact must contain a name and email address, along with an optional phone number. When creating a new contact, the contact can be designated as a general, technical, sales, or site contact. The same contact info can be used for multiple devices. Once a contact is made, the user can apply the same contact to another device by going to the new device's details page, click the green Add button, and then select the appropriate contact from the drop-down list of existing contacts.



Reports menu

The **Reports** menu provides a drop-down list of available reports that can be performed for the device. Available reports vary depending on the device type. See [Generating reports](#) for details on report types.

Actions menu

The **Actions** menu provides a drop-down list of available actions that can be performed concerning the device in aView.

- **Subscribe/Unsubscribe:** Allows a user to subscribe to or unsubscribe from receiving notification alerts from the device. See [Manage User Preferences](#) for details about managing notifications and profiles.
- **Deploy/Undeploy:** Controls the deployment of a device. See [Monitoring devices](#) for details about the deployment status and deploying devices.

Commands menu

The **Commands** menu provides a drop-down list of available remote commands that can be sent to the device. Clicking on a command will execute that command. For a list of available device commands

and details of what they do, refer to the Remote Commands section of the particular device category in this guide.

Pages menu

The **Pages** button provides a drop-down list of pages related to the individual device.

- **Details:** Displays the **Device Details** page. If you are already on the device details page, the page will simply refresh.
- **Events:** Displays the **Events** page for the specific device. See [Device events](#) for details about the **Events** page.
- **Raw Events:** Displays a list of events in raw format.

Device events

The Device **Events** page is displayed by selecting **Pages > Events** on a device's **Device Details** page. This page displays a real-time chronologically sorted table (newest on top) of device events for the individual device. Event management provides a set of alert conditions that are significant to the user. As the event conditions are detected, they are categorized and color-coded for easy recognition. Critical errors and alerts are colored red, while warnings and notices are orange or yellow. All other device events are informational only and not color-coded.

The **Events** page refreshes automatically every few seconds, to keep the information on the page up to date.

Note aView stores the past 30 days of event history for each device.

Using the Filter Menu at the top of list, you can filter the events in the following ways:

- **Level:** Severity level of the alert. selected at once.
- **Range:** The time range of events to display. The default is to display the events for the past 24 hours.
- **Type:** The type of events displayed can be filtered.

You can also export the current page or all events by clicking the **Export** button.

Event details

All events are listed with the following information:

- **Created:** The date that an event occurred and time that the event occurred. The time is displayed in the time zone of the user.

- **Type:** The state of the device that is generating the event. There are currently seven different states that a device can be in.
 - **Status:** Device is reporting its current operational status.
 - **Configuration:** Device or remote operation has initiated a configuration change or information request.
 - **Firmware:** A firmware action has been initiated or the device determined there was a conflict.
 - **Reboot:** The device has restarted.
 - **DHCP:** The device is reporting a change in its DHCP configuration.
 - **Tunnel:** VPN tunnel status.
 - **Remote:** A command has been received from the portal and an action initiated.
- **Level:** The severity level of the event being displayed. aView supports a modified version of the severity levels defined by RFC 5424. The supported six levels of events are listed from lowest to highest alert level below.
 - **Debug:** Info useful to developers for debugging the application, not useful during operations.
 - **Info:** Normal operational messages – used for reporting, measuring throughput, etc. - no action required.
 - **Notice:** Events that are unusual but not error conditions. No immediate action required.
 - **Warning:** Warning messages. Not an error, but indication that an error will occur if action is not taken. This message indicates an item that must be resolved within a given time.
 - **Error:** Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.
 - **Alert:** Should be corrected immediately, therefore the appropriate action or support notification should be initiated to fix the problem.
- **Information:** The data that the device transmitted to aView. These messages can be simple text messages or complete hardware status displays. The information field is selectable. Clicking this link will direct the user to a page that displays all the information of the individual event, including a detailed description of what has occurred.

Cellular 6300-LX				
MAC: 00270429517E				
Export				
Created	Type	Level	Information	
Nov 12 2018 16:26:02 (CST)	Status	Info	Heartbeat	
Nov 12 2018 16:25:06 (CST)	Status	Info	Heartbeat	
Nov 12 2018 16:24:04 (CST)	Status	Info	Heartbeat	
Nov 12 2018 16:23:04 (CST)	Status	Info	Heartbeat	
Nov 12 2018 16:22:06 (CST)	Status	Info	Ethernet status	

Tunnel servers

The **Tunnel Servers** page displays all the known VIG and SIG tunnel endpoints that VPN Gateway devices in aView are connected to. Each tunnel server is listed in the table with the following details:

- **Name:** The name of the tunnel server. Clicking on the name will direct the user to a page that lists details for each VPN Gateway device connected to that tunnel server.
- **Devices:** The number of devices connected to the tunnel server.
- **IP Addresses:** The number of IP addresses associated with the tunnel server. Depending on the network setup, a single tunnel server could have multiple IP addresses and physical servers pooled together that makes up the tunnel server network.
- **Type:** The type of tunnel server; typically either a VIG or SIG.
- **Location:** The listed location for the tunnel server.

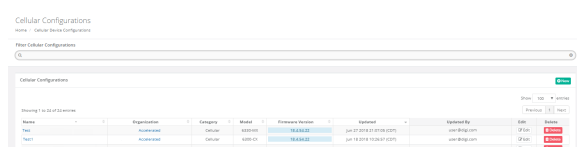
Configurations

The **Configurations** page displays the device configuration profiles available to the user.

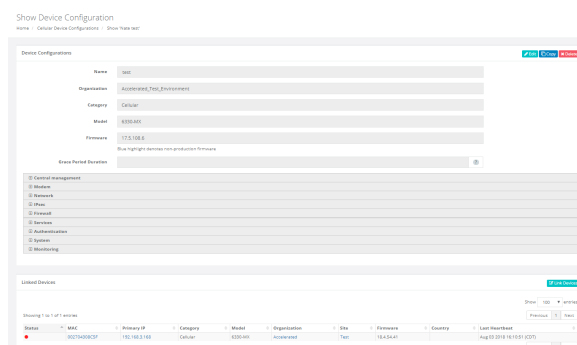
To open the **Configurations** page:

1. Click **Configurations** in the navigation bar.
A sub-menu is displayed, listing categories of device configurations.
2. Click the appropriate type of device configuration from the sub-menu. For details of each configuration option, refer to the individual device configuration sections of this guide.

Note Users must have appropriate permissions to make changes to configurations. See [Permissions](#) for details about how to configure user permissions.



Click on the name of a configuration to open the **Show Device Configuration** page.



Any values in the configuration that are inherited from the parent configuration are highlighted in red. Edit the configuration profile by clicking **Edit** in the top right of the configuration. You can also copy the configuration by clicking **Copy**.

All devices that the configuration profile is linked to are listed at the bottom of the profile. These are referred to as "linked devices".

Reports

aView allows you to create a variety of reports based on various selection criteria. The Reports feature can be selected by clicking on **Reports** in the navigation panel, and then selecting the desired report type.

See [Generating reports](#) for details on report types.

Report history

aView will retain up to ten generated reports per user. These reports can be viewed by clicking on the History link in the Reports drop-down menu of the navigation bar.

Report History

Home > Reports > History

Generated Reports

Showing 1 to 6 of 6 entries

Report ID	Type	Status	Organization	Generated on	Created on	Download	Export
176	Cellular Utilization	Finished	Accredited	Sun 18 Jun 16 10:24:20 (UTC)	Sun 18 Jun 16 10:24:20 (UTC)	Download CSV	Export
175	Cellular Utilization	Finished	Accredited	Sun 18 Jun 16 10:24:20 (UTC)	Sun 18 Jun 16 10:24:20 (UTC)	Download CSV	Export
174	Cellular Utilization	Finished	Accredited	Sun 18 Jun 16 10:24:20 (UTC)	Sun 18 Jun 16 10:24:20 (UTC)	Download CSV	Export
173	Availability	Finished	Not	Sun 17 Jun 16 14:32:24 (UTC)	Sun 17 Jun 16 14:32:24 (UTC)	Download CSV	Export
172	Availability	Finished	Not	Sun 17 Jun 16 14:32:24 (UTC)	Sun 17 Jun 16 14:32:24 (UTC)	Download CSV	Export
171	Availability	Finished	Connect	Sun 17 Jun 16 14:32:24 (UTC)	Sun 17 Jun 16 14:32:24 (UTC)	Download CSV	Export

Showing 1 to 6 of 6 entries

Click on a report ID to display a page with the results of the report. Export a report to a CSV file by clicking **Download CSV**.

Notifications

The **Notifications** page displays the notifications that were sent to the user based on their notification subscriptions. See [Managing Notifications](#) for details on notification subscriptions.

Notifications

Home / Notifications

Filter Notifications

Q

Notifications

Show 25 entries

< Previous Next >

MAC	Category	Model	Organization	Site	Type	Level	Information	Created
00270427BA26	Cellular	6300-CX	Default	Default	DHCP	Info	Cellular WAN IP changed from 10.61.188.153 to 10.63.169.123	Dec 23 2018 11:57:03 (EST)
00270427BA26	Cellular	6300-CX	Default	Default	Status	Notice	Device is up	Dec 23 2018 11:56:59 (EST)
00270427BA26	Cellular	6300-CX	Default	Default	Status	Notice	Device is up	Dec 23 2018 11:56:59 (EST)
00270427BA26	Cellular	6300-CX	Default	Default	Status	Notice	Device is up	Dec 23 2018 11:56:59 (EST)
00270427BA26	Cellular	6300-CX	Default	Default	Reboot	Notice	Device rebooted: Unmanaged	Dec 23 2018 11:56:59 (EST)
00270427BA26	Cellular	6300-CX	Default	Default	Status	Notice	Device is up	Dec 23 2018 11:56:58 (EST)
00270427BA26	Cellular	6300-CX	Default	Default	Status	Alert	Device is down	Dec 22 2018 16:32:23 (EST)
00270427BA26	Cellular	6300-CX	Default	Default	DHCP	Info	Cellular WAN IP changed from 10.63.175.51 to 10.61.188.153	Dec 22 2018 14:13:14 (EST)
00270427BA26	Cellular	6300-CX	Default	Default	Reboot	Notice	Device rebooted: Unmanaged	Dec 23 2018 14:13:07 (EST)
00270427BA26	Cellular	6300-CX	Default	Default	Status	Notice	Device is up	Dec 23 2018 14:12:59 (EST)
00270427BA26	Cellular	6300-CX	Default	Default	Status	Alert	Device is down	Dec 18 2018 12:04:45 (EST)
00270427BA26	Cellular	6300-CX	Default	Default	DHCP	Info	Cellular WAN IP changed from 10.61.164.72 to 10.63.175.51	Dec 18 2018 09:45:33 (EST)

The **Notification** page is a convenient way to look at a list of alerts that have been sent to you. The **Information** column provides a summary of the content of the notification for quick reference. Clicking on an entry in the **Information** column will open a window listing the raw data of the event; click **Go To Event** to view the event that spawned the notification.

You can filter notifications for categories like device type and severity. See [Device events](#) for further information about the event-related filters available for notifications.

Organizations

The **Organizations** page displays all organizations that you have access to.

An organization is a logical entity used to associate devices together. It does not necessarily represent a client.



Clicking on an organization name will display a page listing all devices associated with the organization and all sub-organizations.

Each line also has an **Actions** drop-down that allows you to display the organization's devices and to subscribe to notifications from the organization's devices. Additionally, if your user role includes the **Modify Organizations** permission, you can edit the organization settings, add new users, add new sub-organizations, and delete the organization.

Note Deleting an organization will also delete any devices, users, and sub-organizations associated with that organization.

Create a new sub-organization

Creating new subscriptions requires that your user role includes the **Modify Organizations** permission. See [Roles](#) for more information about user roles.

To create a new sub-organization:

1. From the navigation panel, click **Organizations**.
The **Organizations** page displays.

2. Click **Actions** on the right hand side of an organization's row, and select **New Sub Organization**.

The **New Organization** dialog appears.

The screenshot shows the 'New Organization' dialog box. It has a title bar with the text 'New Organization' and a close button. The dialog contains several fields: 'Name *' with a text input containing 'Organization Name'; 'Parent *' with a dropdown menu showing 'Accelerated'; 'Description' with a text input; 'Service Name' with a dropdown menu; 'Abilities' with three buttons: 'All', 'None' (highlighted in green), and 'Custom', followed by an 'Expand' button with a plus icon; 'Logo' with a 'Choose File' button and an 'Upload' button; and 'Footer' with a text input and a help icon. At the bottom are 'Cancel' and 'Create Organization' buttons.

3. Enter a name for the organization and an optional description.
The remaining fields in the **New Organization** dialog are described in the following sections.
4. Click **Create Organization** when complete.

Organization abilities

Part of the purpose of an organization is to control the access users within that organization have to aView. When creating an organization, there are a list of roles that must be selected to specify the access that organization will have to its devices.

Note Configuring an organization's abilities can only be performed when creating a new organization and cannot be edited after the organization has been created.

1. Follow instructions at [Create a new sub-organization](#) to create a new organization.
2. For **Abilities**, select **All**, **None**, or **Custom**.

3. If **Custom** is selected for **Abilities**, click **Expand** to expand a list of available abilities. The following abilities are available:
 - **Modify Sites:** Controls the ability for users within the organization to edit the Site IDs associated with that organization.
 - **Modify Devices:** Controls the ability for users within the organization to edit the options listed in the Admin Panel section on a device's details page, as well as deploying/undeploying devices.
 - **Modify Organizations:** Controls the ability for users within the organization to edit any sub-organizations that the organization has.
 - **Modify Users:** Controls the ability for users within the organization to edit the settings and permissions of other users.
 - **Modify Configurations:** Controls the ability for users within the organization to edit the Legacy Cellular configuration profiles of a device.
 - **Replace Devices:** Controls the ability for users within that organization to move devices from one organization to another.
 - **Import Devices:** Controls the ability for users to add new devices into aView with the import tool.
 - **Modify Device Configurations:** Controls the ability for users within the organization to edit the Cellular, Dial-to-IP and Remote Manager configuration profiles of a device.
 - **View Configuration History:** Controls the ability for users within the organization to view the history of changes made to a device's configuration profile.
 - **View Admin Panel:** Controls access to the Admin panel of the site. If enabled, the Admin panel will be accessible by a link in the right section of the top navigation bar (between the Account and Logout buttons).
 - **Deploy Devices:** Controls the ability for users within the organization to deploy or undeploy devices. For more information on what device deployment, please refer to the Monitoring Devices section of this guide.
 - **Send Device Commands:** Controls the ability for users within the organization to send remote commands to devices.
 - **Assign Non-Production Firmwares:** Controls the ability for users within the organization to select non-production firmware versions in a device's configuration profile.
4. Click each ability that should be applied to the organization.
5. Complete the other information in the dialog as necessary and click **Create Organization**.

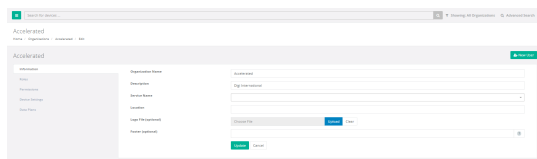
Optional service name

You can associate a Service Name to an organization, as a way of indicating what level of service a support company provides to the organization. Adding or modifying the service name requires that your user role includes the **Modify Organizations** permission. See [Roles](#) for more information about user roles.

To add or modify the Service Name for an organization:

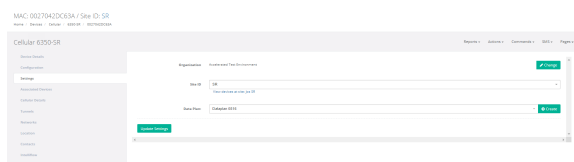
1. From the navigation panel, click **Organizations**.
The **Organizations** page displays.

2. Click **Actions** on the right hand side of an organization's row, and select **Edit Settings**.
The organization's page appears.



3. Click the down arrow (▼) for the **Service Name** field and select the appropriate Service Name.
If the desired Service Name is not available, please contact your aView admin to have the Service Name included.
4. Click **Update**.

Once the Service Name has been assigned to an organization, it will be displayed on any device in that organization or any of its sub-organizations. Also, any notifications that get sent from aView for the organization's devices will include the Service Name in the notification details.

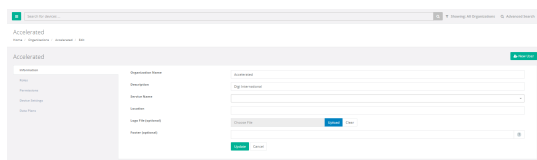


Optional logo and footer

The logo that will appear in the aView application, and the footer text displayed at the bottom of the application, can be changed at an organization level. Any footer that is set for the organization will be applied to all sub-organizations. Footer text can be either text or valid HTML. Adding or modifying the logo and footer requires that your user role includes the **Modify Organizations** permission. See [Roles](#) for more information about user roles.

To set or update the footer text for an organization:

1. From the navigation panel, click **Organizations**.
The **Organizations** page displays.
2. Click **Actions** on the right hand side of an organization's row, and select **Edit Settings**.
The organization's page appears.

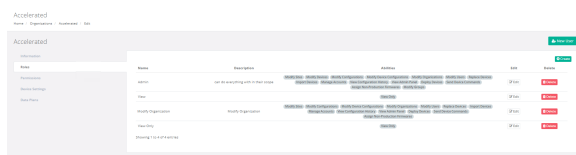


3. For **Logo File (optional)**, click **Upload** and select the logo file.
4. For **Footer (optional)**, type in the desired footer text in either text or valid HTML format.
5. Click **Update**.

Roles

The organization's **Roles** tab is used to group various abilities into roles that can then be assigned to one or more users within that organization to define their permissions when using aView. See [Users](#)

for information about creating and assigning roles to users.



See [Organization abilities](#) for information about the available abilities.

Note Your user role must include the **Modify Organizations** ability in order to view or edit an organization's user roles.

To view and edit an organization's roles:

1. From the navigation panel, click **Organizations**.
The **Organizations** page displays.
2. Click **Actions** on the right hand side of an organization's row, and select **Roles**.
3. To create a new role:

- a. Click **Create**.

The **New Role** dialog displays.

- b. For **Name**, type a name for the role.
 - c. Type an optional description for the role.
 - d. Click the check box for each applicable ability to be included in the role. You can also click **Check all** or **Uncheck all** at the bottom of the list of abilities.
 - e. Click **Create Role**.
4. To edit an existing role:
 - a. Click **Edit** on the right hand side of an role's row.
The **Edit Role** dialog displays.
 - b. Make any appropriate changes to the role.
 - c. Click **Update Role** when complete.

Permissions

The organization's **Permissions** tab allows you to view and assign roles to an organization. See [Roles](#) for more information about creating and editing roles that are available for the organization.

To view and assign roles for an organization:

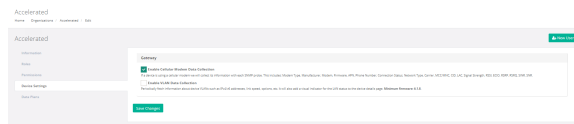
1. From the navigation panel, click **Organizations**.
The **Organizations** page displays.
2. Click **Actions** on the right hand side of an organization's row, and select **Permissions**.
3. To assign a new role to the organization, click **Create**.
The **New Permission** dialog appears.

4. For **Role**, select the appropriate role to include for the organization.
5. Click **Create Permission**.

You can also change the assigned role for a permission by clicking **Edit** on the right hand side of an permission's row and selecting a new role for the permission.

Device settings

The **Device Settings** tab contains all selections to enable or disable optional details or metrics for devices in that organization or its sub-organizations.



The following options are available in the **Device Settings** tab.

- **Gateway—Enable Cellular Modem Data Collection:** when enabled, the aView application will collect cellular statistics from all VPN Gateway devices that belong to that organization or any of its sub-organization. These cellular utilization statistics will be displayed on the device's

details page as the Cellular Utilization chart and the Modem tab. Refer to the Gateway Devices section for more details. The cellular statistics can also be used to generate cellular-based reports for VPN Gateway devices.

- **Gateway—Enable VLAN Data Collection:** when enabled, the aView application will collect details of the LAN ports of the VPN Gateway device, including the VLAN IDs associated with the LAN ports.

Data plans

The **Data Plans** tab allows authorized users to create and manage cellular data plans for the selected organization. Once a data plan is created, the user can apply that data plan to one or more devices by selecting the data plan under the **Settings** tab on the details page for the device.

- **Name:** The name of the data plan. Clicking on the data plan name will display a list of the devices associated to that data plan, including how much data each device has used under the data plan.
- **Number of devices:** The count of devices assigned to this data plan.
- **Data Limit:** The amount of data usage at which point a notification should be generated for the data plan. Note that for this notification to be generated, the Overage Notification option must be selected.
- **Data Used:** The amount of data used by the devices that belong to the data plan.
- **Individual Data Limit:** The amount of data usage for each device under the data plan at which point a notification should be generated. To receive this notification, a user must subscribe to the device and select the Device data usage over limit option in the notification profile. For additional details on setting up a notification profile, refer to the Notification Profiles section.
- **Start Day:** The day of the month to reset the Data Used value of the data plan.
- **Overage Notification:** Selecting this option will send a notification when the Data Used value of the data plan exceeds the Data Limit option of the data plan. When triggered, this notification will be sent to all users that belong to the same organization that the data plan belongs to.
- **Created:** The time when the data plan was created.

Name	Number of Devices	Data Limit	Data Used	Overage Notification	Start Day	Created	Details	Delete
Data Plan 1	1	100MB	100MB	Yes	15	2023-01-15 10:00:00	Details	Delete
Data Plan 2	1	100MB	100MB	Yes	15	2023-01-15 10:00:00	Details	Delete
Data Plan 3	1	100MB	100MB	Yes	15	2023-01-15 10:00:00	Details	Delete

SNMP probes

VPN Gateway devices are monitored using SNMP probes. The settings here control how often the Digi aView application attempts to probe the VPN Gateways that belong to this organization. The default is to probe the device once every 15 minutes and mark the device as down if no response is received after two probes.

See [Configure down status for VPN gateway devices](#) for information on controlling when a VPN Gateway is considered down by Digi aView.

New User

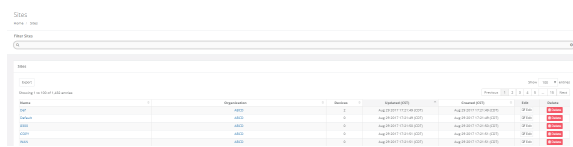
You can create a new user by selecting **New User** from the organization's **Action** menu. See [Users](#) for further information about creating users.

Subscribe to device notifications

You can subscribe to device notifications for the organization by selecting **Subscribe** from the organization's **Actions** menu. See [Notification subscriptions](#) for information about notification subscriptions.

Sites

The **Sites** page displays all the current sites that you have access to. The panel displays all unique sites that have been entered for the organization along with the organization name and number of devices. Note that sites are tied to the organization they are associated with, so there may be multiple sites with the same name, but they are associated to different organizations.



Site	Organization	Devices	MACs
Site 1	Org 1	1	Aug 2017 11:01:00 (UTC)
Site 2	Org 2	2	Aug 2017 11:01:00 (UTC)
Site 3	Org 3	3	Aug 2017 11:01:00 (UTC)
Site 4	Org 4	4	Aug 2017 11:01:00 (UTC)

The **Site** and **Organization** fields are both selectable items. Clicking on **Site** name will display the **Devices** page, listing all devices at that location. Clicking the **Organization** name will display the **Devices** page, listing all devices at that have been defined for that organization. Any device in the list can then be selected and managed by clicking the MAC address.

Users

The **Users** page displays all user accounts under the current user can manage. Authorized users can create new users and modify any existing user.

Name	Email	Organization	Time Zone	Last Login (UTC)	Status	Role
User1	user1@digi.com	Digi	Central Time US & Canada	Mar 27 2017 10:00:00 (UTC)	Inactive	Admin
User2	user2@digi.com	Digi	Central Time US & Canada	Mar 28 2017 10:00:00 (UTC)	Active	Admin
User3	user3@digi.com	Digi	us-east	Mar 27 2017 10:00:00 (UTC)	Inactive	Admin
User4	user4@digi.com	Digi	Central Time US & Canada	Apr 02 2017 10:00:00 (UTC)	Inactive	Admin
User5	user5@digi.com	Digi	Eastern Time US & Canada	Mar 27 2017 10:00:00 (UTC)	Inactive	Admin
User6	user6@digi.com	Digi	Eastern Time US & Canada	Mar 27 2017 10:00:00 (UTC)	Active	Admin
User7	user7@digi.com	Digi	Eastern Time US & Canada	Mar 27 2017 10:00:00 (UTC)	Pending	Admin

Create a new user

To create a new user:

1. From the navigation panel, click **Users**.
The **Uses** page appears.
2. Click **Create**.
The **New User** dialog appears.

New User

Email *

Organization

Role

3. For **Email**, type the user's email address.
4. For **Organization**, select the appropriate organization for the user.
See [Organizations](#) for more information about organizations.
5. For **Role**, select the appropriate role for the user.
See [Roles](#) for further information about roles.
6. Click **Create User**.

When a new user is created, aView will send a welcome email to the user's email address with instructions for setting up their password and account. The user must set up their password and account within 72 hours after the email has been sent. If the user does not respond in time, their account will need to be recreated.

Edit a user

To edit a user:

1. From the navigation panel, click **Users**.
The **Uses** page appears.
2. Click **Edit** on the right hand side of a user's row.
The **User Detail** page appears.

3. Click **Save Changes** after completing your changes to the user information.

See [Manage User Preferences](#) for information about the remaining tabs on the **User Details** page.

Manage users

Users are given specific access and abilities by their organization administrator or the administrator of an organization above them. The abilities and access to certain areas of the aView site are called user "permissions". A permission could include features such as being able to send remote commands, move devices to other organizations, deploy/undeploy devices, and having access to view certain categories of devices.

To manage the permissions a user has, navigate to the Users page, click the Edit pencil icon in the row of the desired user, and then click the Permissions tab. New permissions can be added by clicking the Create plus icon, selecting the new permission from the drop-down list, and then click Create Permission. Note that the list of available permissions are based on the permissions of the user who is managing the user and the permissions available in the user's organization. To remove a permission from a user, click the Delete link.

Permissions

Users are given specific access and abilities by an administrator. The abilities and access to certain areas of the aView application are referred to as user permissions. A permission could include features such the ability to send remote commands, move devices to other organizations, deploy/undeploy devices, and having access to view certain categories of devices.

To manage a user's permissions:

1. From the navigation panel, click **Users**.
The **Uses** page appears.
2. Click **Edit** on the right hand side of a user's row.
The **User Detail** page appears.
3. Click **Permissions**.
The **Permissions** tab appears.
4. To delete a permission associated with the user, click **Delete** on the right hand side of the row associated with the permission.
5. To add a permission to the user:
 - a. Click **Create**.
 - b. Select the appropriate **Organization**.
 - c. Select the **Role** that should be assigned to the user.
Roles are created at the organization level. See [Roles](#) for further information about roles, including how to create them.
6. Click **Create Permission**.

Monitoring devices

- About monitoring devices 44
- Color indicators 44
- Deploy a device 44

About monitoring devices

Device monitoring in aView is controlled by the state of the device. The two states a device can be in are deployed and undeployed.

- **Deployed state:** Indicates that the device should be monitored based on the events that are sent in by the device, and will be listed with a particular status (see [Color indicators](#) for information about deployed device statuses). A device that is deployed will also generate notification alerts, based on the events received and the aView application's access to that device.
- **Undeployed state:** Indicates that the device should not be monitored. Undeployed devices will be listed with a pause icon (||) as their status and with a dark gray status color. aView will still list details and events for undeployed devices, but these events will not generate any notification alerts.

Color indicators

aView marks deployed devices with a color indicator to provide a visual way to note what its status is. Below is a list of color statuses and their meaning.

- **Green:** The device is online and is reachable through the aView system. For details on what triggers a device to go up, refer to the Notification Profiles section of this guide.
- **Red:** The device is down. This status is also referred to as the Alert status. For details on what triggers a device to go down, refer to the Notification Profiles section of this guide.
- **Blue:** The device is running on a backup WAN connection. This indicates that the device's current WAN connection is one of its backup connections (i.e. not WAN1).

Note The blue status only applies to Gateway devices.

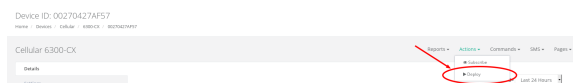
- **Orange:** The device is in dual-WAN modem, but only its WAN1 connection is online. The secondary WAN interface is down.

Note The orange status only applies to Gateway devices.

- **Gray:** The device is inactive, meaning that it has never checked in to aView. This is the state of the device if it is deployed, but no event has ever been received by aView.

Deploy a device

To deploy an individual device, go to the device details page. This can be done by searching for the device's MAC address in the search bar, then clicking on the MAC address of the correct device in the results. Once on the details page, click on the **Actions** drop-down on the right side of the page and select **Deploy**.



Immediately after a device is deployed, aView will automatically send a remote command to the device to get its current status. This ensures that the status of the device is correctly reflected in aView.

Cellular devices

- About cellular devices 46
- Cellular device details 46
- Cellular device remote commands 50
- Cellular configuration requirements for aView 51

About cellular devices

Cellular devices refer to a subset of the Digi Cellular Extender line of products. Supported models are listed below. You can find a list of all the Cellular devices that you have access to by clicking on the Devices tab in the navigation bar, and then selecting the Cellular link from the dropdown.

- 6300-CX
- 6300-LX
- 635x-SR
- 633x-MX
- 6310-DX
- IX14

The screenshot shows a web interface with a search bar and a table of Cellular Devices. The table has columns for MAC, Host, Category, Model, Organization, Site, Firmware, Carrier, dBm, Signal, Network, Phone Number, City, Country, and Last Heartbeat (UTC). There are three rows of data, each with a red status indicator.

MAC	Host	Category	Model	Organization	Site	Firmware	Carrier	dBm	Signal	Network	Phone Number	City	Country	Last Heartbeat (UTC)
00270427B94E	6300-CX	Cellular	6300-CX	Proxip	Proxip	1.0.0.0	Verizon	-75	100%	Verizon	703-200-1000	Proxip	US	2016-10-10 10:10:10
00270427B94E	6300-LX	Cellular	6300-LX	Proxip	Proxip	1.0.0.0	Verizon	-75	100%	Verizon	703-200-1000	Proxip	US	2016-10-10 10:10:10
00270427B94E	6300-LX	Cellular	6300-LX	Proxip	Proxip	1.0.0.0	Verizon	-75	100%	Verizon	703-200-1000	Proxip	US	2016-10-10 10:10:10

Cellular devices are listed in tabular form. The majority of the details are applicable to all device categories. See [Device details page](#) for details on those table entries.

The table entries specific to Cellular devices are:

- **Carrier:** The cellular carrier of the current connection, indicating the owner of the local cellular network and modem tower.
- **Provider:** The cellular provider of the current connection, indicating who provisioned the SIM card.
- **dBm:** The signal strength of the cellular connection measured in dBm.
- **Signal:** The signal strength percentage of the cellular connection.
- **Network:** The technology type of the cellular connection.
- **Phone Number:** The phone number of the current cellular connection.

Cellular device details

The screenshot shows the details page for a Cellular 6300-CX device. The page has a sidebar with navigation links and a main content area with various fields.

Device Details	Organization	Proxip
Device ID	00270427B94E	Proxip
MAC Address	00270427B94E	Proxip
Serial	00270427B94E	Proxip
Status	Online	Proxip
Model	6300-CX	Proxip
Upgrade IP Address	192.168.1.1	Proxip
Network	Verizon	Proxip
Primary Interface	eth0	Proxip
Activated At	Aug 23 2016 10:10:10	Proxip
Last Heartbeat	Aug 23 2016 10:10:10	Proxip
Last Reset	Aug 23 2016 10:10:10	Proxip
Data Plan	None	Proxip

The majority of details provided on the Cellular device details page are applicable to all categories of devices. See [Device details page](#) for details on those table entries.

The device details specific to Cellular devices are:

- **Management IP:** The IP address of the Cellular device's aView IPsec tunnel. If this IP does not match the aView tunnel IP address listed in the local web UI of the Cellular device, a user with the ability to modify devices can edit the Management IP address.
- **Uplink IP Address:** The IP address of the current WAN network connection of the Cellular device.
- **Primary Interface:** The currently used WAN connection interface.

Cellular device Configuration tab

Cellular devices are configured through the aView site. See [Create a new Cellular device configuration profile](#) for further information.

Cellular device Settings tab

The majority of details provided on the Cellular **Settings** tab are applicable to all categories of devices. See [Settings tab](#) for details on those table entries.

The device details specific to Cellular devices are:

- **Data Plan:** The data plan assigned to the device. If the user has the ability to change the data plan, a drop-down will be displayed and lists the available data plans for the organization the device belongs to. Once a data plan is associated with the device, any cellular data used by the device will be tracked in the data plan, which can be viewed and managed by clicking the **Edit** button for an Organization (see [Organizations](#)). You also have the option of creating a new data plan if desired.

Cellular device Associated Devices tab

This tab lists any devices that the Cellular device has associated with, indicating that they are connected to each other. The tab will include the following details about the associated device:

- **Device ID:** The identifying MAC address for the associated device.
- **Model:** If the associated device is a type of device supported by ARMT, this entry will display the type of device ARMT knows it as. If the device is not supported by ARMT, the category will be listed with a dash (-).
- **Interface:** The physical interface of the Cellular device the associated device is connected to.
- **Type:** How the associated device is connected to the Cellular device. For example, a type listed as LAN indicates that the associated device is connected to one of the Cellular device's LAN Ethernet ports.
- **IP Address:** The IP address of the associated device.
- **Connected:** Indicates when the device association was made and how long the associated device has been connected to the Cellular device.

Cellular device Cellular Details tab

The **Cellular Details** tab lists details for the Cellular modem. The name of the cellular modem is listed in the title bar of the **Cellular Details** tab. If a cellular device has multiple modems, there will be multiple modem panels, each one corresponding to one of the cellular device's modems. A modem entry can be removed by clicking the red trash icon at the top-right of the specific tab.

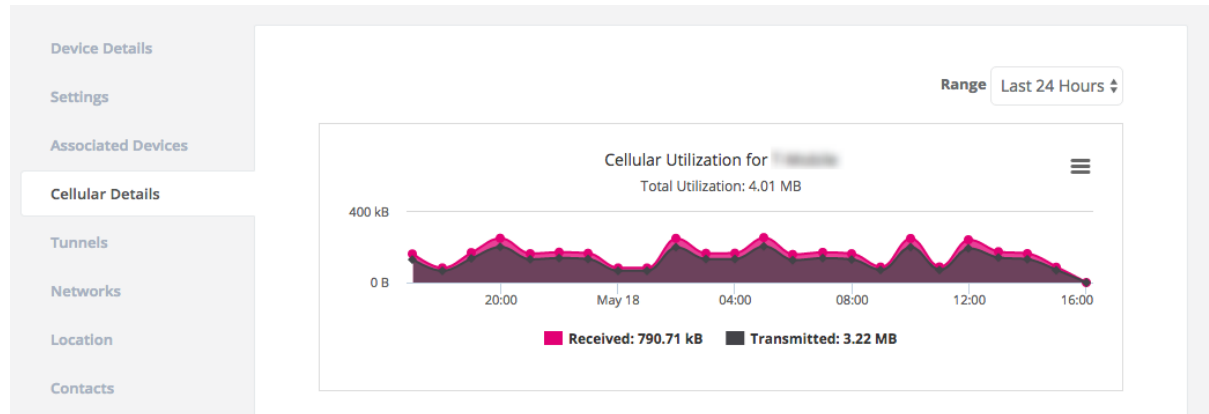
- **Carrier:** The cellular provider of the modem.
- **SKU:** The stock keeping unit of the modem.
- **Signal Strength:** The current RSSI signal strength value, measured in dBm, and percentage of the modem.
- **Signal Bars:** The current signal bars, based on the signal strength.
- **Speed Test:** The five most recent (if any) speed tests performed on the device. Speed tests are generated by sending a Speed Test command to the device.

Note In order to minimize the speed test's impact on cellular data consumption, the results are an estimation of the available throughput of the device, and may not represent the full network speed available.

- **Phone Number:** The phone number of the modem.
- **RSSI:** The Received Signal Strength Indicator (RSSI) of the modem. RSSI provides information about total received wide-band power, including signal interference and thermal noise.
- **RSRP:** An LTE-specific value, representing the Reference Signal Received Power of the modem. RSRP is the average power of resource elements that carry cellular specific reference signals over the entire bandwidth.
- **RSRQ:** An LTE-specific value, representing the Reference Signal Receive Quality (RSRQ) of the modem. RSRQ is a combination of RSSI and RSRP and indicates the quality of the received reference signal.
- **SiNR:** The signal-to-interference-plus-noise ratio of the modem.
- **SNR:** The signal-to-noise ratio of the modem.
- **IMEI:** The IMEI value of the modem.
- **ESN:** The ESN value of the modem. Note that the ESN value only applies to CDMA cellular networks.
- **ICCID:** The ICCID value of the SIM card used by the modem.
- **IMSI:** The IMSI value of the modem.
- **Revision:** The hardware version of the modem.
- **APN:** The APN that the modem is currently connected with. Note that not all modems require an APN.
- **ECIO:** The signal-to-noise ratio of the modem. The lower the E_c/I_o value, the greater the noise.
- **CNTI:** The technology type that the modem is currently connected to.
- **Band:** The frequency or type of cellular band the modem is currently connected to.
- **CID:** The CID identifier of the modem's current connection.
- **LAC:** The LAC identifier of the modem's current connection.
- **MCC:** The mobile country code of the modem's current connection.
- **MNC:** The mobile network code of the modem's current connection.
- **PLMN:** The PLMN ID of the modem's current connection, which is a combination of the MCC and MNC values.
- **USB Speed:** The speed of the USB port(s) on the Remote Manager device, measured in Mbps. 480 indicates USB 2.0 High Speed and 12 indicates USB 2.0 Full Speed.

Cellular utilization chart

If the device supports a cellular modem, a cellular utilization chart will be displayed. The chart shows the amount of cellular data used by the device. The initial timespan will display the data usage for the past 24 hours. You can select different timespans from the Range drop-down.



Cellular device Tunnels tab

The **Tunnel** tab lists status for any IPSec tunnels established by the Cellular device. Each row of the tab indicates a unique IPSec tunnel of the device.

- **Name:** The name of the IPSec tunnel, as specified in the configuration of the Cellular device.
- **Status:** Indicates whether or not the Cellular device has established the IPSec tunnel.
- **Last Updated:** The last time aView received an update concerning this tunnel.
- **IpLocal:** The tunnel IP address assigned to the Cellular device.
- **IpRemote:** The IP address of the server that the Cellular device built a tunnel to.
- **NetLocal:** The network settings on the Cellular device for the tunnel.
- **NetRemote:** The network settings on the server for the tunnel.

Cellular device Network tab

The **Network** tab lists details for network interfaces that belong to the Cellular device. If an Cellular device has multiple networks, there will be multiple network tabs, each one corresponding to one of the device's networks.

- **Connection Type:** the type of network connection for the interface.
- **Priority:** Indicates if the network connection is the current primary or alternate connection.
- **IP Ranges:** The IP addressing for the network.
- **Metric:** The priority level of the network interface. The lower the number, the higher in priority the interface.
- **MTU:** The MTU size of the network interface.
- **Gateway IP:** The default route (gateway IP) of the network interface.
- **Bytes Received:** The total amount of data received, measured in bytes, on the network interface since the Cellular device has been online (resets on reboot).

- **Bytes Transmitted:** The total amount of data transmitted, measured in bytes, on the network interface since the Cellular device has been online (resets on reboot).
- **Ethernet Speed:** If the network type is an Ethernet interface, then this indicates the speed of the Ethernet port.
- **Ethernet Status:** If the network type is an Ethernet interface, then this indicates the status of the physical connection on the Ethernet port.

Cellular device remote commands

Remote commands are sent to a Cellular device through an IPSEC tunnel the device establishes to the Accelerated remote control server, or through the upstream IP address of the device if no tunnel IP is available. All Cellular devices by default establish an IPSEC tunnel to remote.accns.com. See [aView tunnel alternatives](#) for information about additional IPSEC tunnel endpoints.

The tunnel IP address for the Cellular device is stored in aView as the Management IP on the **Device Details** tab. If the Management IP is not known, then aView will use the IP address listed in the **Uplink IP Address** field on the **Device Details** tab for sending remote commands.

When you send a remote command to a device, aView utilizes a DNS service running on the remote control server to verify what tunnel IP address is associated with the device. If the DNS service responds with a valid IP address, aView will send the remote command to that IP address, otherwise it will use the known Management IP or the Uplink IP Address if the Management IP is unknown. If the IP address returned by the DNS service differs than the Management IP listed for the device, aView will update the Management IP after successfully sending the remote command to the device.

Before sending the remote command to the Cellular device, aView will prompt the user to provide the device-level username and password to authenticate with the device. If you do not know the username or password for the device, navigate to the **Configuration** tab of the device in aView and select **Authentication > Users**. Select a user name to change the password. You can also change the password locally on the device by following the instructions in the device's user manual. For example, to view instructions for the EX15, visit <https://www.digi.com/resources/documentation/digidocs/90002344/default.htm#os/user-local-change-pswd-t.htm>.

Once the username and password are provided for the device, aView will then perform a HTTP request to the device to validate that the correct device is at the given IP address. If the correct device is reached and authenticated, the remote command will be sent.

The available remote commands that can be sent to Cellular devices are:

- **Check status:** The Cellular device will immediately send its current status.
- **Check signal strength:** The Cellular device will send its signal strength and network info once every 10 seconds for the next 15 minutes.
- **Perform Speed Test:** The Cellular device will perform a speed test and send the Upload/Download results.

Note In order to minimize the speed test's impact on cellular data consumption, the results are an estimation of the available throughput of the device, and may not represent the full network speed available.

- **ARPing Attached Device:** The Cellular device will attempt to ARPing the client device attached to its Ethernet port.
- **Send Wake-on-LAN to Attached Device:** The Cellular device will send a wake-on-LAN packet to the client device attached to its Ethernet port.

- **Check Configuration:** The Cellular device will immediately pull its configuration and reboot to apply any new settings.
- **Update Modem Firmware:** The Cellular device will query the Digi firmware server. If a new version of firmware is found for the active firmware used on the embedded modem in the Cellular device, it will download the new firmware and update the embedded modem. Note the Cellular device must be running firmware version 17.8.128 or higher to process this command.
- **Reboot:** Reboot the Cellular device.

Cellular device emergency SMS commands

As an alternative to the Remote commands, you can also send commands via SMS messaging to a Cellular device. The SIM card used by the Cellular device must have SMS enabled, or you will not be able to send SMS commands.

The available SMS commands that can be sent are:

- **Set Configuration:** A pop-up window appears where a user can enter in a configuration option or set of options to apply to the Cellular device. Multiple config options must be separated by a comma. For example, if a user wants to set the APN of a Cellular device to managedvpn, they would enter "modem_apn=managedvpn".
- **Configuration Reset:** Restore default configuration on the Cellular device and reboot.
- **Firmware Reset:** Restore to the backup firmware image on the Cellular device, and reboot.
- **Factory Reset:** Restore default configuration on the Cellular device, restore to the backup firmware image, and reboot.
- **Remote Control:** Tell the Cellular device to bring up its remote control tunnel (useful if on low data plan, so the remote control tunnel is not always up using data).
- **Reboot:** Reboot the Cellular device.

Cellular configuration requirements for aView

In order for the aView site to monitor a Cellular device, it must send its syslogs to the aView syslog server IP address, the domain of which is logs.accns.com.

For a Cellular device to get its configuration from the aView site, it must be set to pull its configuration from the aView configuration server configuration.accns.com. The device must also be able to sync its date and time with an NTP server; the default is time.accns.com.

In the device configuration, ensure the following options are set in **Service > Web administration**:

- **Enable** is selected.
- **Port** is set to **443**.
- **Access control list** -> **Zones** includes the **IPSec** zone.

This zone is included by default, but it's mentioned here for the user to verify that it is still present, in case the device is running settings that deviate from the default configuration.

The screenshot shows the 'Services' configuration page. Under 'Web administration', the 'Enable' checkbox is checked and the 'Port' is set to 443. Under 'Access control list', there is a list of zones. The second zone is highlighted with a red box, showing 'Zone' set to 'IPsec'.

View Cellular configuration profiles

To view the current list of group configuration profiles a user has access to:

1. Click on the **Configurations** button in the navigation panel.
2. Select **Cellular** in the drop-down.

The screenshot shows the 'Cellular Configurations' page. It displays a table of cellular configurations. The table has columns for Name, Organization, Category, Model, Firmware Version, Updated, and Updated By. The table is filtered to show 10 of 12 total entries.

Create a new Cellular device configuration profile

To create a new group configuration profile:

1. Click on the **Configurations** button in the navigation panel.
2. Select **Cellular** in the drop-down.
3. Click the **plus** icon located at the top right of the window.
4. Select the firmware version. The appropriate configuration schema will automatically load.
5. Set any desired settings in the presented configuration schema. Hovering your mouse over the name for a configuration option will display a pop-up providing help details about that option, including any default values. Once all the desired configuration options have been specified, click **Create**.

Note If the desired firmware is not listed, it must be uploaded onto the firmware management service, which is hosted at distro.accns.com.

Apply a Cellular configuration profile

To apply a group configuration profile to a Cellular device:

1. Go to the device details page for the specific device. This can be done by searching for the device's MAC address in the search bar, then clicking on the MAC address of the correct device in the results.
2. Once on the details page, click on the **Configuration** tab, select the new configuration profile from the **Group Configuration** drop-down, and click the **Save** button.

Individual device configuration settings

In addition to applying a group configuration profile to a device, authorized users will also have the option of setting configuration options to apply only to an individual device. These individual device configuration options are listed in the **Configuration** tab, below the **Group Configuration** option.

When a new group configuration is selected for a device, a list of inherited configuration settings from that group configuration profile will be displayed. Authorized users can then click on any setting and select the **Override** option to change the selected configuration option. It is important to note that any configuration option overridden in this way will only apply to that individual device. Any other devices that are linked to the same group configuration will only receive configuration settings from the group configuration profile, not any of the overridden settings from another individual device's configuration.

- **Inherit All:** This button can be used to reset an individual device's configuration back to the group configuration profile's settings. Any configuration options previously overridden in the individual device configuration will be undone and reset back to the settings inside the group configuration.

Delete a Cellular device configuration profile

Group configuration profiles can be deleted by clicking on the Delete icon for the appropriate profile on the Cellular Configurations page. A confirmation pop-up will ask the user to confirm that they wish to delete the configuration profile. If there are any devices linked to the configuration profile that is being deleted, the profile will not be deleted. The user must first unlink the configuration profile from the device and then they can remove the profile.

Dial-to-IP devices

- About dial-to-IP devices 56
- Dial-to-IP device details 56
- View Dial-to-IP configuration profiles 59
- Create a new Dial-to-IP device configuration profile 60
- Apply a Dial-to-IP configuration profile 60
- Individual device configuration settings 61
- Delete a Dial-to-IP device configuration profile 61

About dial-to-IP devices

Dial-to-IP devices refer to the Digi Dial-to-IP Converter line of products. You can find a list of all the Dial-to-IP devices that you have access to by clicking **Devices** in the navigation bar, and then selecting **Dial-to-IP**. Supported models are:

- 5300-DC
- 5301-DC

ID	Host	Category	Model	Organization	Site	Hardware	Chip	Country	Last Heartbeat (STI)
5300-DC	192.168.1.1	Dial-to-IP	5300-DC	Test Org	Test Site	5300-DC	5300-DC	US	2023-10-27 14:23:23 (STI)
5301-DC	192.168.1.2	Dial-to-IP	5301-DC	Test Org	Test Site	5301-DC	5301-DC	US	2023-10-27 14:23:23 (STI)
5302-DC	192.168.1.3	Dial-to-IP	5302-DC	Test Org	Test Site	5302-DC	5302-DC	US	2023-10-27 14:23:23 (STI)
5303-DC	192.168.1.4	Dial-to-IP	5303-DC	Test Org	Test Site	5303-DC	5303-DC	US	2023-10-27 14:23:23 (STI)
5304-DC	192.168.1.5	Dial-to-IP	5304-DC	Test Org	Test Site	5304-DC	5304-DC	US	2023-10-27 14:23:23 (STI)
5305-DC	192.168.1.6	Dial-to-IP	5305-DC	Test Org	Test Site	5305-DC	5305-DC	US	2023-10-27 14:23:23 (STI)
5306-DC	192.168.1.7	Dial-to-IP	5306-DC	Test Org	Test Site	5306-DC	5306-DC	US	2023-10-27 14:23:23 (STI)
5307-DC	192.168.1.8	Dial-to-IP	5307-DC	Test Org	Test Site	5307-DC	5307-DC	US	2023-10-27 14:23:23 (STI)
5308-DC	192.168.1.9	Dial-to-IP	5308-DC	Test Org	Test Site	5308-DC	5308-DC	US	2023-10-27 14:23:23 (STI)
5309-DC	192.168.1.10	Dial-to-IP	5309-DC	Test Org	Test Site	5309-DC	5309-DC	US	2023-10-27 14:23:23 (STI)

Dial-to-IP device details

Field	Value
Organization	Test Org
Site	Test Site
Hardware	5301-DC
Chip	5301-DC
Country	US
Last Heartbeat (STI)	2023-10-27 14:23:23 (STI)
Management IP	192.168.1.1
Uplink IP Address	192.168.1.2
Primary Interface	eth0
Associated Devices	5300-DC

The majority of details provided on the Dial-to-IP device details page are applicable to all categories of devices. See [Device details page](#) for details on those table entries.

The following are device details specific to Dial-to-IP devices:

- **Management IP:** The IP address of the Dial-to-IP device's aView IPsec tunnel. If this IP does not match the aView tunnel IP address listed in the local web UI of the Dial-to-IP device, a user with the ability to modify devices can edit the Management IP address.
- **Uplink IP Address:** The IP address of the current WAN network connection of the Dial-to-IP device.
- **Primary Interface:** The currently used WAN connection interface.

Dial-to-IP device Configuration tab

Dial-to-IP devices are configured through the aView site. See [Create a new Dial-to-IP device configuration profile](#) for further information.

Dial-to-IP device Associated Devices tab

This tab lists any devices that the Dial-to-IP device has associated with, indicating that they are connected to each other. The tab will include the following details about the associated device.

- **Device ID:** The identifying MAC address for the associated device.
- **Model:** If the associated device is a type of device supported by ARMT, this entry will display the type of device ARMT knows it as. If the device is not supported by ARMT, the category will be listed with a dash (-).
- **Interface:** The physical interface of the Dial-to-IP device the associated device is connected to.
- **Type:** How the associated device is connected to the Dial-to-IP device. For example, a type listed as WAN indicates that the associated device is connected to one of the Dial-to-IP device's WAN Ethernet ports.
- **IP Address:** The IP address of the associated device.
- **Connected:** Indicates when the device association was made and how long the associated device has been connected to the Dial-to-IP device.

Dial-to-IP device Tunnels tab

The Tunnel tab lists status for any IPSec tunnels established by the Dial-to-IP device. Each row of the tab indicates a unique IPSec tunnel of the device.

- **Name:** The name of the IPSec tunnel, as specified in the configuration of the Dial-to-IP device.
- **Status:** Indicates whether or not the Dial-to-IP device has established the IPSec tunnel.
- **Last Updated:** The last time aView received an update concerning this tunnel.
- **IpLocal:** The tunnel IP address assigned to the Dial-to-IP device.
- **IpRemote:** The IP address of the server that the Dial-to-IP device built a tunnel to.
- **NetLocal:** The network settings on the Dial-to-IP device for the tunnel.
- **NetRemote:** The network settings on the server for the tunnel.

Dial-to-IP device Network tab

The Network tab lists details for network interfaces that belong to the Dial-to-IP device. If a Dial-to-IP device has multiple networks, there will be multiple network tabs, each one corresponding to one of the device's networks.

- **Connection Type:** the type of network connection for the interface.
- **Priority:** Indicates if the network connection is the current primary or alternate connection.
- **IP Ranges:** The IP addressing for the network.
- **MTU:** The MTU size of the network interface.
- **Gateway IP:** The default route (gateway IP) of the network interface.
- **Bytes Received:** The total amount of data received, measured in bytes, on the network interface since the Dial-to-IP device has been online (resets on reboot).
- **Bytes Transmitted:** The total amount of data transmitted, measured in bytes, on the network interface since the Dial-to-IP device has been online (resets on reboot).
- **Ethernet Speed:** If the network type is an Ethernet interface, then this indicates the speed of the Ethernet port.
- **Ethernet Status:** If the network type is an Ethernet interface, then this indicates the status of the physical connection on the Ethernet port.

Dial-to-IP device remote commands

Remote commands are sent to a Dial-to-IP device through an IPSEC tunnel the device establishes to the Accelerated remote control server, or through the upstream IP address of the device if no tunnel IP is available. All Dial-to-IP devices by default establish an IPsec tunnel to remote.accns.com. See [aView tunnel alternatives](#) for information about additional IPsec tunnel endpoints.

The tunnel IP address for the Dial-to-IP device is stored in aView as the Management IP on the **Device Details** tab. If the Management IP is not known, then aView will use the IP address listed in the **Uplink IP Address** field on the **Device Details** tab for sending remote commands.

When you send a remote command to a device, aView utilizes a DNS service running on the remote control server to verify what tunnel IP address is associated with the device. If the DNS service responds with a valid IP address, aView will send the remote command to that IP address, otherwise it will use the known Management IP or the Uplink IP Address if the Management IP is unknown. If the IP address returned by the DNS service differs than the Management IP listed for the device, aView will update the Management IP after successfully sending the remote command to the device.

Before sending the remote command to the Dial-to-IP device, aView will prompt the user to provide the device-level username and password to authenticate with the device. If you do not know the username or password for the device, navigate to the **Configuration** tab of the device in aView and select **Authentication > Users**. Select a user name to change the password. You can also change the password locally on the device by following the instructions in the device's user manual. For example, to view instructions for the EX15, visit

<https://www.digi.com/resources/documentation/digidocs/90002344/default.htm#os/user-local-change-pswd-t.htm>.

Once the username and password are provided for the device, aView will then perform a HTTP request to the device to validate that the correct device is at the given IP address. If the correct device is reached and authenticated, the remote command will be sent.

The available remote commands that can be sent to Dial-to-IP devices are:

- **Check status:** The Dial-to-IP device will immediately send its current status.
- **Check signal strength:** The Dial-to-IP device will send its signal strength and network info once every 10 seconds for the next 15 minutes.
- **Perform Speed Test:** The Dial-to-IP device will perform a speed test and send the Upload/Download results.
- **ARPing Attached Device:** The Dial-to-IP device will attempt to ARPing the client device attached to its Ethernet port.
- **Send Wake-on-LAN to Attached Device:** The Dial-to-IP device will send a wake-on-LAN packet to the client device attached to its Ethernet port.
- **Check Configuration:** The Dial-to-IP device will immediately pull its configuration and reboot to apply any new settings.
- **Reboot:** Reboot the Dial-to-IP device.

Dial-to-IP device emergency SMS commands

As an alternative to the Remote commands, you can also send commands via SMS messaging to a Dial-to-IP device. The SIM card used by the Dial-to-IP device must have SMS enabled, or you will not be able to send SMS commands.

The available SMS commands that can be sent are:

- **Set Configuration:** A pop-up window appears where a user can enter in a configuration option or set of options to apply to the Dial-to-IP device. Multiple config options must be separated by

a comma. For example, if a user wants to set the APN of a Dial-to-IP device to managedvpn, they would enter "modem_apn=managedvpn".

- **Configuration Reset:** Restore default configuration on the Dial-to-IP device and reboot.
- **Firmware Reset:** Restore to the backup firmware image on the Dial-to-IP device, and reboot.
- **Factory Reset:** Restore default configuration on the Dial-to-IP device, restore to the backup firmware image, and reboot.
- **Remote Control:** Tell the Dial-to-IP device to bring up its remote control tunnel (useful if on low data plan, so the remote control tunnel is not always up using data).
- **Reboot:** Reboot the Dial-to-IP device.

Dial-to_IP configuration requirements for aView

In order for the aView site to monitor a Dial-to_IP device, it must send its syslogs to the aView syslog server IP address, the domain of which is logs.accns.com.

For a Dial-to_IP device to get its configuration from the aView site, it must be set to pull its configuration from the aView configuration server configuration.accns.com. The device must also be able to sync its date and time with an NTP server; the default is time.accns.com.

In the device configuration, ensure the following options are set in **Service > Web administration**:

- **Enable** is selected.
- **Port** is set to **443**.
- **Access control list -> Zones** includes the **IPSec** zone.

This zone is included by default, but it's mentioned here for the user to verify that it is still present, in case the device is running settings that deviate from the default configuration.

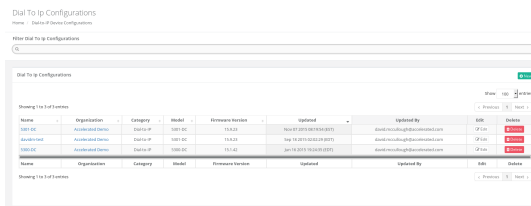
The screenshot shows the configuration interface for a device. The 'Services' section is expanded, and 'Web administration' is selected. The 'Enable' checkbox is checked, and the 'Port' is set to 443. The 'Access control list' section is also expanded, and the 'Zones' section is further expanded. A table lists the zones: 'Internal', 'IPsec', and 'Setup'. The 'IPsec' zone is highlighted with a red box.

Zone	Value
1. Zone	Internal
2. Zone	IPsec
3. Zone	Setup

View Dial-to-IP configuration profiles

To view the current list of group configuration profiles a user has access to:

1. Click on the **Configurations** button in the navigation panel.
2. Select **Dial-to-IP** in the drop-down.

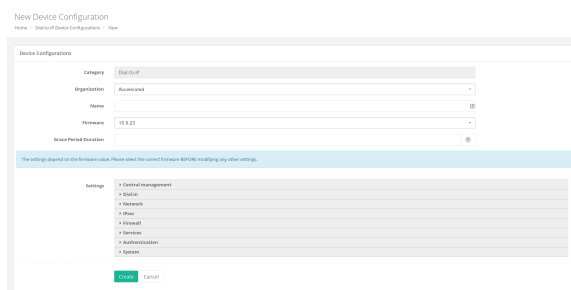


Create a new Dial-to-IP device configuration profile

To create a new group configuration profile:

1. Click on the **Configurations** button in the navigation panel.
2. Select **Dial-to-IP** in the drop-down.
3. Click the **plus** icon located at the top right of the window.
4. Select the firmware version. The appropriate configuration schema will automatically load.
5. Set any desired settings in the presented configuration schema. Hovering your mouse over the name for a configuration option will display a pop-up providing help details about that option, including any default values. Once all the desired configuration options have been specified, click **Create**.

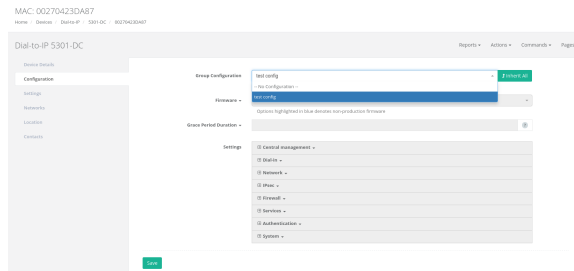
Note If the desired firmware is not listed, it must be uploaded onto the firmware management service, which is hosted at distro.accns.com.



Apply a Dial-to-IP configuration profile

To apply a group configuration profile to a Dial-to-IP device:

1. Go to the device details page for the specific device. This can be done by searching for the device's MAC address in the search bar, then clicking on the MAC address of the correct device in the results.
2. Once on the details page, click on the **Configuration** tab, select the new configuration profile from the **Group Configuration** drop-down, and click the **Save** button.



Individual device configuration settings

In addition to applying a group configuration profile to a device, authorized users will also have the option of setting configuration options to apply only to an individual device. These individual device configuration options are listed in the **Configuration** tab, below the **Group Configuration** option.

When a new group configuration is selected for a device, a list of inherited configuration settings from that group configuration profile will be displayed. Authorized users can then click on any setting and select the **Override** option to change the selected configuration option. It is important to note that any configuration option overridden in this way will only apply to that individual device. Any other devices that are linked to the same group configuration will only receive configuration settings from the group configuration profile, not any of the overridden settings from another individual device's configuration.

- **Inherit All:** This button can be used to reset an individual device's configuration back to the group configuration profile's settings. Any configuration options previously overridden in the individual device configuration will be undone and reset back to the settings inside the group configuration.

Delete a Dial-to-IP device configuration profile

To delete group configuration profiles:

1. From the Navigation bar, select **Configurations > Dial-to-IP**.
The **Dial-to-IP Configurations** page displays.
2. Click **Delete** for the appropriate Dial-to-IP configuration profile.
3. Click **OK** to confirm.

If there are any devices linked to the configuration profile that is being deleted, the profile will not be deleted. You must first unlink the configuration profile from the device and then delete the profile. See [Apply a Dial-to-IP configuration profile](#) for information about changing a device's configuration profile.

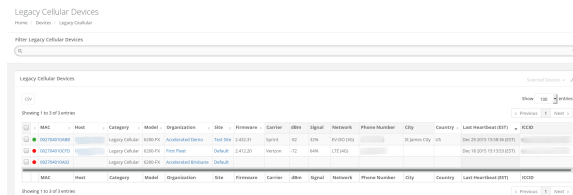
Legacy cellular devices

- About legacy cellular devices 63
- Legacy cellular device details 63
- Remote commands 66
- Legacy Cellular configuration requirements for aView 67

About legacy cellular devices

Legacy Cellular devices refer to the Digi Cellular Extender line of products. Supported models are listed below. A user can find a list of all the cellular devices they have access to by clicking on the Devices tab in the navigation bar, and then select the Cellular link from the drop-down.

- 6200-FX
- NetBridge-SX



The screenshot shows a web interface titled "Legacy Cellular Devices". It features a search bar and a table with columns: Host, Category, Model, Organization, Site, Firmware, Carrier, dBm, Signal, Network, Phone Number, City, Country, and Last Heartbeat (UTC). The table lists three devices, all of which are "6200-FX" models from "Accelerated Brisbane". The first device has a status of "Device is up", while the others are "Device is down".

Legacy Cellular devices are listed in tabular form. The majority of the details are applicable to all device categories. See [Device details page](#) for details on those table entries.

The table entries specific to cellular devices are:

- **Carrier:** The cellular carrier of the current connection, indicating the owner of the local cellular network and modem tower.
- **Provider:** The cellular provider of the current connection, indicating who provisioned the SIM card.
- **dBm:** The RSSI signal strength of the cellular connection measure in dBm.
- **Signal:** The RSSI signal strength percentage of the cellular connection.
- **Network:** The technology type of the cellular connection.
- **Phone Number:** The phone number of the current cellular connection.

Legacy cellular device details

MAC: 002704010A02
Home / Devices / Legacy Cellular / 6200-FX / 002704010A02

Legacy Cellular 6200-FX Reports Actions Commands Pages

Device Details	Organization: Accelerated Brisbane Site ID: Davids Test Lab Configuration: davidm-default MAC Address: 002704010A02 Serial: 6200010001461366 Status: Device is up Model: 6200-FX Cellular IP Address: View details Firmware Version: 2.432.31 Client MAC Address: N/A Client IP Address: N/A Ethernet Status: unplugged USB Conditioner: N/A USB List: 0F3d-f8aa Management Tunnel Status: Not Connected Power Outlet #1: On Power Outlet #2: On Activated At: Jul 07 2014 00:09:20 (EDT) Last Heartbeat: May 18 2016 16:13:25 (EDT) Last Restart: May 16 2016 21:11:18 (EDT) Data Plan: David Plan Data Plan Individual Limit: N/A Data Plan Usage: 10.23 MB
----------------	---

The majority of details provided on the cellular device details page are applicable to all categories of devices. See [Device details page](#) for details on those table entries.

The device details specific to cellular devices are listed below.

- **Cellular IP Address:** The IP address received when connecting to the cellular network.
- **Client MAC Address:** The MAC address of the client device (the device connected to the Cellular Extender's Ethernet port).
- **Client IP Address:** The IP address the Cellular Extender device assigned to the client device (the device connected to its Ethernet port).
- **Ethernet Status:** The status of the physical link on the Ethernet port of the Cellular Extender.
- **USB Conditioner:** Indicates if a USB Conditioner hub device is connected between the Cellular Extender and the USB modem.
- **USB List:** Lists the vendor and product IDs of any USB devices connected to the Cellular Extender.
- **Management Tunnel Status:** Indicates whether the remote command IPSec tunnel is up and active, or disabled. If disabled or down, users will not be able to send remote commands to the Legacy Cellular Device. Note that SMS commands will still work if the SIM card used by the Legacy Cellular device has SMS enabled.

Legacy Cellular device Settings tab

The majority of details provided on the Legacy Cellular **Settings** tab are applicable to all categories of devices. See [Settings tab](#) for details on those table entries.

The device details specific to Legacy Cellular devices are:

- **Data Plan:** The data plan assigned to the device. If the user has the ability to change the data plan, a drop-down will be displayed and lists the available data plans for the organization the device belongs to. Once a data plan is associated with the device, any cellular data used by the device will be tracked in the data plan, which can be viewed and managed by clicking the **Edit** button for an Organization (see [Organizations](#)). You also have the option of creating a new data plan if desired.

Legacy Cellular device Configuration tab

Cellular devices are configured through the aView site. See [Create a new Legacy Cellular configuration profile](#) for further information.

Legacy Cellular Associated device tab

This tab lists any devices that the Legacy Cellular device has associated with, indicating that they are connected to each other. The tab will include the following details about the associated device.

- **Device ID:** The identifying MAC address for the associated device.
- **Model:** If the associated device is a type of device supported by ARMT, this entry will display the type of device ARMT knows it as. If the device is not supported by ARMT, the category will be listed with a dash (-).
- **Interface:** The physical interface of the Legacy Cellular device the associated device is connected to.

- **Type:** How the associated device is connected to the Legacy Cellular device. For example, a type listed as LAN indicates that the associated device is connected to one of the Legacy Cellular device's LAN Ethernet ports.
- **IP Address:** The IP address of the associated device.
- **Connected:** Indicates when the device association was made and how long the associated device has been connected to the Legacy Cellular device.

Legacy Cellular device Cellular details tab

The **Cellular Details** tab lists details for the cellular modem. The name of the cellular modem is listed in the title bar of the **Cellular Details** tab. In the example above, the cellular modem name is Sierrawireless340u. If a cellular device has multiple modems, there will be multiple tables, each one corresponding to one of the cellular device's modems. A modem entry can be removed by clicking the red trash icon at the top-right of the specific tab.

- **Carrier:** The cellular provider of the modem.
- **Signal Strength:** The current RSSI signal strength value, measured in dBm, and percentage of the modem.
- **Signal Bars:** The current signal bars, based on the signal strength.
- **Speed Test:** The five most recent (if any) speed tests performed on the device. Speed tests are generated by sending a Speed Test command to the device.

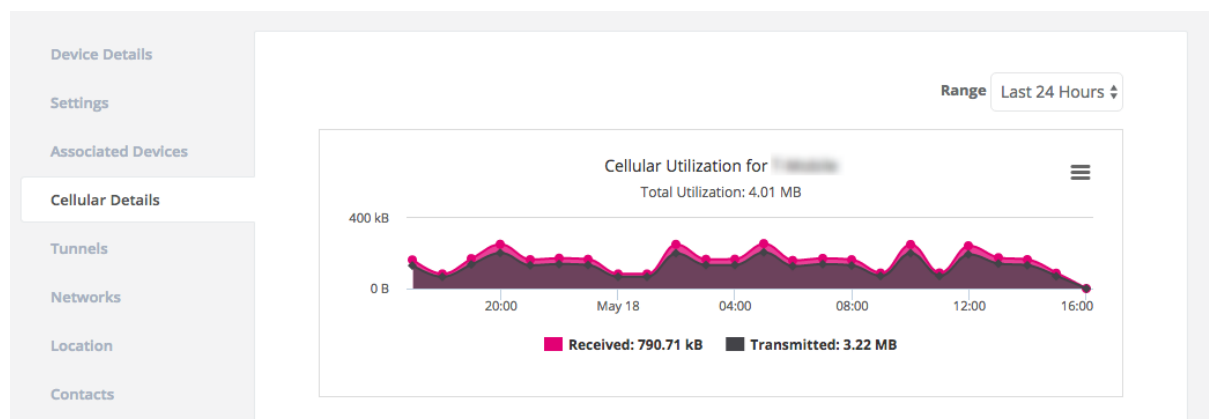
Note In order to minimize the speed test's impact on cellular data consumption, the results are an estimation of the available throughput of the device, and may not represent the full network speed available.

- **Phone Number:** The phone number of the modem.
- **RSSI:** The Received Signal Strength Indicator (RSSI) of the modem. RSSI provides information about total received wide-band power, including signal interference and thermal noise.
- **RSRP:** An LTE-specific value, representing the Reference Signal Received Power of the modem. RSRP is the average power of resource elements that carry cellular specific reference signals over the entire bandwidth.
- **RSRQ:** An LTE-specific value, representing the Reference Signal Receive Quality (RSRQ) of the modem. RSRQ is a combination of RSSI and RSRP and indicates the quality of the received reference signal.
- **SiNR:** The signal-to-interference-plus-noise ratio of the modem.
- **SNR:** The signal-to-noise ratio of the modem.
- **IMEI:** The IMEI value of the modem.
- **ESN:** The ESN value of the modem. Note that the ESN value only applies to CDMA cellular networks.
- **ICCID:** The ICCID value of the modem.
- **Revision:** The hardware version of the modem.
- **APN:** The APN that the modem is currently connected with. Note that not all modems require an APN.
- **ECIO:** The signal-to-noise ratio of the modem. The lower the Ec/Io value, the greater the noise.
- **CNTI:** The technology type that the modem is currently connected to.

- **Band:** The frequency or type of cellular band the modem is currently connected to.
- **CID:** The CID identifier of the modem's current connection.
- **LAC:** The LAC identifier of the modem's current connection.
- **MCC:** The mobile country code of the modem's current connection.
- **MNC:** The mobile network code of the modem's current connection.
- **PLMN:** The PLMN ID of the modem's current connection, which is a combination of the MCC and MNC values.
- **USB Speed:** The speed of the USB port(s) on the Legacy Cellular device, measured in Mbps. 480 indicates USB 2.0 High Speed and 12 indicates USB 2.0 Full Speed.

Cellular utilization chart

If the device supports a cellular modem, a cellular utilization chart will be displayed. The chart shows the amount of cellular data used by the device. The initial timespan will display the data usage for the past 24 hours. You can select different timespans from the Range drop-down.



Legacy Cellular device Tunnels tab

The **Tunnels** tab lists status for any IPSec tunnels established by the Legacy Cellular device. Each row of the tab indicates a unique IPSec tunnel of the device.

- **Name:** The name of the IPSec tunnel, as specified in the configuration of the Legacy Cellular device.
- **Status:** Indicates whether or not the Legacy Cellular device has established the IPSec tunnel.

Remote commands

Remote commands are sent to a cellular device through an IPSec tunnel the cellular device establishes to the Digi remote control server. If the remote control IPSec tunnel is disconnected, then a user will not be able to send remote commands to the cellular device. The available remote commands that can be sent to cellular devices are listed below.

- **Check status:** The cellular device will immediately send its current status.
- **Check signal strength:** The cellular device will send its signal strength and network info once every 10 seconds for the next 15 minutes.

- **Perform Speed Test:** The cellular device will perform a speed test and send the Upload/Download results.

Note In order to minimize the speed test's impact on cellular data consumption, the results are an estimation of the available throughput of the device, and may not represent the full network speed available.

- **ARPing Attached Device:** The cellular device will attempt to ARPing the client device attached to its Ethernet port.
- **Send Wake-on-LAN to Attached Device:** The cellular device will send a wake-on-LAN packet to the client device attached to its Ethernet port.
- **Check Configuration:** The cellular device will immediately pull its configuration and reboot to apply any new settings.
- **Reboot:** Reboot the cellular device.

Legacy Cellular device emergency SMS commands

As an alternative to the Remote commands, you can also send commands via SMS messaging to a Legacy Cellular device. The SIM card used by the Legacy Cellular device must have SMS enabled, or you will not be able to send SMS commands.

The available SMS commands that can be sent are:

- **Set Configuration:** A pop-up window appears where a user can enter in a configuration option or set of options to apply to the Legacy Cellular device. Multiple config options must be separated by a comma. For example, if a user wants to set the APN of a Legacy Cellular device to managedvpn, they would enter "modem_apn=managedvpn".
- **Configuration Reset:** Restore default configuration on the Legacy Cellular device and reboot.
- **Firmware Reset:** Restore to the backup firmware image on the Legacy Cellular device, and reboot.
- **Factory Reset:** Restore default configuration on the Legacy Cellular device, restore to the backup firmware image, and reboot.
- **Remote Control:** Tell the Legacy Cellular device to bring up its remote control tunnel (useful if on low data plan, so the remote control tunnel is not always up using data).
- **Reboot:** Reboot the Legacy Cellular device.

Remote power commands

If a Remote Power device is connected via serial-to-USB cable to the Cellular Extender, these remote commands can be used to toggle the power on or off on either of the Remote Power device's outlets.

Legacy Cellular configuration requirements for aView

In order for the aView site to monitor a Legacy Cellular device, it must send its syslogs to the aView syslog server IP address, the domain of which is logs.accns.com.

For a Legacy Cellular device to get its configuration from the aView site, it must be set to pull its configuration from the aView configuration server configuration.accns.com. The device must also be able to sync its date and time with an NTP server; the default is time.accns.com.

In the device configuration, ensure the following options are set in **Service > Web administration**:

- **Enable** is selected.
- **Port** is set to **443**.
- **Access control list** -> **Zones** includes the **IPSec** zone.

This zone is included by default, but it's mentioned here for the user to verify that it is still present, in case the device is running settings that deviate from the default configuration.

The screenshot shows the 'Services' configuration page. Under 'Web administration', the 'Enable' checkbox is checked and the 'Port' is set to 443. Under 'Access control list', the 'Zones' section is expanded, showing a list of zones: 1. Zone: Internal, 2. Zone: IPSec (highlighted with a red box), and 3. Zone: Setup.

Create a new Legacy Cellular configuration profile

Before creating a new cellular configuration profile, first decide if the profile should inherit any settings from another configuration profile (referred to as the 'parent configuration'). This adds the benefit of having a structured and/or tiered configuration environment, where a new configuration inherits all the defaults for an organization, and the user adds the necessary changes to those base settings. To view the current list of configuration profiles a user has access to, click on the Configurations button in the navigation panel and then select Legacy Cellular in the drop-down.

The screenshot shows the 'Legacy Cellular Configurations' page. It displays a table of configurations. The table has columns: Name, Organization, Updated, and Actions. The table lists several configurations, including 'Legacy Cellular' and 'Legacy Cellular (Parent)'. The 'Legacy Cellular' configuration is highlighted with a red box.

Name	Organization	Updated	Actions
Legacy Cellular	Legacy Cellular	Nov 04 2015 10:00:00 (UTC)	View Edit Delete
Legacy Cellular (Parent)	Legacy Cellular	Nov 04 2015 10:00:00 (UTC)	View Edit Delete
Legacy Cellular (Child)	Legacy Cellular	Nov 04 2015 10:00:00 (UTC)	View Edit Delete
Legacy Cellular (Child)	Legacy Cellular	Nov 04 2015 10:00:00 (UTC)	View Edit Delete
Legacy Cellular (Child)	Legacy Cellular	Nov 04 2015 10:00:00 (UTC)	View Edit Delete

To create a new configuration profile, first navigate to the Configurations section of aView by clicking on the Configurations button in the navigation panel, and then select Legacy Cellular in the drop-down. Next click the plus icon located at the top right of the window to create a new cellular configuration. Specify a name for the configuration profile and select the desired parent configuration. If a user does not select a parent configuration, the profile will inherit the system default values for a cellular device.

Next, enter in any other desired configuration options. Refer to the help boxes for each configuration option for details on what the option is used for as well as what the default value is for the option. Required fields are marked with asterisks (*) and any values inherited from the parent configuration are listed in red. Once all the desired configuration options have been specified, click Create.

Legacy Cellular Configuration: Nate Test
Home / Legacy Cellular Configurations / Nate Test

Settings
 Admin Settings
 Device Management
 Basic IP
 DHCP Options
 DNS Options
 Network Management
 Logging Options
 Port Forwarding
 Monitoring
 Storage

Configuration Name *
 Organization: **Accredited Demo**
 Parent Configuration: **Accredited Demo**
 Firmware Image (IG): **selected value: 6.06.01**
 Firmware Image (IG): **selected value: 6.06.01**
 Config Server: **https://www.accredi.com**
 EIS override: **selected value: 6.06.01**
 Certificate URL: **https://www.accredi.com/certificates/6.06.01**
 Notifications: **selected value: 6.06.01**
 Configuration Change Causes Reboot?: **selected value: 6.06.01**
 Firmware Server: **selected value: 6.06.01**
 System Unattended Reboot: **selected value: 6.06.01**
 Ping Test List: **selected value: 6.06.01**
 Network Manager: **selected value: 6.06.01**
 Enable Remote Control Tunnel: **selected value: 6.06.01**
 SMI Check Frequency: **selected value: 6.06.01**
 Upload Server: **selected value: 6.06.01**
 Restart: **selected value: 6.06.01**
 Enable Watchdog: **selected value: 6.06.01**

Linked Devices
 Showing 1 of 177 entries
 Previous Next

Device ID	Model	Organization	Site	Carrier	APN	Signal	Network	Phone Number	Firmware	Capacity	Last Heartbeat
002704010A8B	6200-FX	Accredited Demo	Test Site	Verizon	verizon	100	4G	201-123-4567	6.06.01	100	2023-10-26 15:15:00 (UTC)

 Showing 1 of 177 entries
 Previous Next

Apply a cellular configuration profile

To apply a configuration profile to a cellular device, go to the device details page for the specific device. This can be done by searching for the device's MAC address in the search bar, then clicking on the MAC address of the correct device in the results. Once on the details page, select the new configuration profile from the Configuration drop-down menu below the Admin panel.

Device ID: 002704010A8B
Home / Legacy Cellular / 6200-FX / 002704010A8B

Legacy Cellular 6200-FX
Reports Actions Comments Settings Pages

Details
Settings
 Devices
 Locations
 Contacts

Organization: **Accredited Demo**
 Model ID: **6200-FX**
 Show Details of this Test Site
 Service Name: **6200-FX**
 Configuration: **selected value: 6.06.01**
 Data Plan: **selected value: 6.06.01**
 Update Settings

Delete a configuration profile

Configuration profiles can be deleted by selecting the desired configuration name on the Legacy Cellular **Configurations** page, then select the **Delete Configuration** button at the top right of the profile. Note that if there are any devices linked to the configuration profile that is being deleted, the profile will not be deleted. You must first unlink the configuration profile from the device and then you can remove the profile.

VPN Gateway devices

- About VPN Gateway devices 71
- Configure down status for VPN gateway devices 71
- VPN Gateway device details 72
- VPN Gateway Remote commands 77
- VPN Gateway configuration requirements for aView 78

About VPN Gateway devices

Gateway devices refer to the AT&T VPN Gateway line of products. Supported models are listed below. You can find a list of all the Gateway devices you have access to by clicking on the **Devices** link in the navigation bar, and then select the Gateway link from the drop-down.

- U115
- U110
- VPN Gateway 8300
- VPN Gateway 8200
- VPN Gateway 8100

Name	Host	Category	Model	Organization	Site	Firmware	Tunnels	Connection	City	Country	Last Heartbeat (DTI)
VPN-GW-8100-001	192.168.1.1	Gateway	8100	ORGANIZATION	Site	1.1.1.1	1	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8200-002	192.168.1.2	Gateway	8200	ORGANIZATION	Site	1.1.1.1	2	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8300-003	192.168.1.3	Gateway	8300	ORGANIZATION	Site	1.1.1.1	3	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8100-004	192.168.1.4	Gateway	8100	ORGANIZATION	Site	1.1.1.1	1	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8200-005	192.168.1.5	Gateway	8200	ORGANIZATION	Site	1.1.1.1	2	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8300-006	192.168.1.6	Gateway	8300	ORGANIZATION	Site	1.1.1.1	3	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8100-007	192.168.1.7	Gateway	8100	ORGANIZATION	Site	1.1.1.1	1	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8200-008	192.168.1.8	Gateway	8200	ORGANIZATION	Site	1.1.1.1	2	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8300-009	192.168.1.9	Gateway	8300	ORGANIZATION	Site	1.1.1.1	3	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8100-010	192.168.1.10	Gateway	8100	ORGANIZATION	Site	1.1.1.1	1	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8200-011	192.168.1.11	Gateway	8200	ORGANIZATION	Site	1.1.1.1	2	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8300-012	192.168.1.12	Gateway	8300	ORGANIZATION	Site	1.1.1.1	3	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8100-013	192.168.1.13	Gateway	8100	ORGANIZATION	Site	1.1.1.1	1	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8200-014	192.168.1.14	Gateway	8200	ORGANIZATION	Site	1.1.1.1	2	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8300-015	192.168.1.15	Gateway	8300	ORGANIZATION	Site	1.1.1.1	3	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8100-016	192.168.1.16	Gateway	8100	ORGANIZATION	Site	1.1.1.1	1	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8200-017	192.168.1.17	Gateway	8200	ORGANIZATION	Site	1.1.1.1	2	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8300-018	192.168.1.18	Gateway	8300	ORGANIZATION	Site	1.1.1.1	3	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8100-019	192.168.1.19	Gateway	8100	ORGANIZATION	Site	1.1.1.1	1	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8200-020	192.168.1.20	Gateway	8200	ORGANIZATION	Site	1.1.1.1	2	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8300-021	192.168.1.21	Gateway	8300	ORGANIZATION	Site	1.1.1.1	3	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8100-022	192.168.1.22	Gateway	8100	ORGANIZATION	Site	1.1.1.1	1	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8200-023	192.168.1.23	Gateway	8200	ORGANIZATION	Site	1.1.1.1	2	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8300-024	192.168.1.24	Gateway	8300	ORGANIZATION	Site	1.1.1.1	3	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8100-025	192.168.1.25	Gateway	8100	ORGANIZATION	Site	1.1.1.1	1	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8200-026	192.168.1.26	Gateway	8200	ORGANIZATION	Site	1.1.1.1	2	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8300-027	192.168.1.27	Gateway	8300	ORGANIZATION	Site	1.1.1.1	3	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8100-028	192.168.1.28	Gateway	8100	ORGANIZATION	Site	1.1.1.1	1	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8200-029	192.168.1.29	Gateway	8200	ORGANIZATION	Site	1.1.1.1	2	VPN			Dec 29 2015 15:10:00 (DTI)
VPN-GW-8300-030	192.168.1.30	Gateway	8300	ORGANIZATION	Site	1.1.1.1	3	VPN			Dec 29 2015 15:10:00 (DTI)

Gateway devices are listed in tabular form. The majority of the details are applicable to all device categories. See [Device details page](#) for details on those table entries. The table entries specific to Gateway devices are:

- **Tunnels:** The current number of VPN tunnels the Gateway device has up as of when this page was loaded.
- **Connection:** The connection currently being used by the Gateway device as of when this page was loaded.

Configure down status for VPN gateway devices

VPN Gateway devices are monitored by Digi aView using SNMP probes.

Configuring when a Gateway device is considered down (red status) in Digi aView is done by adjusting the **Probe Interval** and **Missed Probes before Down** options in the **Organization** settings for the Gateway device. These settings will apply to all devices that belong to that organization.

ATAP

Information

Roles

Permissions

Device Settings

Data Plans

SNMP Probes

Probe Interval

Every 15 minutes

Missed Probes Before Down

2 missed probes for down status

With these settings, your device could be down for up to 30 minutes before reporting.

Save Changes

Probe Interval

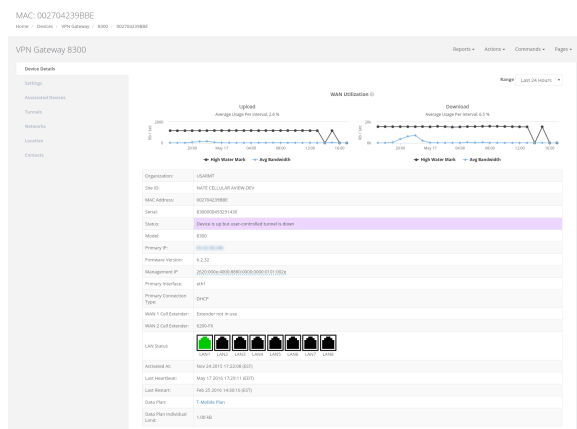
The **Probe Interval** option controls how often Digi aView sends an SNMP probe to the VPN Gateway. By default, Digi aView probes the VPN Gateway once every 15 minutes. Each probe pulls the most recent status details from the VPN Gateway and updates the details in Digi aView with the results.

Missed Probes Before Down

The **Missed Probes Before Down** option controls how many probes can be missed before Digi aView considers a device as **Down**. The default number of missed probes is two. When the **Missed Probes Before Down** (two) is combined with the default probe interval of 15 minutes, the amount of time at which Digi aView considers a Gateway device as down if it has not heard from the device is 30 minutes (2 times 15 minutes).

Note In addition to performing SNMP probes to the VPN Gateway, the VPN Gateway itself can send SNMP informs/traps to Digi aView. This can also affect when Digi aView considers the device as down. For Digi aView to consider the device as down, no SNMP probe responses, SNMP traps, or SNMP informs would have been received within the specified time window, as specified in these **SNMP Probe** settings (default 30 minutes).

VPN Gateway device details



The majority of details provided on the Gateway device details page are applicable to all categories of devices. See [Device details page](#) for details on those table entries.

The device details specific to Gateway devices are:

- **Primary IP:** The IP address of the current WAN network connection of the Gateway device.
- **Firmware Rollback:** The rollback firmware version. Issuing the Rollback remote command to the Gateway device will cause it to revert to the rollback firmware version specified here.
- **Management IP:** The IP address of the Gateway device's management tunnel. If this IP does not match the maintenance tunnel IP address listed for the Gateway device in the AT&T Service Manager, a user with the ability to modify devices will be given an option to edit the management IP address.
- **Configuration Model:** The configuration model associated in the Service Manager profile for the VPN Gateway.

- **Primary Interface:** The currently used WAN connection interface. For example, eth1 corresponds to the WAN1 port of the VPN Gateway.
- **Primary Connection Type:** The type of network configuration of the current WAN connection.
- **WAN 1 Cell Extender:** Indicates if the WAN via Cell Extender option is enabled in the Gateway device's AT&T Service Manager profile.

Note This field will only appear if there is a valid value entered in the Service Manager profile (not blank).

- **WAN 2 Cell Extender:** Indicates if the WAN2 via Cell Extender option is enabled in the Gateway device's AT&T Service Manager profile.

Note This field will only appear if there is a valid value entered in the Service Manager profile (not blank).

- **Time in Backup:** If the current status of the VPN Gateway is in backup mode, this will indicate the duration that the VPN Gateway has been running in backup mode. This field will only be displayed when the VPN Gateway is in backup mode.
- **LAN Status:** The status of the eight LAN ports of the VPN Gateway. A black color status indicates that nothing is physically connected to the LAN port. A green status indicates that some network device is physically connected to the LAN port. Hover over each port to display text with network details about the port.

VPN Gateway WAN utilization

If a VPN Gateway's Service Manager profile has COS or non-COS bandwidth monitoring enabled, and the VPN Gateway's profile has the WAN Utilization SNMP inform enabled, a WAN utilization chart will be displayed detailing the amount of bandwidth used by the device. Note, the VPN Gateway must be on firmware version 6.2 or higher in order to enable non-COS bandwidth monitoring. For COS bandwidth monitoring, the VPN Gateway must be on firmware version 6.4.546 or higher.

VPN Gateway device Settings tab

The majority of details provided on the VPN Gateway **Settings** tab are applicable to all categories of devices. See [Settings tab](#) for details on those table entries.

The device details specific to VPN Gateway devices are:

- **Data Plan:** The data plan assigned to the device. If the user has the ability to change the data plan, a drop-down will be displayed and lists the available data plans for the organization the device belongs to. Once a data plan is associated with the device, any cellular data used by the device will be tracked in the data plan, which can be viewed and managed by clicking the **Edit** button for an Organization (see [Organizations](#)). You also have the option of creating a new data plan if desired.

VPN Gateway devices Associated Devices tab

This tab lists any devices that the Gateway device has associated with, indicating that they are connected to each other. The tab will include the following details about the associated device:

- **Device ID:** The identifying MAC address for the associated device.
- **Model:** If the associated device is a type of device supported by ARMT, this entry will display the type of device ARMT knows it as. If the device is not supported by ARMT, the category will be listed with a dash (-).
- **Interface:** The physical interface of the Gateway device the associated device is connected to.
- **Type:** How the associated device is connected to the Gateway device. For example, a type listed as WAN indicates that the associated device is connected to one of the Gateway device's WAN Ethernet ports.
- **IP Address:** The IP address of the associated device.
- **Connected:** Indicates when the device association was made and how long the associated device has been connected to the Gateway device.

VPN Gateway devices Cellular Details tab

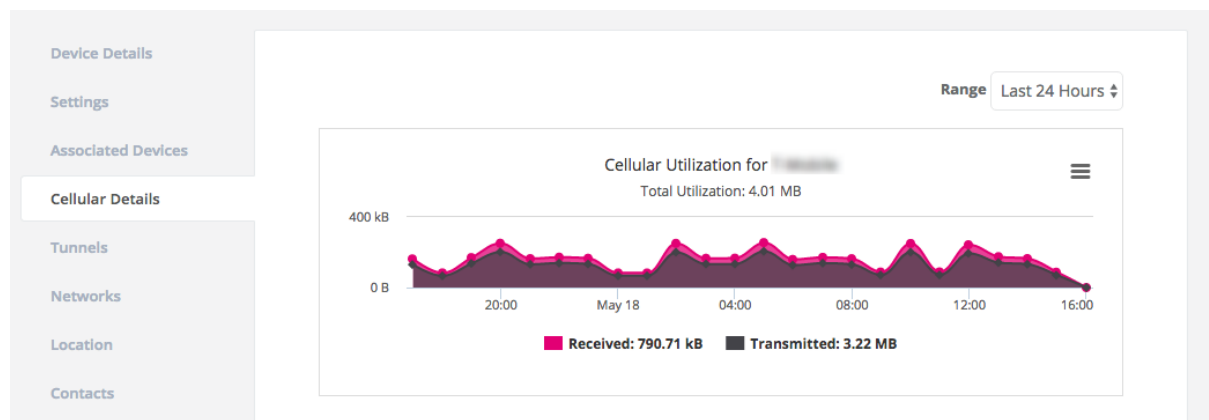
The **Cellular Details** tab lists details for the VPN Gateway's cellular modem, if it is using one. The name of the cellular modem is listed in the title bar of the Modem table. If a Gateway device has multiple modems, there will be multiple modem panels, each one corresponding to one of the cellular device's modems. A modem entry can be removed by clicking the red trash icon at the top-right of the specific tab.

- **Carrier:** The cellular provider of the modem.
- **Signal Strength:** The current RSSI signal strength value, measured in dBm, and percentage of the modem.
- **Phone Number:** The phone number of the modem.
- **RSSI:** The Received Signal Strength Indicator (RSSI) of the modem. RSSI provides information about total received wide-band power, including signal interference and thermal noise.
- **RSRP:** An LTE-specific value, representing the Reference Signal Received Power of the modem. RSRP is the average power of resource elements that carry cellular specific reference signals over the entire bandwidth.
- **RSRQ:** An LTE-specific value, representing the Reference Signal Receive Quality (RSRQ) of the modem. RSRQ is a combination of RSSI and RSRP and indicates the quality of the received reference signal.
- **SiNR:** The signal-to-interference-plus-noise ratio of the modem.
- **SNR:** The signal-to-noise ratio of the modem.
- **IMEI:** The IMEI value of the modem.
- **ESN:** The ESN value of the modem. Note that the ESN value only applies to CDMA cellular networks.
- **ICCID:** The ICCID value of the modem.
- **IMSI:** The IMSI value of the modem.
- **Revision:** The hardware version of the modem.
- **APN:** The APN that the modem is currently connected with. Note that not all modems require an APN.
- **ECIO:** The signal-to-noise ratio of the modem. The lower the E_c/I_o value, the greater the noise.
- **CNTI:** The technology type that the modem is currently connected to.
- **Band:** The frequency or type of cellular band the modem is currently connected to.

- **CID:** The CID identifier of the modem's current connection.
- **LAC:** The LAC identifier of the modem's current connection.
- **MCC:** The mobile country code of the modem's current connection.
- **MNC:** The mobile network code of the modem's current connection.
- **PLMN:** The PLMN ID of the modem's current connection, which is a combination of the MCC and MNC values.

VPN Gateway device Cellular Utilization chart

If a VPN Gateway's primary WAN connection is a cellular connection, and the device belongs to an organization with the Enable Cellular Modem Data Collection option enabled (see the Device Settings details in the Organizations section), a cellular utilization chart will be displayed on the Cellular Details tab detailing the amount of cellular data used by the device.



VPN Gateway device Tunnels tab

The **Tunnel** tab lists details for the VPN tunnel established by the gateway device. If a Gateway device has multiple tunnels active, there will be multiple tunnel tabs, each one corresponding to one of the Gateway device's tunnels.

- **Name:** The name of the tunnel, as specified in the Service Manager profile.
- **Connection ID:** The unique identifier for the current tunnel connection.
- **Connection Type:** The type of network connection the tunnel is established over.
- **Account:** The account that the tunnel settings are registered under.
- **User ID:** The ATTUID that the tunnel settings are registered under.
- **Duration:** The total time the current tunnel has been established as of when this page was loaded.
- **Mode:** Indicates if the user can control the tunnel.
- **Endpoint Type:** The authentication server that will be used by the tunnel endpoint.
- **Endpoint IP:** The IP address of the tunnel endpoint.
- **WAN Connection:** The type of network configuration of the current WAN connection (WAN1, WAN2, etc.).
- **AGNS Managed:** The service the tunnel is authenticated for.

- **Auth Server:** The server where the tunnel details are configured.
- **Auth Protocol:** The authentication protocol for the tunnel.
- **Initiator:** Indicates how the tunnel was initiated.
- **Last Updated:** The last time aView received an update concerning this tunnel.

VPN Gateway device Location tab

The location details for a VPN Gateway device are provided through the AT&T Service Manager profile of the device. As such, location details are displayed as read-only for VPN Gateway devices. If you want to set the location of a VPN Gateway device, they can do so through the Service Manager profile for the VPN Gateway. In the profile, users can specify address details for the location, which aView will then use to look up location coordinates for the device, or users can specify the latitude and longitude coordinates manually in the Service Manager profile.

VPN Gateway device Intelliflow tab

The Intelliflow tab displays metrics gathered from the summarized netflows sent from the VPN Gateway device to the aView netflow collector. For these netflows to be sent, the VPN Gateway's Service Manager profile must:

- Have the ARMT Netflow flag enabled.
- Use version 10 of netflow.
- Send its netflows to the aView netflow collector.
- Add a firewall rule to the VPN Gateway device's policy list to allow netflow packets to pass out through the device's maintenance tunnel to aView.

The metrics displayed on the Intelliflow tab detail the top 10 sources and destinations.

- **Source:** A source is an endpoint that clients request data from.
- **Destintation:** A client connected to the VPN Gateway devices's LAN ports, or the VPN Gateway device itself.

The source/destination labeling is used, because most network traffic is clients downloading traffic from the Internet. If a customer's VPN Gateway traffic is instead mostly uploading data, the source/destination labels will be reversed, meaning the clients connected to the VPN Gateway will be the source, and the destination will be the endpoints the clients are uploading data to.

Note Only IPv4 traffic is captured by the VPN Gateway and sent as summarized netflows to aView.

VPN Gateway Connectivity Tests tab

This tab lists the 10 most recent backup connectivity tests reported by the VPN Gateway device, including:

- **Result:** whether the test passed or failed
- **Reason:** the error code (if applicable)
- **Category:** the category of the failed test (if applicable)
- **Source:** whether the test was manually triggered or automated
- **Date:** when the test was executed

VPN Gateway IDS tab

This tab lists a count of IDS (intrusion detection) alerts detected by the VPN Gateway. The alerts are broken down by IDS type and displayed on a table, showing details for each type of alert and how many of each alert type was received.

The alerts are sent from the VPN Gateway to a Kafka REST API on ARMT. The VPN Gateway must be running firmware version 6.5.0 or higher to send these alerts. The chart on the tab lists a total number of alerts received per day (if any) over the past 30 days.

VPN Gateway Remote commands

Remote commands are sent to a VPN Gateway device through its management tunnel. If the Gateway device's management tunnel to the aView site is disconnected, then you will not be able to send remote commands to the Gateway device. The available remote commands that can be sent to gateway devices are listed below. Any responses from sending one of these remote commands to a Gateway device will be listed as an event in aView.

Firmware version 6.1.8 or newer

- **Arping:** Send an network ARPing to a specified IP address.
- **Check Status:** Perform an immediate SNMP probe of the gateway. device.
- **Firmware:** either check if a firmware update is available, or tell the Gateway device to upgrade its firmware. The specified firmware version is based on the firmware URL defined in the gateway's AT&T Service Manager profile. There is also an option to revert the device to the rollback firmware version.
- **Ping:** ping a specified IP address.
- **Profile Query:** Send the command to perform a partial or full configuration update from the device's AT&T Service Manager profile.
- **Reboot:** Send the command to reboot the Gateway device.
- **Tracepath:** trace the path to a specified network IP address, discovering MTU along this path
- **Traceroute:** trace the network path to a specified IP address.
- **Wan Toggle:** enable or disable a WAN interface on the Gateway device for a specified amount of time. The Gateway device must be on firmware version 6.5.0 or higher to accept this command.
- **Backup WAN Test:** manually run a backup connectivity test on the secondary WAN connection. The Gateway device must be on firmware version 6.5.0 or higher to accept this command.
- **Tunnels:** provides the ability to check the status of all configured outbound tunnels of a Gateway device, including bring a tunnel up/down, bounce a tunnel, or checking a tunnel's status. The name and index of the desired outbound tunnel must be specified to perform these commands.

Firmware versions older than 6.1.8

- **Check Device Status:** Perform an immediate SNMP probe of the gateway device.
- **Check Configuration:** Send the command to perform a partial or full update depending on the

configuration option specified in the gateway device's AT&T Service Manager profile.

- **Reboot Device:** Send the command to reboot the Gateway device.

VPN Gateway configuration requirements for aView

aView utilizes a management tunnel to communicate with the gateway device. The management tunnel must be configured correctly in order for aView to be able to probe and send commands to the Gateway device. Contact your AT&T Service Manager specialist if assistance is needed configuring the management tunnel of the Gateway device.

In addition to the management tunnel, the Gateway device must be configured to send its SNMP Informs to the aView server. Several of the notifications sent by aView are based on the SNMP informs sent by the Gateway device. Contact your AT&T Service Manager specialist if assistance is needed configuring the SNMP Inform options of the Gateway device.

Remote Manager devices

- About Remote Manager devices 80
- Remote Manager device details 80
- Remote Manager device remote commands 84
- Remote Manager configuration requirements for aView 85

About Remote Manager devices

Remote Manager devices refer to the Digi Remote Manager line of products. Supported models are listed below. A user can find a list of all the Remote Manager devices they have access to by clicking on the Devices tab in the navigation bar, and then select the Remote Manager link from the dropdown.

- 5300-RM
- 5400-RM
- 5401-RM
- ConnectIT4

[illegible]

Remote Manager devices are listed in tabular form. The majority of the details are applicable to all device categories. See [Device details page](#) for details on those table entries.

The table entries specific to Remote Manager devices are listed below.

- **Phone Number:** The phone number of the current cellular connection.
- **ICCID:** The number used to identify the SIM card used by the device.

Remote Manager device details

MAC: 0027042952B5
Name: Device Remote Manager 5400 RM 0027042952B5

Reports + Actions + Connectors + SMC + Pages

Remote Manager 5400 RM

Device Details

Configuration

Settings

Configuration Details

Networks

Location

Connectors

Organization

Site ID

Configuration

MAC Address

Serial

Status

Model

Version of A&B&E

Firmware

Firmware Version

Firmware Identifier

Activated At

Last Modified

Last Disarm

Data Plan

0001

Default

800-704-2952 (Cont.) Sep 06 2016 15:00:00 (GMT)

0027042952B5

S4000-000000000000

Device is up

S4000-000

10.0.0.0/24

Firmware not found

10.0.0.0/24

10.0.0.0/24

Sep 06 2016 15:00:00 (GMT)

Sep 06 2016 15:00:00 (GMT)

Sep 02 2016 15:00:00 (GMT)

Not

The majority of details provided on the Remote Manager device details page are applicable to all categories of devices. See [Device details page](#) for details on those table entries.

The device details specific to Remote Manager devices are:

- **Management IP:** The IP address of the Remote Manager device's aView IPsec tunnel. If this IP does not match the aView tunnel IP address listed in the local web UI of the Remote Manager device, a user with the ability to modify devices will be given an option to edit the Management IP address.
- **Uplink IP Address:** The IP address of the current WAN network connection of the Remote

Manager device.

- **Primary Interface:** The currently used WAN connection interface.

Remote Manager Configuration tab

Remote Manager devices are configured through the aView site. See [Create a new Remote Manager device configuration profile](#) for details.

Remote Manager device Settings tab

The majority of details provided on the Remote Manager **Settings** tab are applicable to all categories of devices. See [Settings tab](#) for details on those table entries.

The device details specific to Remote Manager devices are:

- **Data Plan:** The data plan assigned to the device. If the user has the ability to change the data plan, a drop-down will be displayed and lists the available data plans for the organization the device belongs to. Once a data plan is associated with the device, any cellular data used by the device will be tracked in the data plan, which can be viewed and managed by clicking the **Edit** button for an Organization (see [Organizations](#)). You also have the option of creating a new data plan if desired.

Remote Manager Associated devices tab

This tab lists any devices that the Remote Manager device has associated with, indicating that they are connected to each other. The tab will include the following details about the associated device.

- **Device ID:** The identifying MAC address for the associated device.
- **Model:** If the associated device is a type of device supported by ARMT, this entry will display the type of device ARMT knows it as. If the device is not supported by ARMT, the category will be listed with a dash (-).
- **Interface:** The physical interface of the Remote Manager device the associated device is connected to.
- **Type:** How the associated device is connected to the Remote Manager device. For example, a type listed as LAN indicates that the associated device is connected to one of the Remote Manager device's LAN Ethernet ports.
- **IP Address:** The IP address of the associated device.
- **Connected:** Indicates when the device association was made and how long the associated device has been connected to the Remote Manager device.

Remote Manager Cellular Details tab

The **Cellular Details** tab lists details for the Remote Manager modem. The name of the cellular modem is listed in the title bar of the Cellular Details tab. If a Remote Manager device has multiple modems, there will be multiple modem panels, each one corresponding to one of the cellular device's modems. A modem entry can be removed by clicking the red trash icon at the top-right of the specific tab.

- **Carrier:** The cellular provider of the modem.
- **SKU:** The stock keeping unit of the modem.

- **Signal Strength:** The current RSSI signal strength value, measured in dBm, and percentage of the modem.
- **Signal Bars:** The current signal bars, based on the signal strength.
- **Speed Test:** The five most recent (if any) speed tests performed on the device. Speed tests are generated by sending a Speed Test command to the device.

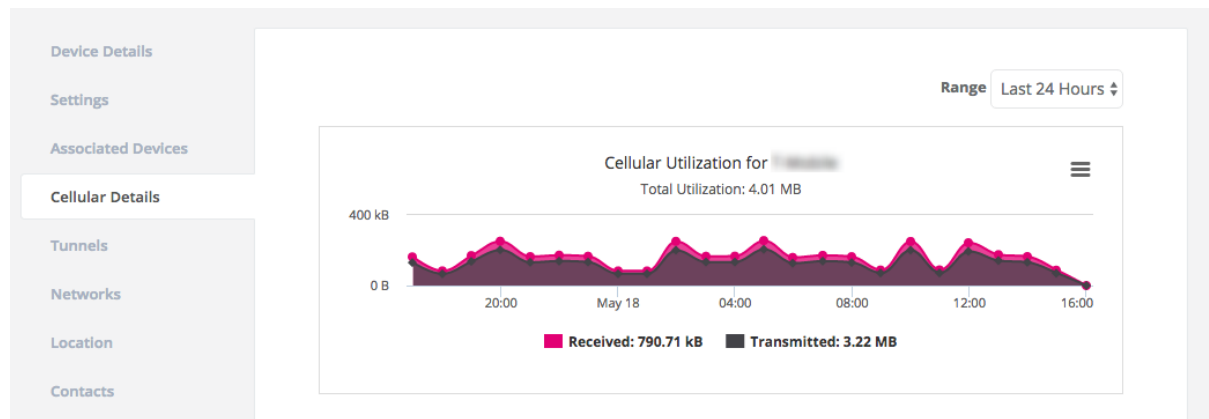
Note In order to minimize the speed test's impact on cellular data consumption, the results are an estimation of the available throughput of the device, and may not represent the full network speed available.

- **Phone Number:** The phone number of the modem.
- **RSSI:** The Received Signal Strength Indicator (RSSI) of the modem. RSSI provides information about total received wide-band power, including signal interference and thermal noise.
- **RSRP:** An LTE-specific value, representing the Reference Signal Received Power of the modem. RSRP is the average power of resource elements that carry cellular specific reference signals over the entire bandwidth.
- **RSRQ:** An LTE-specific value, representing the Reference Signal Receive Quality (RSRQ) of the modem. RSRQ is a combination of RSSI and RSRP and indicates the quality of the received reference signal.
- **SiNR:** The signal-to-interference-plus-noise ratio of the modem.
- **SNR:** The signal-to-noise ratio of the modem.
- **IMEI:** The IMEI value of the modem.
- **ESN:** The ESN value of the modem. Note that the ESN value only applies to CDMA cellular networks.
- **ICCID:** The ICCID value of the SIM card used by the modem.
- **IMSI:** The IMSI value of the modem.
- **Revision:** The hardware version of the modem.
- **APN:** The APN that the modem is currently connected with. Note that not all modems require an APN.
- **ECIO:** The signal-to-noise ratio of the modem. The lower the Ec/Io value, the greater the noise.
- **CNTI:** The technology type that the modem is currently connected to.
- **Band:** The frequency or type of cellular band the modem is currently connected to.
- **CID:** The CID identifier of the modem's current connection.
- **LAC:** The LAC identifier of the modem's current connection.
- **MCC:** The mobile country code of the modem's current connection.
- **MNC:** The mobile network code of the modem's current connection.
- **PLMN:** The PLMN ID of the modem's current connection, which is a combination of the MCC and MNC values.
- **USB Speed:** The speed of the USB port(s) on the Remote Manager device, measured in Mbps. 480 indicates USB 2.0 High Speed and 12 indicates USB 2.0 Full Speed.

Cellular utilization chart

If the device supports a cellular modem, a cellular utilization chart will be displayed. The chart shows the amount of cellular data used by the device. The initial timespan will display the data usage for the

past 24 hours. You can select different timespans from the Range drop-down.



Remote Manager Tunnels tab

The **Tunnel** tab lists status for any IPSec tunnels established by the Remote Manager device. Each row of the tab indicates a unique IPSec tunnel of the device.

- **Name:** The name of the IPSec tunnel, as specified in the configuration of the Remote Manager device.
- **Status:** Indicates whether or not the Remote Manager device has established the IPSec tunnel.
- **Last Updated:** The last time aView received an update concerning this tunnel.
- **IpLocal:** The tunnel IP address assigned to the Remote Manager device.
- **IpRemote:** The IP address of the server that the Remote Manager device built a tunnel to.
- **NetLocal:** The network settings on the Remote Manager device for the tunnel.
- **NetRemote:** The network settings on the server for the tunnel.

Remote Manager Network tab

The Network tab lists details for network interfaces that belong to the Remote Manager device. If a Remote Manager device has multiple networks, there will be multiple network tabs, each one corresponding to one of the device's networks.

- **Connection Type:** the type of network connection for the interface.
- **Metric:** The priority level of the network interface. The lower the number, the higher in priority the interface.
- **Priority:** Indicates if the network connection is the current primary or alternate connection.
- **IP Ranges:** The IP addressing for the network.
- **MTU:** The MTU size of the network interface.
- **Gateway IP:** The default route (gateway IP) of the network interface.
- **Bytes Received:** The total amount of data received, measured in bytes, on the network interface since the Remote Manager device has been online (resets on reboot).
- **Bytes Transmitted:** The total amount of data transmitted, measured in bytes, on the network interface since the Remote Manager device has been online (resets on reboot).

- **Ethernet Speed:** If the network type is an Ethernet interface, then this indicates the speed of the Ethernet port.
- **Ethernet Status:** If the network type is an Ethernet interface, then this indicates the status of the physical connection on the Ethernet port.

Remote Manager device remote commands

Remote commands are sent to a Remote Manager device through an IPSEC tunnel the device establishes to the Accelerated remote control server, or through the upstream IP address of the device if no tunnel IP is available. All Remote Manager devices by default establish an IPsec tunnel to remote.accns.com. See [aView tunnel alternatives](#) for information about additional IPsec tunnel endpoints.

The tunnel IP address for the Remote Manager device is stored in aView as the Management IP on the **Device Details** tab. If the Management IP is not known, then aView will use the IP address listed in the **Uplink IP Address** field on the **Device Details** tab for sending remote commands.

When you send a remote command to a device, aView utilizes a DNS service running on the remote control server to verify what tunnel IP address is associated with the device. If the DNS service responds with a valid IP address, aView will send the remote command to that IP address, otherwise it will use the known Management IP or the Uplink IP Address if the Management IP is unknown. If the IP address returned by the DNS service differs than the Management IP listed for the device, aView will update the Management IP after successfully sending the remote command to the device.

Before sending the remote command to the Remote Manager device, aView will prompt the user to provide the device-level username and password to authenticate with the device. If you do not know the username or password for the device, navigate to the **Configuration** tab of the device in aView and select **Authentication > Users**. Select a user name to change the password. You can also change the password locally on the device by following the instructions in the device's user manual. For example, to view instructions for the EX15, visit

<https://www.digi.com/resources/documentation/digidocs/90002344/default.htm#os/user-local-change-pswd-t.htm>.

Once the username and password are provided for the device, aView will then perform a HTTP request to the device to validate that the correct device is at the given IP address. If the correct device is reached and authenticated, the remote command will be sent.

The available remote commands that can be sent to Remote Manager devices are:

- **Check status:** The Remote Manager device will immediately send its current status.
- **Check signal strength:** The Remote Manager device will send its signal strength and network info once every 10 seconds for the next 15 minutes.
- **Perform Speed Test:** The Remote Manager device will perform a speed test and send the Upload/Download results.

Note In order to minimize the speed test's impact on cellular data consumption, the results are an estimation of the available throughput of the device, and may not represent the full network speed available.

- **ARPing Attached Device:** The Remote Manager device will attempt to ARPing the client device attached to its Ethernet port.
- **Send Wake-on-LAN to Attached Device:** The Remote Manager device will send a wake-on-LAN packet to the client device attached to its Ethernet port.

- **Check Configuration:** The Remote Manager device will immediately pull its configuration and reboot to apply any new settings.
- **Update Modem Firmware:** The Remote Manager device will query the Digi firmware server. If a new version of firmware is found for the active firmware used on the embedded modem in the Remote Manager device, it will download the new firmware and update the embedded modem. Note the Remote Manager device must be running firmware version 17.8.128 or higher to process this command.
- **Reboot:** Reboot the Remote Manager device.

Remote Manager device emergency SMS commands

As an alternative to the Remote commands, you can also send commands via SMS messaging to a Remote Manager device. The SIM card used by the Remote Manager device must have SMS enabled, or you will not be able to send SMS commands.

The available SMS commands that can be sent are:

- **Set Configuration:** A pop-up window appears where a user can enter in a configuration option or set of options to apply to the Remote Manager device. Multiple config options must be separated by a comma. For example, if a user wants to set the APN of a Remote Manager device to managedvpn, they would enter "modem_apn=managedvpn".
- **Configuration Reset:** Restore default configuration on the Remote Manager device and reboot.
- **Firmware Reset:** Restore to the backup firmware image on the Remote Manager device, and reboot.
- **Factory Reset:** Restore default configuration on the Remote Manager device, restore to the backup firmware image, and reboot.
- **Remote Control:** Tell the Remote Manager device to bring up its remote control tunnel (useful if on low data plan, so the remote control tunnel is not always up using data).
- **Reboot:** Reboot the Remote Manager device.

Remote Manager configuration requirements for aView

In order for the aView site to monitor a Remote Manager device, it must send its syslogs to the aView syslog server IP address, the domain of which is logs.accns.com.

For a Remote Manager device to get its configuration from the aView site, it must be set to pull its configuration from the aView configuration server configuration.accns.com. The device must also be able to sync its date and time with an NTP server; the default is time.accns.com.

In the device configuration, ensure the following options are set in **Service > Web administration**:

- **Enable** is selected.
- **Port** is set to **443**.
- **Access control list** -> **Zones** includes the **IPSec** zone.

This zone is included by default, but it's mentioned here for the user to verify that it is still present, in case the device is running settings that deviate from the default configuration.

The screenshot shows the 'Services' configuration page. Under 'Web administration', the 'Enable' checkbox is checked, and the 'Port' is set to 443. Below this, the 'Access control list' section is expanded, showing a list of zones. The 'IPsec' zone is highlighted with a red box.

View Remote Manager configuration profiles

To view the current list of group configuration profiles a user has access to:

1. Click on the **Configurations** button in the navigation panel.
2. Select **Remote Manager** in the drop-down.

The screenshot shows the 'Device Configurations' table. The table has columns for Name, Organization, Primary, Role, Configuration Schema, Schema Version, Version, and Created By. The table lists several configurations for Remote Manager, including 'Remote Manager', 'Remote Manager', 'Remote Manager', 'Remote Manager', and 'Remote Manager'.

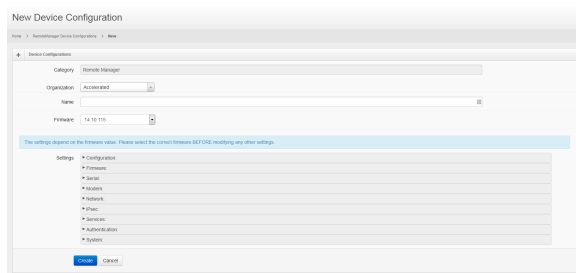
Name	Organization	Primary	Role	Configuration Schema	Schema Version	Version	Created By
Remote Manager	Accnetel	Remote Manager	1000-000	1000-000	1	Aug 28 2014 11:21:27 (GMT)	web_presentation@accnetel.com
Remote Manager	Accnetel	Remote Manager	1000-000	1000-000	1	Aug 28 2014 11:21:27 (GMT)	
Remote Manager	Accnetel	Remote Manager	1000-000	1000-000	1	Aug 28 2014 11:21:27 (GMT)	
Remote Manager	Accnetel	Remote Manager	1000-000	1000-000	1	Aug 28 2014 11:21:27 (GMT)	
Remote Manager	Accnetel	Remote Manager	1000-000	1000-000	1	Aug 28 2014 11:21:27 (GMT)	

Create a new Remote Manager device configuration profile

To create a new group configuration profile:

1. Click on the **Configurations** button in the navigation panel.
2. Select **Remote Manager** in the drop-down.
3. Click the **plus** icon located at the top right of the window.
4. Select the firmware version. The appropriate configuration schema will automatically load.
5. Set any desired settings in the presented configuration schema. Hovering your mouse over the name for a configuration option will display a pop-up providing help details about that option, including any default values. Once all the desired configuration options have been specified, click **Create**.

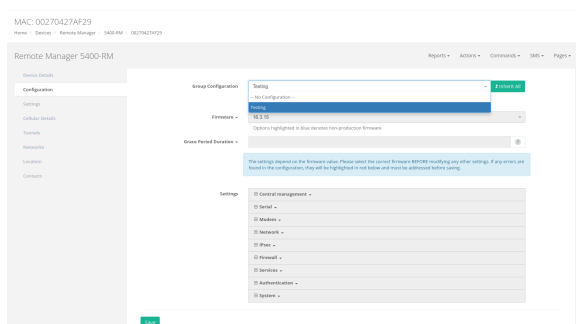
Note If the desired firmware is not listed, it must be uploaded onto the firmware management service, which is hosted at distro.accns.com.



Apply a Remote Manager configuration profile

To apply a group configuration profile to a Remote Manager device:

1. Go to the device details page for the specific device. This can be done by searching for the device's MAC address in the search bar, then clicking on the MAC address of the correct device in the results.
2. Once on the details page, click on the **Configuration** tab, select the new configuration profile from the **Group Configuration** drop-down, and click the **Save** button.



Individual device configuration settings

In addition to applying a group configuration profile to a device, authorized users will also have the option of setting configuration options to apply only to an individual device. These individual device configuration options are listed in the **Configuration** tab, below the **Group Configuration** option.

When a new group configuration is selected for a device, a list of inherited configuration settings from that group configuration profile will be displayed. Authorized users can then click on any setting and select the **Override** option to change the selected configuration option. It is important to note that any configuration option overridden in this way will only apply to that individual device. Any other devices that are linked to the same group configuration will only receive configuration settings from the group configuration profile, not any of the overridden settings from another individual device's configuration.

- **Inherit All:** This button can be used to reset an individual device's configuration back to the group configuration profile's settings. Any configuration options previously overridden in the individual device configuration will be undone and reset back to the settings inside the group configuration.

Delete a Remote Manager configuration profile

Configuration profiles can be deleted by clicking on the Delete icon for the appropriate profile on the Remote Manager **Configurations** page. A confirmation pop-up will ask the user to confirm that they wish to delete the configuration profile. If there are any devices linked to the configuration profile that is being deleted, the profile will not be deleted. The user must first unlink the configuration profile from the device and then they can remove the profile.

WiFi devices

- About WiFi devices 90
- WiFi device details 90
- Configuration 91
- WiFi configuration requirements for aView 91

About WiFi devices

WiFi devices refer to the Digi WiFi Extender line of products. Supported models are listed below. A user can find a list of all the WiFi devices they have access to by clicking on the Devices tab in the navigation bar, and then select the WiFi link from the drop-down.

■ 4200-NX

WiFi Devices

Home > Devices > WiFi

Filter WiFi Devices

WiFi Devices

Showing 1 to 3 of 3 entries

Icon	Host	Category	Model	Organization	Site	Powerline	Chip	Capacity	Last heartbeat (UTC)
WiFi	00C0CA49DA74	WiFi	4200-NX	Academichigher	Strong World	1.42334	WiFi	100	Dec 20 2015 10:00:00 (UTC)
WiFi	00C0CA49DA74	WiFi	4200-NX	Academichigher high organization	Stark Tower	1.42334	WiFi	100	Dec 20 2015 10:00:00 (UTC)
WiFi	00C0CA49DA74	WiFi	4200-NX	Academichigher	Stark Tower	1.42334	WiFi	100	Dec 20 2015 10:00:00 (UTC)

Showing 1 to 3 of 3 entries

WiFi device details

Device ID: 00C0CA49DA74

Home > Devices > WiFi > 4200-NX > 00C0CA49DA74

WiFi 4200-NX

Details > Reports > Actions > Pages

Details

Organization	Academichigher
Site ID	Strong World
WAN Address	00C0CA49DA74
Serial	00C0CA49DA74
Status	Online > up
Model	4200-NX
IP Address	
Powerline Version	1.42334
Activated At	Dec 20 2015 10:00:00 (UTC)
Last Heartbeat	Dec 20 2015 10:00:00 (UTC)
Last Report	Dec 20 2015 10:00:00 (UTC)

The majority of details provided on the WiFi device details page are applicable for all categories of devices. See [Device details page](#) for details on those table entries.

The device details specific to WiFi devices are:

- **IP Address:** The WAN IP address of the WiFi device.

Associated devices tab

This tab lists any devices that the WiFi device has associated with, indicating that they are connected to each other. The tab will include the following details about the associated device.

- **Device ID:** The identifying MAC address for the associated device.
- **Model:** If the associated device is a type of device supported by ARMT, this entry will display the type of device ARMT knows it as. If the device is not supported by ARMT, the category will be listed with a dash (-).
- **Interface:** The physical interface of the WiFi device the associated device is connected to.
- **Type:** How the associated device is connected to the WiFi device. For example, a type listed as WAN indicates that the associated device is connected to one of the WiFi device's WAN Ethernet ports.
- **IP Address:** The IP address of the associated device.
- **Connected:** Indicates when the device association was made and how long the associated device has been connected to the WiFi device.

Rogue access points tab

The WiFi device can be configured to search for other wireless Access Points (APs). Any of these nearby APs that also happen to be on the same LAN as the WiFi device will be flagged as a rogue AP. This tab lists any rogue APs discovered by the WiFi device. The following details are included about each rogue AP.

- **MAC:** The identifying MAC address of the rogue AP.
- **SSID:** The wireless SSID broadcasted by the rogue AP.
- **IP:** The IP address of the rogue AP.

Configuration

WiFi devices are configured through the AT&T Service Manager.

WiFi configuration requirements for aView

In order for the aView site to monitor a WiFi device, it must send its syslogs to the aView syslog server IP address, the domain of which is logs.accns.com

uCPE devices

- About uCPE devices 93
- uCPE device details 93
- uCPE device remote commands 96
- uCPE configuration requirements for aView 98

About uCPE devices

uCPE devices refer to the Digi uCPE line of products. Supported models are listed below. A user can find a list of all the uCPE devices they have access to by clicking on the **Devices** tab in the navigation bar, and then select the uCPE link from the dropdown.

■ HERO 9400-UA

uCPE Devices

Filter uCPE Devices

Showing 1 to 21 of 21 entries

Model	Primary IP	Category	Model	Organization	Site	Processor	OS	Country	Last heartbeat (UTC)
HERO9400UA01	192.168.1.101	uCPE	HERO 9400	Single	Default	16.0.15			May 17 2016 15:32:00 (UTC)
HERO9400UA02	192.168.1.102	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 18 2016 15:32:00 (UTC)
HERO9400UA03	192.168.1.103	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA04	192.168.1.104	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA05	192.168.1.105	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA06	192.168.1.106	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA07	192.168.1.107	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA08	192.168.1.108	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA09	192.168.1.109	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA10	192.168.1.110	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA11	192.168.1.111	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA12	192.168.1.112	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA13	192.168.1.113	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA14	192.168.1.114	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA15	192.168.1.115	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA16	192.168.1.116	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA17	192.168.1.117	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA18	192.168.1.118	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA19	192.168.1.119	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA20	192.168.1.120	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)
HERO9400UA21	192.168.1.121	uCPE	HERO 9400	Assessment/Reference	HERO 9400	16.1.1.00			May 17 2016 15:32:00 (UTC)

Showing 1 to 21 of 21 entries

uCPE device details

MAC: 002704296011

Model: HERO 9400-UA

uCPE 9400-UA

Reports • Actions • Contracts • Pages

Device Details	Organization	Organization
Device ID	Default	
Configuration	uCPE Test - Last checked at Mar 17 2016 15:32:00 (UTC)	
MAC Address	002704296011	
Serial	HERO9400UA01	
Status	Ready to Deploy	
Model	HERO 9400	
Primary IP Address	192.168.1.101	
Primary Interface	eth0	
Activated At	Mar 17 2016 15:32:00 (UTC)	
Last heartbeat	Aug 17 2016 15:32:00 (UTC)	
Last Report	Aug 17 2016 15:32:00 (UTC)	
Data Plan	N/A	

The majority of details provided on the uCPE device details page are applicable to all categories of devices. For details on those table entries, refer to the Devices section of this guide. The device details specific to uCPE devices are listed below.

- **Management IP:** The IP address of the uCPE device's aView IPsec tunnel. If this IP does not match the aView tunnel IP address listed in the local web UI of the uCPE device, a user with the ability to modify devices will be given an option to edit the Management IP address.
- **Uplink IP Address:** The IP address of the current WAN network connection of the uCPE device.
- **Primary Interface:** The currently used WAN connection interface.

Configuration tab

uCPE devices are configured through the aView site. See [Create a new uCPE device configuration profile](#) for details.

uCPE device Settings tab

The majority of details provided on the uCPE **Settings** tab are applicable to all categories of devices. See [Settings tab](#) for details on those table entries.

The device details specific to uCPE devices are:

- **Data Plan:** The data plan assigned to the device. If the user has the ability to change the data plan, a drop-down will be displayed and lists the available data plans for the organization the device belongs to. Once a data plan is associated with the device, any cellular data used by the device will be tracked in the data plan, which can be viewed and managed by clicking the **Edit** button for an Organization (see [Organizations](#)). You also have the option of creating a new data plan if desired.

Associated devices

This tab lists any devices that the uCPE device has associated with, indicating that they are connected to each other. The tab will include the following details about the associated device.

- **Device ID:** The identifying MAC address for the associated device.
- **Model:** If the associated device is a type of device supported by ARMT, this entry will display the type of device ARMT knows it as. If the device is not supported by ARMT, the category will be listed with a dash (-).
- **Interface:** The physical interface of the uCPE device the associated device is connected to.
- **Type:** How the associated device is connected to the uCPE device. For example, a type listed as LAN indicates that the associated device is connected to one of the uCPE device's LAN Ethernet ports.
- **IP Address:** The IP address of the associated device.
- **Connected:** Indicates when the device association was made and how long the associated device has been connected to the uCPE device.

uCPE device Cellular Details tab

The **Cellular Details** tab lists details for the uCPE modem. The name of the cellular modem is listed in the title bar of the **Cellular Details** tab. If a uCPE device has multiple modems, there will be multiple modem panels, each one corresponding to one of the uCPE device's modems. A modem entry can be removed by clicking the red trash icon at the top-right of the specific tab.

- **Carrier:** The cellular provider of the modem.
- **SKU:** The stock keeping unit of the modem.
- **Signal Strength:** The current RSSI signal strength value, measured in dBm, and percentage of the modem.
- **Signal Bars:** The current signal bars, based on the signal strength.
- **Speed Test:** The five most recent (if any) speed tests performed on the device. Speed tests are generated by sending a Speed Test command to the device.

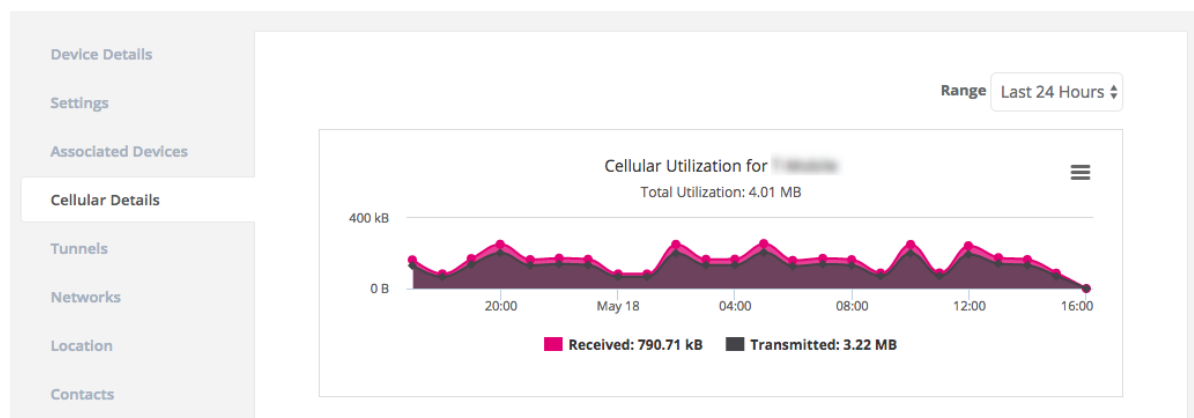
Note In order to minimize the speed test's impact on cellular data consumption, the results are an estimation of the available throughput of the device, and may not represent the full network speed available.

- **Phone Number:** The phone number of the modem.
- **RSSI:** The Received Signal Strength Indicator (RSSI) of the modem. RSSI provides information about total received wide-band power, including signal interference and thermal noise.

- **RSRP:** An LTE-specific value, representing the Reference Signal Received Power of the modem. RSRP is the average power of resource elements that carry cellular specific reference signals over the entire bandwidth.
- **RSRQ:** An LTE-specific value, representing the Reference Signal Receive Quality (RSRQ) of the modem. RSRQ is a combination of RSSI and RSRP and indicates the quality of the received reference signal.
- **SiNR:** The signal-to-interference-plus-noise ratio of the modem.
- **SNR:** The signal-to-noise ratio of the modem.
- **IMEI:** The IMEI value of the modem.
- **ESN:** The ESN value of the modem. Note that the ESN value only applies to CDMA cellular networks.
- **ICCID:** The ICCID value of the SIM card used by the modem.
- **IMSI:** The IMSI value of the modem.
- **Revision:** The hardware version of the modem.
- **APN:** The APN that the modem is currently connected with. Note that not all modems require an APN.
- **ECIO:** The signal-to-noise ratio of the modem. The lower the E_c/I_o value, the greater the noise.
- **CNTI:** The technology type that the modem is currently connected to.
- **Band:** The frequency or type of cellular band the modem is currently connected to.
- **CID:** The CID identifier of the modem's current connection.
- **LAC:** The LAC identifier of the modem's current connection.
- **MCC:** The mobile country code of the modem's current connection.
- **MNC:** The mobile network code of the modem's current connection.
- **PLMN:** The PLMN ID of the modem's current connection, which is a combination of the MCC and MNC values.
- **USB Speed:** The speed of the USB port(s) on the uCPE device, measured in Mbps. 480 indicates USB 2.0 High Speed and 12 indicates USB 2.0 Full Speed.

Cellular utilization chart

If the device supports a cellular modem, a cellular utilization chart will be displayed. The chart shows the amount of cellular data used by the device. The initial timespan will display the data usage for the past 24 hours. You can select different timespans from the Range drop-down.



uCPE device Tunnels tab

The **Tunnels** tab lists status for any IPsec tunnels established by the uCPE device. Each row of the tab indicates a unique IPsec tunnel of the device.

- **Name:** The name of the IPsec tunnel, as specified in the configuration of the uCPE device.
- **Status:** Indicates whether or not the uCPE device has established the IPsec tunnel.
- **IpLocal:** The tunnel IP address assigned to the uCPE device.
- **IpRemote:** The IP address of the server that the uCPE device built a tunnel to.
- **NetLocal:** The network settings on the uCPE device for the tunnel.
- **NetRemote:** The network settings on the server for the tunnel.

uCPE device Network tab

The **Network** tab lists details for network interfaces that belong to the uCPE device. If a uCPE device has multiple networks, there will be multiple network tabs, each one corresponding to one of the device's networks.

- **Connection Type:** the type of network connection for the interface.
- **Metric:** The priority level of the network interface. The lower the number, the higher in priority the interface.
- **Priority:** Indicates if the network connection is the current primary or alternate connection.
- **IP Ranges:** The IP addressing for the network.
- **MTU:** The MTU size of the network interface.
- **Gateway IP:** The default route (gateway IP) of the network interface.
- **Bytes Received:** The total amount of data received, measured in bytes, on the network interface since the uCPE device has been online (resets on reboot).
- **Bytes Transmitted:** The total amount of data transmitted, measured in bytes, on the network interface since the uCPE device has been online (resets on reboot).
- **Ethernet Speed:** If the network type is an Ethernet interface, then this indicates the speed of the Ethernet port.
- **Ethernet Status:** If the network type is an Ethernet interface, then this indicates the status of the physical connection on the Ethernet port.

uCPE device remote commands

Remote commands are sent to a uCPE device through an IPSEC tunnel the device establishes to the Accelerated remote control server, or through the upstream IP address of the device if no tunnel IP is available. All uCPE devices by default establish an IPsec tunnel to remote.accns.com. See [aView tunnel alternatives](#) for information about additional IPsec tunnel endpoints.

The tunnel IP address for the uCPE device is stored in aView as the Management IP on the **Device Details** tab. If the Management IP is not known, then aView will use the IP address listed in the **Uplink IP Address** field on the **Device Details** tab for sending remote commands.

When you send a remote command to a device, aView utilizes a DNS service running on the remote control server to verify what tunnel IP address is associated with the device. If the DNS service responds with a valid IP address, aView will send the remote command to that IP address, otherwise it will use the known Management IP or the Uplink IP Address if the Management IP is unknown. If the

IP address returned by the DNS service differs than the Management IP listed for the device, aView will update the Management IP after successfully sending the remote command to the device.

Before sending the remote command to the uCPE device, aView will prompt the user to provide the device-level username and password to authenticate with the device. If you do not know the username or password for the device, navigate to the **Configuration** tab of the device in aView and select **Authentication > Users**. Select a user name to change the password. You can also change the password locally on the device by following the instructions in the device's user manual. For example, to view instructions for the EX15, visit <https://www.digi.com/resources/documentation/digidocs/90002344/default.htm#os/user-local-change-pswd-t.htm>.

Once the username and password are provided for the device, aView will then perform a HTTP request to the device to validate that the correct device is at the given IP address. If the correct device is reached and authenticated, the remote command will be sent.

The available remote commands that can be sent to uCPE devices are:

- **Check status:** The uCPE device will immediately send its current status.
- **Check signal strength:** The uCPE device will send its signal strength and network info once every 10 seconds for the next 15 minutes.
- **Perform Speed Test:** The uCPE device will perform a speed test and send the Upload/Download results.

Note In order to minimize the speed test's impact on cellular data consumption, the results are an estimation of the available throughput of the device, and may not represent the full network speed available.

- **ARPing Attached Device:** The uCPE device will attempt to ARPing the client device attached to its Ethernet port.
- **Send Wake-on-LAN to Attached Device:** The uCPE device will send a wake-on-LAN packet to the client device attached to its Ethernet port.
- **Check Configuration:** The uCPE device will immediately pull its configuration and reboot to apply any new settings.
- **Update Modem Firmware:** The uCPE device will query the Digi firmware server. If a new version of firmware is found for the active firmware used on the embedded modem in the uCPE device, it will download the new firmware and update the embedded modem. Note the uCPE device must be running firmware version 17.8.128 or higher to process this command.
- **Reboot:** Reboot the uCPE device.

uCPE device emergency SMS commands

As an alternative to the Remote commands, you can also send commands via SMS messaging to a uCPE device. The SIM card used by the uCPE device must have SMS enabled, or you will not be able to send SMS commands.

The available SMS commands that can be sent are:

- **Set Configuration:** A pop-up window appears where a user can enter in a configuration option or set of options to apply to the uCPE device. Multiple config options must be separated by a comma. For example, if a user wants to set the APN of a uCPE device to managedvpn, they would enter "modem_apn=managedvpn".
- **Configuration Reset:** Restore default configuration on the uCPE device and reboot.

- **Firmware Reset:** Restore to the backup firmware image on the uCPE device, and reboot.
- **Factory Reset:** Restore default configuration on the uCPE device, restore to the backup firmware image, and reboot.
- **Remote Control:** Tell the uCPE device to bring up its remote control tunnel (useful if on low data plan, so the remote control tunnel is not always up using data).
- **Reboot:** Reboot the uCPE device.

uCPE configuration requirements for aView

In order for the aView site to monitor a uCPE device, it must send its syslogs to the aView syslog server IP address, the domain of which is logs.accns.com.

For a uCPE device to get its configuration from the aView site, it must be set to pull its configuration from the aView configuration server configuration.accns.com. The device must also be able to sync its date and time with an NTP server; the default is time.accns.com.

In the device configuration, ensure the following options are set in **Service > Web administration**:

- **Enable** is selected.
- **Port** is set to **443**.
- **Access control list -> Zones** includes the **IPSec** zone.

This zone is included by default, but it's mentioned here for the user to verify that it is still present, in case the device is running settings that deviate from the default configuration.

The screenshot shows the configuration interface for a uCPE device. The 'Services' section is expanded, and 'Web administration' is selected. The 'Enable' checkbox is checked, and the 'Port' is set to 443. The 'Access control list' section is also expanded, showing a list of zones. The 'IPsec' zone is highlighted in the list.

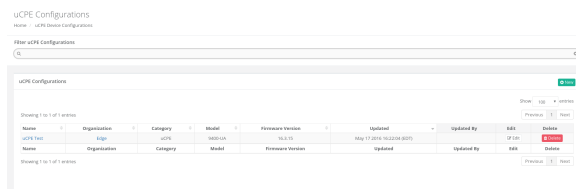
Web administration		
Enable	☒	
Port	443	

Access control list		
IPv4 Addresses		
IPv6 Addresses		
Interfaces		
Zones		
1.	Zone	Internal
2.	Zone	IPsec
3.	Zone	Setup

View list of uCPE configuration profiles

To view the current list of group configuration profiles a user has access to:

1. Click on the **Configurations** button in the navigation panel.
2. Select **uCPE** in the drop-down.

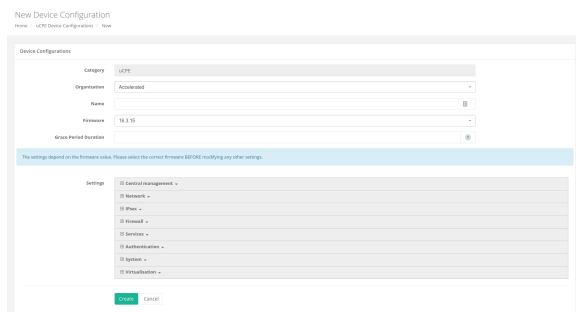


Create a new uCPE device configuration profile

To create a new group configuration profile:

1. Click on the **Configurations** button in the navigation panel.
2. Select **uCPE** in the drop-down.
3. Click the **plus** icon located at the top right of the window.
4. Select the firmware version. The appropriate configuration schema will automatically load.
5. Set any desired settings in the presented configuration schema. Hovering your mouse over the name for a configuration option will display a pop-up providing help details about that option, including any default values. Once all the desired configuration options have been specified, click **Create**.

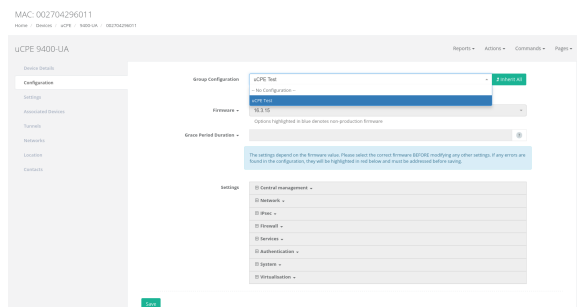
Note If the desired firmware is not listed, it must be uploaded onto the firmware management service, which is hosted at distro.accns.com.



Apply a uCPE configuration profile

To apply a group configuration profile to a uCPE device:

1. Go to the device details page for the specific device. This can be done by searching for the device's MAC address in the search bar, then clicking on the MAC address of the correct device in the results.
2. Once on the details page, click on the **Configuration** tab, select the new configuration profile from the Group Configuration drop-down, and click the **Save** button.



Individual uCPE device configuration settings

In addition to applying a group configuration profile to a device, authorized users will also have the option of setting configuration options to apply only to an individual device. These individual device configuration options are listed in the Configuration tab, below the Group Configuration option.

When a new group configuration is selected for a device, a list of inherited configuration settings from that group configuration profile will be displayed. Authorized users can then click on any setting and select the Override option to change the selected configuration option. It is important to note that any configuration option overridden in this way will only apply to that individual device. Any other devices that are linked to the same group configuration will only receive configuration settings from the group configuration profile, not any of the overridden settings from another individual device's configuration.

- **Inherit All:** This button can be used to reset an individual device's configuration back to the group configuration profile's settings. Any configuration options previously overridden in the individual device configuration will be undone and reset back to the settings inside the group configuration.

Delete a uPCE configuration profile

Configuration profiles can be deleted by clicking on the X delete icon for the appropriate profile on the uCPE **Configurations** page. A confirmation pop-up will ask the user to confirm that they wish to delete the configuration profile. If there are any devices linked to the configuration profile that is being deleted, the profile will not be deleted. The user must first unlink the configuration profile from the device and then they can remove the profile.

Adding devices to aView

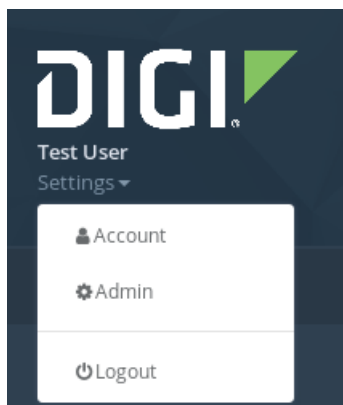
Add a gateway device	102
Add devices	102

Add a gateway device

Gateway devices are added, configured, and deleted from the AT&T Service Manager. The aView tool receives a daily update from the Service Manager with a list of gateway devices. This list is then synced with the list of gateway devices currently in aView. If any new devices are found in the Service Manager file, they are added in aView, and if the Service Manager configuration settings are imported. If a device is not found in the the Service Manager file, but it exists in aView, then that device is removed from aView.

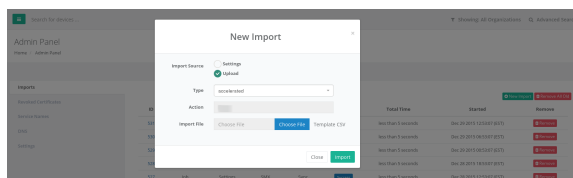
Add devices

Any non-Gateway device can be added by aView site administrators, as long as it is a recognized device type (cellular, WiFi, etc.). The user should contact their aView site administrator if they do not have permission to add devices. To add devices to the aView site, use the admin device importer, found by clicking the Admin button in the top navigation bar.



Next click on the green **New Import** button. If a device import is already running, this button will not be available and the user must wait for the current import to finish. Refresh the **Admin** page to check on the status of the running import.

In the **New Import** dialog, ensure that the following options are selected.



The file that is uploaded must contain details for the new devices in a specific format. Download the file template by clicking the Template CSV link.

Note Keep the first line of the CSV file exactly as is. These column headers are required for the device importer to work properly. If the column headers are deleted, then the devices will not be imported.

Enter in the device details that are listed in the template CSV file. Note that a MAC address, a serial number, and an organization must be specified in order to add a new device. The other fields are optional.

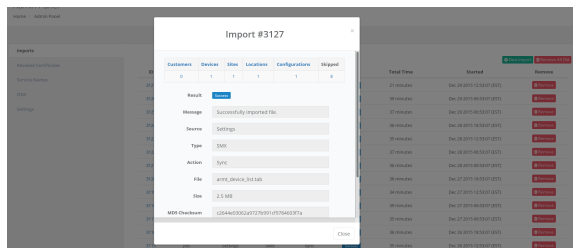
If you are specifying a value in the config_name column of the CSV file for a device, that value must correspond to an existing configuration profile for that category of devices in aView, and the configuration profile must be in the same organization as the device. If no config_name is specified, then one of the two actions will be taken:

- If the organization specified for the device in the import file is the same organization that the device is currently assigned to, then the import will not change or remove the configuration profile currently assigned to the device.
- If the organization specified for the device in the import file is different than the organization that the device is currently assigned to, the device will be moved to the new organization, and the old configuration profile previously assigned to the device will be disassociated from the device, as the old configuration profile belongs to the old organization.

See the Configuration sections for each type of device in this guide for more details about setting up configuration profiles.

Note Configurations cannot be specified in the CSV file for Gateway or WiFi devices. Those devices' configuration profiles are setup in the AT&T Service Manager.

Once the CSV file is created and selected, click the green Import button to add the devices. Once the import is complete (refresh the Admin page to check its status), the user can review the import results by clicking on the import ID.



Generating reports

Availability report	105
Cellular network type report	106
Cellular signal strength report	107
VIG report	108

Availability report

The Availability Report creates an ad hoc report on device availability, including detailed uptime data and graphs. Availability reports are based on the events that are sent in by the devices into aView. The downtime percentage is calculated by adding up the time when the device was reported as down (red status) or unreachable (gray status) and subtracting the result from the total time. The uptime percentage is calculated by subtracting the downtime percentage from 100%.

Create an availability report

To create a new availability report:

1. Click on the **Availability** link in the **Reports** drop-down menu of the navigation bar.

New Report

HomeReportsAvailability

Availability Filter

Organization

Accountant

Include Sub Organizations

Entity Categories

All

Entity Models

All

Deployment

All

Order By

Last Activity

In Descending Order

Time Span

Last Day

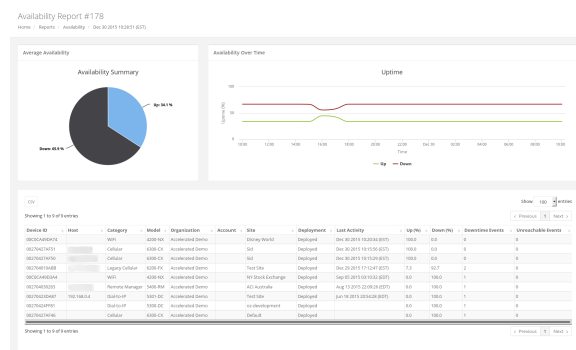
Submit

Cancel

2. From the report form, select the desired criteria for the report:

- **Organization:** The organization that the devices are associated with. The user can also specify whether or not to include devices that belong to sub-organizations of the selected organization by clicking the hierarchy icon button next to the Organization drop-down.
- **Device Categories:** The categories of devices to run the report on. Multiple device categories and/or models can be selected together.
- **Device Models:** The models of devices to run the report on. Multiple device categories and/or models can be selected together.
- **Deployment:** Select to run the report on all devices, deployed-only, or undeployed-only. See [Monitoring devices](#) for a description for deployed versus undeployed.
- **Order by:** Select the parameter that is used to order and list the results of the report.
- **Time span:** The time frame for what events are used to generate the report.

3. Once all the desired options are specified, click **Create** to generate the availability report. The resulting availability report can be exported to a CSV file by clicking the **CSV** button in the report.



Depending on the number of devices and the time span of the report, it may take several minutes for the report to complete. The report generation process is done in the background. You can navigate away from this page without interrupting or stopping the process. You can check on the report process by going to the report **History** page and clicking on the appropriate report ID.

Cellular network type report

The Cellular Network Type Report creates an ad hoc report on cellular network type and the time duration devices spent on a given network. Cellular network type reports are based on the events that are sent in by the devices into aView.

Create a cellular network type report

To create a new cellular network type report:

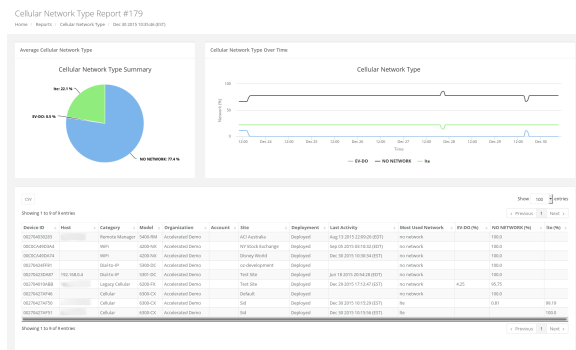
1. Click on the **Cellular Network Type** link in the Reports drop-down menu of the navigation bar.

The screenshot shows the 'New Report' form for 'Cellular Network Type'. The form has the following fields and options:

- Organization:** A dropdown menu with 'AcmeCo' selected. Below it is a checkbox labeled 'Include Sub-Organizations'.
- Device Models:** A dropdown menu with 'All' selected.
- Deployment:** A dropdown menu with 'All' selected.
- Order By:** A dropdown menu with 'Last Activity' selected.
- Time Span:** A dropdown menu with 'Last Day' selected.
- Buttons:** 'Create' (green) and 'Cancel' (grey) buttons at the bottom.

2. From the report form, select the desired criteria for the report.
 - **Organization:** The organization that the devices are associated with. The user can also specify whether or not to include devices that belong to sub-organizations of the selected organization by clicking the hierarchy icon button next to the Organization drop-down.
 - **Device Categories:** The categories of devices to run the report on. Multiple device categories and/or models can be selected together.
 - **Device Models:** The models of devices to run the report on. Multiple device categories and/or models can be selected together.
 - **Deployment:** Select to run the report on all devices, deployed-only, or undeployed-only. See [Monitoring devices](#) for a description for deployed versus undeployed.
 - **Order by:** Select the parameter that is used to order and list the results of the report.
 - **Time span:** The time frame for what events are used to generate the report.
3. Once all the desired options are specified, click **Create** to generate the cellular network type report. The resulting cellular network type report can be exported to a CSV file by clicking the CSV button in the report.

Depending on the number of devices and the time span of the report, it may take several minutes for the report to complete. The report generation process is done in the background. You can navigate away from this page without interrupting or stopping the process. You can check on the report process by going to the report **History** page and then clicking on the appropriate report ID.



Cellular signal strength report

The Cellular Signal Strength Report creates an ad hoc report on cellular signal strength. Cellular signal strength reports are based on the events that are sent in by the devices into aView. The average dBm and percentage listed for each device in table represents the the average signal strength for the selected time span of the report. The average dBm and percentage listed while hovering over the map represents the average signal strength for all devices included in the report at the selected time.

Create a cellular signal strength report

To create a new cellular signal strength report:

1. Click on the **Cellular Signal Strength** link in the Reports drop-down menu of the navigation bar.

New Report

Report: Reports > Cellular Signal Strength

Cellular Signal Strength form:

Organization: Acme Corp

Device Models: All

Deployment: All

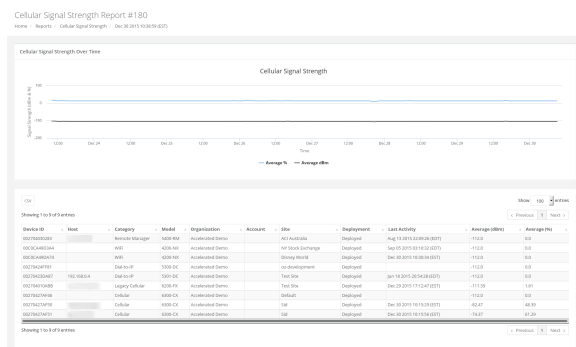
Order By: Last Activity

Time Span: Last Day

Buttons: Create, Cancel

2. From the report form, select the desired criteria for the report.
 - **Organization:** The organization that the devices are associated with. The user can also specify whether or not to include devices that belong to sub-organizations of the selected organization by clicking the hierarchy icon button next to the Organization drop-down.
 - **Device Categories:** The categories of devices to run the report on. Multiple device categories and/or models can be selected together.
 - **Device Models:** The models of devices to run the report on. Multiple device categories and/or models can be selected together.
 - **Deployment:** Select to run the report on all devices, deployed-only, or undeployed-only. See [Monitoring devices](#) for a description for deployed versus undeployed.
 - **Order by:** Select the parameter that is used to order and list the results of the report.
 - **Time span:** The time frame for what events are used to generate the report.

- Once all the desired options are specified, click **Create** to generate the cellular signal strength report. The resulting cellular signal strength report can be exported to a CSV file by clicking the **CSV** button in the report.



Depending on the number of devices and the time span of the report, it may take several minutes for the report to complete. The report generation process is done in the background. You can navigate away from this page without interrupting or stopping the process. You can check on the report process by going to the report History page and then clicking on the appropriate report ID.

VIG report

The VIG Report creates an ad hoc report of a list of VPN Gateway units and what VIGs they are associated with (if any). VIG reports are based on the events that are sent in by the VPN Gateway devices into aView.

Create a VIG report

To create a new VIG report:

1. Click on the **VIG Report** link in the Reports drop-down menu of the navigation bar.

New Report

Home / Reports / Vig

Vig Form

Organization

☐ Include Sub-Organizations

Deployment

Order By

[Create](#) [Cancel](#)

- From the report form, select the desired criteria for the report:
 - Organization:** The organization that the devices are associated with. The user can also specify whether or not to include devices that belong to sub-organizations of the selected organization by clicking the hierarchy icon button next to the Organization drop-down.
 - Deployment Status:** Select to run the report on all devices, deployed-only, or undeployed-only. See [Monitoring devices](#) for a description for deployed versus undeployed.
 - Order by:** Select the parameter that is used to order and list the results of the report.

3. Once all the desired options are specified, click **Create** to generate the VIG report. The resulting VIG report can be exported to a CSV file by clicking the CSV button in the report.

Depending on the number of devices and the time span of the report, it may take several minutes for the report to complete. The report generation process is done in the background. You can navigate away from this page without interrupting or stopping the process. You can check on the report process by going to the report History page and then clicking on the appropriate report ID.

The resulting VIG report can be exported to a CSV file by clicking the **Download CSV** button in the report.

Vig Report #101000

View

Refresh

[View All](#)
[View by Category](#)
[View by Status](#)
[View by Date Range](#)

Invoice #	Date	Category	Model	Description	Amount	Qty	Description	Exp. date	Exp. #	View More	View Details
00000000000000000000	1/28/21 01:15	Category	0100	AWP/ATA	ATA		Software				
00000000000000000000	1/28/21 01:15	Category	0100	AWP/ATA	ATA		AWP TEST LOG				
00000000000000000000	1/28/21 01:11	Category	0100	AWP/ATA	ATA		NEW SCHEDULE AWP TEST LOG				
00000000000000000000	1/28/21 01:09	Category	0100	AWP/ATA	ATA		NEW 1 PROGR AWP				
00000000000000000000	1/28/21 01:10	Category	0100	AWP/ATA	ATA		AWP TEST LOG				
00000000000000000000	1/28/21 01:09	Category	0100	AWP/ATA	ATA		AWP/ATA WARNING TALS				
00000000000000000000	1/28/21 01:14	Category	0100	AWP/ATA	ATA		AWP/ATA WARNING EXTENDERS				
00000000000000000000	1/28/21 01:08	Category	0100	AWP/ATA	ATA		AWP/ATA WARNING TALS				

Controlling device down status

About device down status in aView	111
Configure down status options for devices	111

About device down status in aView

You can configure when a device is considered down (red status) in aView. When a device goes into the down status, you can elect to receive a notification of the event. See [Notification profiles](#) for details on configuring a user's notification.

Only the following device categories have adjustable options. Other devices cannot be changed in this aspect.

- Cellular
- Dial-to-IP
- Remote Manager
- Legacy cellular

Configure down status options for devices

To configure when a device is considered down (red status) in aView:

- For Cellular, Dial-to-IP, Remote Manager, and uPCE devices, set the **Grace Period Duration** and/or **Heartbeat Interval** options in the device configuration profile.

New Device Configuration

Device Configuration

Category: Cellular

Organization: AccessNet

Name: [text field]

Address: 10.0.0.0

Grace Period Duration: [text field]

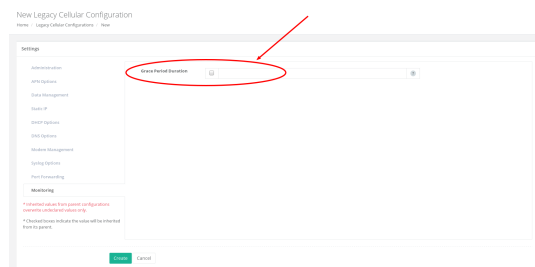
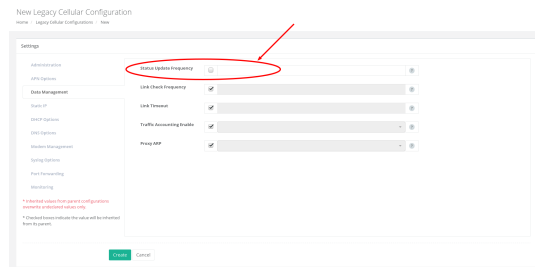
Settings:

- General management
- Network
- Network
- Device
- Services
- Advanced settings
- System

Heartbeat Interval: [text field]

Save Cancel

- For Legacy Cellular devices, set the **Status Update Frequency** and/or **Grace Period Duration** options in the device configuration profile.



Grace Period Interval option

The **Grace Period Interval** option controls how long in addition to the check-in time aView should wait before considering a device as Down. The default grace period is 109 minutes. When this is combined with the default **Heartbeat Interval** of 30 minutes, this means that by default aView considers a device as down if it has not heard from the device within 139 minutes, or 2 hours and 19 minutes.

Heartbeat Interval option

The **Heartbeat Interval** option (for Legacy Cellular devices, this is the **Status Update Frequency** option) controls how often a device checks in to aView. By default, devices send a status check-in to aView once every 30 minutes.

Examples: Adjusting device down status

If a user would like to show an Cellular device as down after 1 day of inactivity, they can do so by adjusting the **Heartbeat Interval** option (for Legacy Cellular devices, this is the **Status Update Frequency** option) and **Grace Period** accordingly. Below are several example settings that can be used to achieve this.

Option 1:

- **Grace Period:** 23h50m
- **Heartbeat Interval:** 10m

Option 2:

- **Grace Period:** 23h
- **Heartbeat Interval:** 1h

Option 3:

- **Grace Period:** 18h
- **Heartbeat Interval:** 6h

Configure down status for VPN gateway devices

VPN Gateway devices are monitored by Digi aView using SNMP probes.

Configuring when a Gateway device is considered down (red status) in Digi aView is done by adjusting the **Probe Interval** and **Missed Probes before Down** options in the **Organization** settings for the Gateway device. These settings will apply to all devices that belong to that organization.

The screenshot shows the 'SNMP Probes' configuration page in the Digi aView interface. On the left is a sidebar with navigation links: Information, Roles, Permissions, Device Settings, Data Plans, and SNMP Probes (which is highlighted). The main content area has a 'New User' button in the top right. Below it, there are two configuration sections. The first is 'Probe Interval', which has a red status icon and a slider set to 'Every 15 minutes'. The second is 'Missed Probes Before Down', also with a red status icon and a slider set to '2 missed probes for down status'. Below these sliders, a text box explains: 'With these settings, your device could be down for up to 30 minutes before reporting.' At the bottom of the configuration area is a green 'Save Changes' button.

Probe Interval

The **Probe Interval** option controls how often Digi aView sends an SNMP probe to the VPN Gateway. By default, Digi aView probes the VPN Gateway once every 15 minutes. Each probe pulls the most recent status details from the VPN Gateway and updates the details in Digi aView with the results.

Missed Probes Before Down

The **Missed Probes Before Down** option controls how many probes can be missed before Digi aView considers a device as **Down**. The default number of missed probes is two. When the **Missed Probes Before Down** (two) is combined with the default probe interval of 15 minutes, the amount of time at which Digi aView considers a Gateway device as down if it has not heard from the device is 30 minutes (2 times 15 minutes).

Note In addition to performing SNMP probes to the VPN Gateway, the VPN Gateway itself can send SNMP informs/traps to Digi aView. This can also affect when Digi aView considers the device as down. For Digi aView to consider the device as down, no SNMP probe responses, SNMP traps, or SNMP informs would have been received within the specified time window, as specified in these **SNMP Probe** settings (default 30 minutes).

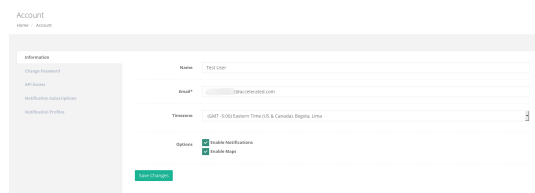
Manage User Preferences

The **Account** page allows you to modify your aView user information and subscribe to various device notifications.

To manage the account:

1. Click **Settings** at the top of the navigation panel.
2. Select **Account**.

The **Account** page displays.



The **Account** page allows you to modify the name associated with the account, along with the e-mail address for the account.

Note Any subscriptions in aView will send notification alerts to this email address.

This page also allows you to set the time zone so that all data is displayed in local time, and select whether to enable Notifications for the account and whether geographic Map displays should be made available.

Once all the desired information has been entered or changed, click **Save Changes** to save the information.

Changing your password

The **Change Password** panel of the **Account** page allows you to update your password, which is used to login to aView. You must enter your current password and a new password. All passwords must be at least 6 characters in length.

The password can be reset by clicking on the **Forgot your password** button of the **Login** page. See [Login page](#) for further information.

Managing Notifications

Notifications provide a convenient way of being alerted when a device or group of devices changes state. You can subscribe to notifications for an individual-device or for an organization. When you subscribes to a device or organization, a notification profile must be applied to the subscription. The

notification profile is where a user configures exactly what type of notifications they would like to receive from the device or organization.

1. Click **Settings** at the top of the navigation panel.
2. Select **Account**.

The **Account** page displays.

- To view the devices and/or organizations you are currently subscribed to, click **Notification Subscriptions**.
- To create a new notification profile or view existing notification profiles, click **Notification Profiles**.

Note If you subscribe to an individual device, and also subscribe to the organization that the device belongs to, you may receive two identical notifications from the device, depending on what notification profile is applied to each subscription.

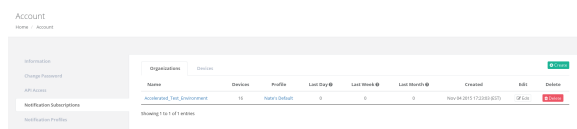
Notification subscriptions

To subscribe to an individual device, go to the device details page. This can be done by searching for the device's MAC address in the search bar, then clicking on the MAC address of the correct device in the results. Once on the details page, click on the **Subscribe** button listed in the **Actions** drop-down at the top right of the page.



To subscribe to an organization, click on the Organizations tab in the navigation panel. From there, click the Actions drop-down for the appropriate organization, and then click Subscribe.

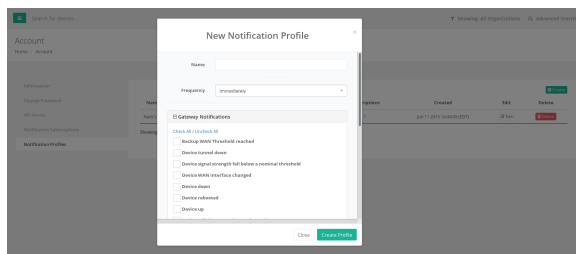
A user can manage their notification subscriptions by clicking the Account button at the top right of any page on the aView site. From there, click the Notification Subscriptions tab. This lists all the organizations that the user is subscribed to. To view the devices the user is subscribed to, select the Devices tab inside the notification subscriptions table.



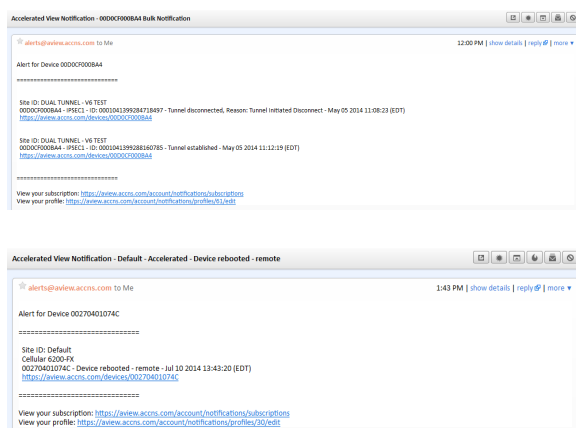
To delete a subscription (aka "unsubscribe"), click the Delete trash icon for the appropriate subscription. Users can also unsubscribe to a device or organization in the same manner that they subscribed to it.

Notification profiles

This tab in the user preferences displays the existing profiles for the user. You can create a new profile by clicking on the plus icon at the top-right of the list. This will bring up the new notification profile modal. The modal gives you the ability to name the profile and specify the type of alerts that should generate a notification. Note that multiple device types can be subscribed to the same notification profile and alert on various conditions.



For each alert type you can define when a notification should be issued. The notification can be disabled or sent at various time intervals up to 24 hours. Interval notifications are referred to as "Bulk" notifications in the email that is sent by the notification system.



The following are details for each notification and what triggers it:

■ VPN Gateway notifications:

- **Device up:** This notification will trigger the device to show as up (green status) in aView. This notification is generated whenever the gateway device is considered unreachable (gray status) or down (red status) and the device checks back in to aView by either of the following:
 - The gateway device sends an SNMP inform to aView.
 - aView is able to probe the gateway device through its management tunnel.
- **Device down:** The VPN Gateway device is probed once every 15 minutes. If aView misses two consecutive probes and also has not received any SNMP informs within the past 30 minutes, the device will be marked as down (red status) and this notification will be sent. The time specifying when a gateway device is considered down cannot be adjusted.
- **Device firmware changed:** The gateway device is running on a different firmware version from the last time the device was probed.
- **Device primary IP changed:** The gateway device's current WAN IP address has changed. To enable this SNMP inform, enable the Active WAN IP Change option in the Service Manager profile for the VPN Gateway.
- **Device rebooted:** The gateway device sent an SNMP inform that it was rebooted. To enable this SNMP inform, enable the Device Reboot option in the Service Manager profile for the VPN Gateway.

- **Backup WAN autotest failed:** The gateway device sent an SNMP inform that its scheduled autotest has failed on either the WAN2 or Cellular interface. To enable this SNMP inform, enable the W2 Autotest Failure and Dial Autotest Failure options in the Service Manager profile for the VPN Gateway.
- **Backup WAN threshold reached:** The gateway device sent an SNMP inform that it has been connected with either the WAN2 or Cellular interface longer than the threshold time. The gateway device will continue to use the backup connection if this inform is sent; the inform is meant to be a warning that the gateway device has been in backup mode for an extended period of time. To enable this SNMP inform, enable the Dial Backup Threshold option in the Service Manager profile for the VPN Gateway.
- **Device WAN interface changed:** The gateway device sent an SNMP inform that it has switched to a new WAN interface. To enable this SNMP inform, enable the Active WAN IP Change option in the Service Manager profile for the VPN Gateway.
- **Device cellular location changed:** The cellular location details reported by the Gateway device changed. See [VPN Gateway device Location tab](#) for more details about determining the cellular location of a Gateway device.
- **Device signal strength fell below a nominal threshold:** The cellular signal strength reported by the VPN Gateway device has dropped below a specified threshold percentage. This threshold is defined by the aView admin in the Admin panel of the site.
- **Device data usage over limit:** The device exceeded the specified Individual Data Limit value listed in the Data Plan associated to the device. See [Data plans](#) for more information on Data Plans.
- **Ping test succeeded:** The VPN Gateway device sent an SNMP inform that it successfully pinged an IP address specified in its Service Manager profile. The VPN Gateway must be running version 6.2 or higher to have ping tests enabled.
- **Ping test failed:** The VPN Gateway device sent an SNMP inform that it failed to ping an IP address specified in its Service Manager profile. The VPN Gateway must be running version 6.2 or higher to have ping tests enabled.
- **Device network type changed:** The SNMP probe response from the VPN Gateway device indicated that the cellular network (4G LTE, 3G HSPA+, etc.) type that it is connected on has changed.
- **VRRP state changed:** The VPN Gateway device sent an SNMP inform that its VRRP state changed. Note that VRRP must be enabled in the VPN Gateway's Service Manager profile to receive this inform.

- Legacy Cellular notifications:
 - **Device up:** This notification is generated whenever the Legacy Cellular device is considered down (red status) and the device checks back in to the aView monitor by sending a syslog or if the device is reachable through remote control commands. This notification will trigger the device to show as up (green status) in aView.
 - **Device down:** The Legacy Cellular device sends a heartbeat syslog once every 30 minutes. If aView has not received any other syslogs within the past 139 minutes (2 hours 19 minutes), the device will be marked as down (red status) and a notification will be sent. The time specifying when a Legacy Cellular device is considered down can be adjusted by changing the configuration of the device. See [Controlling device down status](#) for further information.
 - **Device signal strength fell below a nominal threshold:** The cellular signal strength reported by the Legacy Cellular device has dropped below a specified threshold percentage. This threshold is defined by the aView admin in the Admin panel of the site.
 - **Device firmware changed:** The Legacy Cellular device is running on a different firmware version from the last firmware version the device logged.
 - **Device primary IP changed:** The Legacy Cellular device sent a syslog stating that the IP address it received from the Legacy Cellular network has changed.
 - **Device network type changed:** The Legacy Cellular device sent a syslog stating that the Legacy Cellular network (4G LTE, 3G HSPA+, etc.) type that it is connected on has changed.
 - **Device rebooted:** The Legacy Cellular device sent a syslog that it rebooted. The notification and log will include the reason for the reboot.
 - **Device cellular location changed:** The cellular location details reported by the Legacy Cellular device changed. See [Location tab](#) for more details about determining a device's cellular location.
 - **Device data usage over limit:** The device exceeded the specified Individual Data Limit value listed in the Data Plan associated to the device. See [Data plans](#) for more information on Data Plans.

■ WiFi notifications:

- **Device up:** This notification is generated whenever the WiFi device is considered down (red status) and the device checks back in to the aView monitor by sending a syslog. This notification will trigger the device to show as up (green status) in aView.
- **Device down:** The WiFi device sends a heartbeat syslog once every 15 minutes. If aView misses two consecutive heartbeats and has not received any other syslogs within the past 30 minutes, the device will be marked as down (red status) and this notification will be sent. The time specifying when a WiFi device is considered down cannot be adjusted.
- **Device firmware changed:** The WiFi device is running on a different firmware version from the last firmware version the device logged.
- **Device primary IP changed:** The WiFi device sent a syslog stating that its WAN IP address has changed.
- **Device detected rogue Access Point:** The WiFi device sent a syslog stating that it found a rogue Access Point on its network. The notification will include the SSID, MAC address, and IP address of the rogue Access Point.
- **Device rebooted:** The WiFi device sent a syslog that it rebooted. The notification and log will include the reason for the reboot.

■ Dial-to-IP notifications

- **Device up:** This notification is generated whenever the Dial-to-IP device is considered down (red status) and the device checks back in to the aView monitor by sending a syslog or if the device is reachable through remote control commands. This notification will trigger the device to show as up (green status) in aView.
- **Device down:** The Dial-to-IP device sends a heartbeat syslog once every 30 minutes. If aView has not received any syslogs within the past 139 minutes (2 hours 19 minutes), the device will be marked as down (red status) and a notification will be sent. The time specifying when a Dial-to-IP device is considered down can be adjusted by changing the configuration of the device. See [Controlling device down status](#) for further information.
- **Device rebooted:** The Dial-to-IP device sent a syslog that it rebooted. The notification and log will include the reason for the reboot.
- **Device firmware changed:** The Dial-to-IP device is running on a different firmware version from the last firmware version the device logged.
- **Device primary IP changed:** The Dial-to-IP device sent a syslog stating that the IP address it received from the cellular network has changed.
- **Device network type changed:** The Dial-to-IP device sent a syslog stating that the cellular network (4G LTE, 3G HSPA+, etc.) type that it is connected on has changed.
- **Device WAN interface changed:** The Dial-to-IP device sent a syslog stating that it has switched to a new WAN interface.
- **Device data usage over limit:** The device exceeded the specified Individual Data Limit value listed in the Data Plan associated to the device. See [Data plans](#) for more information on Data Plans. Note this alert only applies to the 5300-DC model.
- **Device cellular location changed:** The cellular location details reported by the Dial-to-IP device changed. See [Location tab](#) for more details about determining a device's cellular location. Note this alert only applies to the 5300-DC model.

- Remote Manager notifications:
 - **Device up:** This notification is generated whenever the Remote Manager device is considered down (red status) and the device checks back in to the aView monitor by sending a syslog or if the device is reachable through remote control commands. This notification will trigger the device to show as up (green status) in aView.
 - **Device down:** The Remote Manager device sends a heartbeat syslog once every 30 minutes. If aView has not received any syslogs within the past 139 minutes (2 hours 19 minutes), the device will be marked as down (red status) and a notification will be sent. The time specifying when a Remote Manager device is considered down can be adjusted by changing the configuration of the device. See [Controlling device down status](#) for further information.
 - **Device rebooted:** The Remote Manager device sent a syslog that it rebooted. The notification and log will include the reason for the reboot.
 - **Device firmware changed:** The Remote Manager device is running on a different firmware version from the last firmware version the device logged.
 - **Device primary IP changed:** The Remote Manager device sent a syslog stating that the IP address it received from the cellular network has changed.
 - **Device network type changed:** The Remote Manager device sent a syslog stating that the cellular network (4G LTE, 3G HSPA+, etc.) type that it is connected on has changed.
 - **Device WAN interface changed:** The Remote Manager device sent a syslog stating that it has switched to a new WAN interface.
 - **Device port down:** The Remote Manager sent a syslog stating that either one of its serial ports has been disconnected. To receive this notification, the CTS or DCD pin must be selected as monitorable for each desired serial port in the configuration profile of the Remote Manager device.
 - **Device signal strength fell below a nominal threshold:** The cellular signal strength reported by the Remote Manager device has dropped below a specified threshold percentage. This threshold is defined by the aView admin in the Admin panel of the site.
 - **Device ethernet port connected:** The Remote Manager sent a syslog stating that a client device was connected to its Ethernet port and it has physical Ethernet connectivity to that device.
 - **Device ethernet port disconnected:** The Remote Manager sent a syslog stating that it lost physical connectivity to a client device that was previously connected via Ethernet to the Remote Manager.
 - **Device cellular location changed:** The cellular location details reported by the Remote Manager device changed. See [Location tab](#) for more details about determining a device's cellular location.
 - **Device data usage over limit:** The device exceeded the specified Individual Data Limit value listed in the Data Plan associated to the device. See [Data plans](#) for more information on Data Plans.

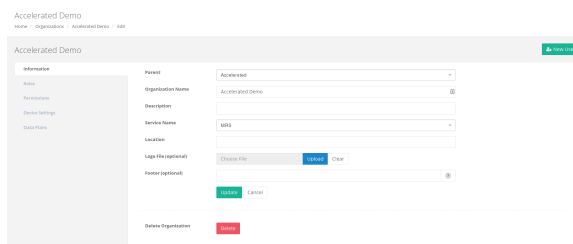
- Cellular notifications:
 - **Device recovered:** This notification is generated whenever the Cellular device is considered down (red status) and the device checks back in to the aView monitor by sending a syslog or if the device is reachable through remote control commands. This notification will trigger the device to show as up (green status) in aView.
 - **Device down:** The Cellular device sends a heartbeat syslog once every 30 minutes. If aView has not received any syslogs within the past 139 minutes (2 hours 19 minutes), the device will be marked as down (red status) and a notification will be sent. The time specifying when a Cellular device is considered down can be adjusted by changing the configuration of the device. See [Controlling device down status](#) for further information.
 - **Device rebooted:** The Cellular device sent a syslog that it rebooted. The notification and log will include the reason for the reboot.
 - **Device firmware changed:** The Cellular device is running on a different firmware version from the last firmware version the device logged.
 - **Device primary IP changed:** The Cellular device sent a syslog stating that the IP address it received from the cellular network has changed.
 - **Device network type changed:** The Cellular device sent a syslog stating that the cellular network (4G LTE, 3G HSPA+, etc.) type that it is connected on has changed.
 - **Device WAN interface changed:** The Cellular device sent a syslog stating that it has switched to a new WAN interface.
 - **Device signal strength fell below a nominal threshold:** The cellular signal strength reported by the Cellular device has dropped below a specified threshold percentage. This threshold is defined by the aView admin in the Admin panel of the site.
 - **Device ethernet port connected:** The Cellular sent a syslog stating that a client device was connected to its Ethernet port and it has physical Ethernet connectivity to that device.
 - **Device ethernet port disconnected:** The Cellular sent a syslog stating that it lost physical connectivity to a client device that was previously connected via Ethernet to the device.
 - **Device cellular location changed:** The cellular location details reported by the Cellular device changed. See [Location tab](#) for more details about determining a device's cellular location.
 - **Device data usage over limit:** The device exceeded the specified Individual Data Limit value listed in the Data Plan associated to the device. See [Data plans](#) for more information on Data Plans.

- uCPE notifications:
 - **Device recovered:** This notification is generated whenever the uCPE device is considered down (red status) and the device checks back in to the aView monitor by sending a syslog or if the device is reachable through remote control commands. This notification will trigger the device to show as up (green status) in aView.
 - **Device down:** The uCPE device sends a heartbeat syslog once every 30 minutes. If aView has not received any syslogs within the past 139 minutes (2 hours 19 minutes), the device will be marked as down (red status) and a notification will be sent. The time specifying when a uCPE device is considered down can be adjusted by changing the configuration of the device. See [Controlling device down status](#) for further information.
 - **Device rebooted:** The uCPE device sent a syslog that it rebooted. The notification and log will include the reason for the reboot.
 - **Device firmware changed:** The uCPE device is running on a different firmware version from the last firmware version the device logged.
 - **Device primary IP changed:** The uCPE device sent a syslog stating that the IP address it received from the cellular network has changed.
 - **Device WAN interface changed:** The uCPE device sent a syslog stating that it has switched to a new WAN interface.
 - **Device cellular location changed:** The cellular location details reported by the uCPE device changed. See [Location tab](#) for more details about determining a device's cellular location.
 - **Device data usage over limit:** The device exceeded the specified Individual Data Limit value listed in the Data Plan associated to the device. See [Data plans](#) for more information on Data Plans.

Managing User Access

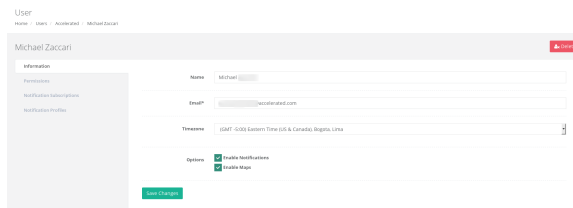
The following section details how to control the level of access a user has to devices and organizations within aView. This is done by [Roles](#) and [Permissions](#).

To view the roles and permissions associated with an organization, navigate to the **Organizations** page, click on the drop-down action box on the right hand side of the desired organization's row, and select **Edit Settings**. The roles and permissions will be listed as tabs on the organization's edit page.



The screenshot shows the 'Accelerated Demo' organization edit page. The left sidebar contains a navigation menu with 'Information', 'Roles', 'Permissions', 'Device Settings', and 'Device Profile'. The main content area has a 'Parent' dropdown set to 'Accelerated', an 'Organization Name' field with 'Accelerated Demo', a 'Description' field, a 'Device Name' dropdown set to 'MDC', a 'Location' field, a 'Logo File (optional)' field with a 'Choose File' button and a 'Upload' button, and a 'Favicon (optional)' field with a 'Choose File' button and a 'Cancel' button. At the bottom, there is a 'Delete Organization' button.

To view the permissions associated with a user, navigate to the Users page and select either the desired user's email address or **Edit** icon. The user's permissions will be listed as a tab on the edit page.



The screenshot shows the 'User' edit page for 'Michael Zaccari'. The left sidebar contains a navigation menu with 'Information', 'Permissions', 'Notification Subscriptions', and 'Notification Profile'. The main content area has a 'Name' field with 'Michael', an 'Email' field with 'michael@accelerated.com', a 'Timezone' dropdown set to '(GMT-05:00) Eastern Time (US & Canada, Regina, LNA)', and a 'Options' section with checkboxes for 'Enable Notifications' and 'Enable MFA'. At the bottom, there is a 'Save Changes' button.

If your user has the ability to manage other users, you will also have the ability to edit the user's notification subscriptions and profiles. See [Managing Notifications](#) for more details on notifications.

Workflows

Staging for initial connectivity	125
Subscribing to alerts	128
Adjusting alerts for downed devices	130
Creating new organizations	132
Permissions between organizations	141
Offline cellular connectivity test	146
Scheduled testing of inactive SIM slot	148
aView tunnel alternatives	150
Cellular signal strength threshold test	160

Staging for initial connectivity

Goal

To manually configure a router that has yet to connect to its intended cellular network in order to speed up the out-of-box experience for remote deployments.

Setup

Digi devices leverage a standardized list of known APNs (per carrier) that enable auto-discovery for initial network connectivity. Non-standard APNs should be programmed manually, and doing so can also decrease the registration time of standard APNs when they are known. Since the router has yet to establish an Internet connection, this configuration change is accomplished leveraging the local web UI. Alternatively, an active Internet connection can be connected via the router's WAN port to bring it online independent of engaging the cellular connection.

Staging via WAN Port

Instead of manipulating local device settings, Digi devices can be brought online using an alternative Internet connection over its WAN Ethernet port. The router will sync with its aView configuration template once online, meaning non-standard APNs and other settings can be pushed to the device using the WAN port (which then allows the device to connect as intended via its cellular modem).

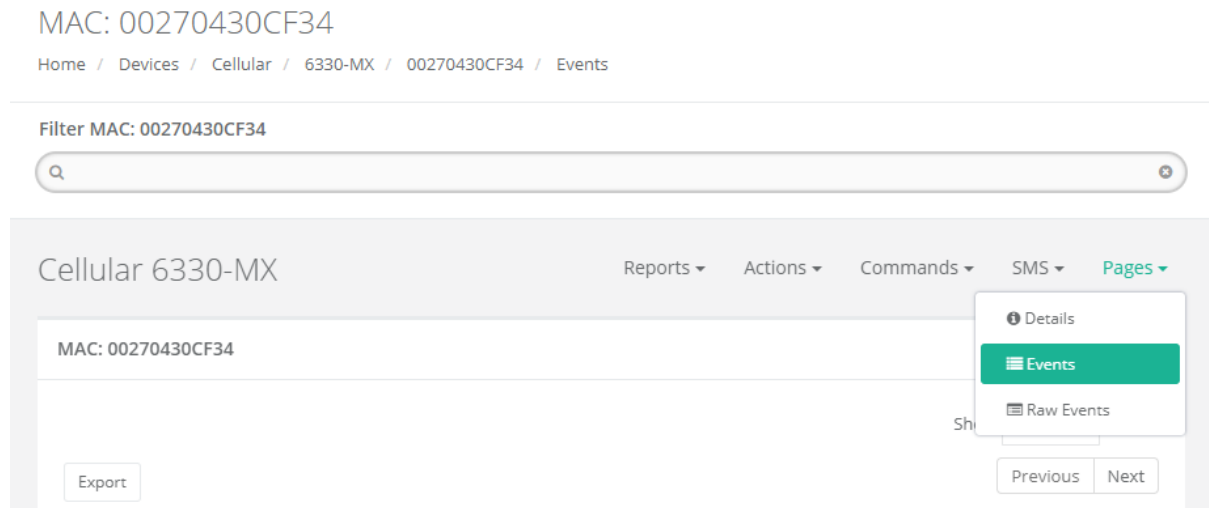
Confirming aView Config

Before bringing the device online for the first time, it is best to validate that a group configuration is linked to the router in aView. To do so, browse to the device (by clicking on its MAC address) and navigate to the **Configuration** tab. A group configuration should be populated by default, indicating that the device is properly linked to its template.

If "No Configuration" is populated, try selecting one from the corresponding pull-down menu. If there aren't any selections available, a new configuration template may need to be created/duplicated.

Connecting the Ethernet WAN

Once connected to the Internet, the router sync with its assigned configuration. Any changes will be captured in the Events/ Raw Events log.



Local Staging

The local UI can be accessed using a standard web browser, and provides a limited selection of router settings by default (full settings are available after disabling central management). Enter the cellular connection's APN here to ensure it connects to the intended cellular network properly.

Accessing the Local UI

1. Connect to the router via WiFi or its LAN Ethernet port.
2. Browse to the router's default gateway address -- this will be 192.168.210.1 per the default settings on most devices.
3. Proceed past the warning that the connection is not private.
4. Authenticate to the router using the admin credentials -- root/ default unless it has been otherwise changed.

5. Navigate to the **Configuration** tab.

6330-MX 0027043082be

You are being shown a limited set of configuration options. Please [click here](#) to access the device's full configuration. If you wish to manage this device locally, de-select the **Enable central management** option below and click **Save**.

System Configuration Expand All

Enable central management	☒
Modem	
APN	
APN lock	☐
Carrier switching	☒
PIN	
Access technology	All technologies
Authentication method	Automatic

6. Specify the APN in the **APN** field.
7. Enabling **APN lock** will force the router to only attempt to connect on the specified APN. This should be used as a last resort, assuming the device doesn't connect to the programmed APN, only after verifying the APN configuration with your cellular carrier.

Verifying APN Attempts

Once the APN has been specified:

1. Navigate to the **System Logs** menu.
2. Press ctrl + F to search for APN, or for the specified APN from the previous procedure.

If APN lock wasn't enabled per the process above, the router will attempt to connect to the specified APN and move on to the list of known APNs associated with the carrier if it is unable to connect successfully.

Should this occur, and the APN has been verified to be accurate, enable APN lock. This will force the router to exclusively attempt to connect using the specified APN, which can help the device overcome any potential timing issues on the cellular network (assuming the APN has been verified as valid per the SIM's provisioning).

The screenshot displays the Accelerated Digi aView web interface. On the left is a dark sidebar with navigation links: Status, Configuration, Dashboard, Events, System Logs, and System. The main content area shows the device identifier '6330-MX' and '0027043082be'. At the top right, there are status indicators for '4G' and 'LTE', and a 'Manage Device' button with 'State: Registered' below it. Below these, a dropdown menu shows 'All selected (4)'. The 'Current System Log' section displays a list of log entries with timestamps and messages. One entry is highlighted in blue: 'Jan 31 16:26:47 6330-MX mm: Trying APN 'TEST VALUE' on modem interface modem'.

Subscribing to alerts

Goal

To create custom notification profiles for a user account that can then be leveraged to trigger email alerts by subscribing to either individual devices or organizations as a whole.

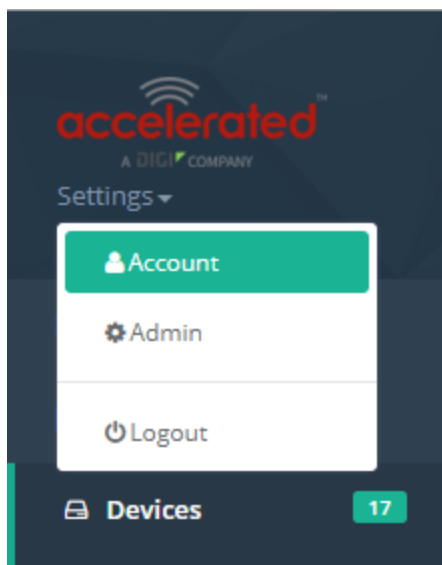
Setup

Notification profiles must be generated before creating a subscription. Both device-facing and organization-facing subscriptions can leverage the same notification profile to trigger alerts in parallel.

Note Both notification profiles and notification subscriptions are associated with individual user accounts. This means that, in order to stand up congruent alerts for multiple users, each user account will have to create the same set of parameters.

Notification Profiles

1. From the **Settings** menu option in the top-left corner of aView, select **Account**.



2. Navigate to **the Notification Profiles** tab. Existing profiles are listed as well as the corresponding subscribed events (the number of triggers for the profile) and the number of active subscriptions associated with the profile.
3. Click **Create** to stand up a new profile or Edit to adjust an existing one.
4. Enter a name for the notification profile, specify its frequency, and select the relevant alerts. Available alerts are described in [Cellular Notifications](#).

Note The **Frequency** can be adjusted to create a buffer period for the alert to prevent false positives.

Cellular Notifications

- **Device recovered:** This notification is generated whenever the Cellular device is considered down (red status) and the device checks back in to the aView monitor by sending a syslog or if the device is reachable through remote control commands. This notification will trigger the device to show as up (green status) in aView.
- **Device down:** The Cellular device sends a heartbeat syslog once every 30 minutes. If aView has not received any syslogs within the past 139 minutes (2 hours 19 minutes), the device will be marked as down (red status) and a notification will be sent. The time specifying when a Cellular device is considered down can be adjusted by changing the configuration of the device. See the Cellular Down Status section of the aView user manual.
- **Device rebooted:** The Cellular device sent a syslog that it rebooted. The notification and log will include the reason for the reboot.
- **Device firmware changed:** The Cellular device is running on a different firmware version from the last firmware version the device logged.

- **Device primary IP changed:** The Cellular device sent a syslog stating that the IP address it received from the cellular network has changed.
- **Device network type changed:** The Cellular device sent a syslog stating that the cellular network (4G LTE, 3G HSPA+, etc.) type that it is connected on has changed.
- **Device WAN interface changed:** The Cellular device sent a syslog stating that it has switched to a new WAN interface.
- **Device signal strength fell below a nominal threshold:** The cellular signal strength reported by the Cellular device has dropped below a specified threshold percentage. This threshold is defined by the aView admin in the **Admin** panel of the site.
- **Device ethernet port connected:** The Cellular sent a syslog stating that a client device was connected to its Ethernet port and it has physical Ethernet connectivity to that device.
- **Device ethernet port disconnected:** The Cellular sent a syslog stating that it lost physical connectivity to a client device that was previously connected via Ethernet to the device.
- **Device cellular location changed:** The cellular location details reported by the Cellular device changed. For more details about determining the cellular location of a Cellular device, refer to the Devices section.
- **Device data usage over limit:** The device exceeded the specified Individual Data Limit value listed in the Data Plan associated to the device. For more information on Data Plans, refer to the Organizations section of the aView user manual.

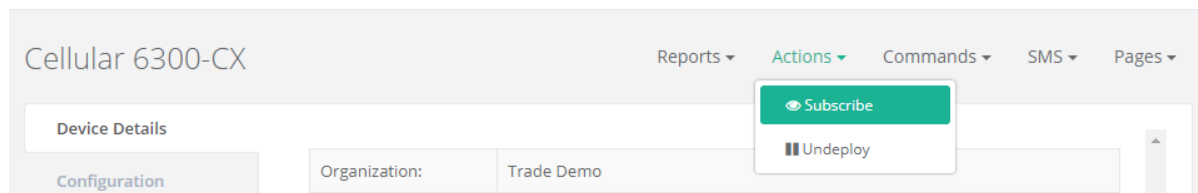
Notification Subscriptions

Individual Devices

1. Navigate to the **Device Details** page by clicking on a device's MAC address.
2. Select **Subscribe** from the **Actions** pull-down menu.

MAC: 002704296783

Home / Devices / Cellular / 6300-CX / 002704296783



3. Select the relevant notification profile from the pull-down menu. If a new profile is needed, click the **Create New Profile** button. See [Notification Profiles](#) for more information.

Adjusting alerts for downed devices

Goal

To adjust how long it takes before a router is flagged as offline in aView.

Setup

Devices in aView are flagged as down after a specified duration after missing its regular check-in. This "specified duration" is indicated in aView as the **Grace Period Duration**, and the check-in interval is designated as its **Heartbeat Interval**. Their default values are 109 minutes and 30 minutes, respectively, meaning the combination of these values -- 139 minutes -- is the default duration before an offline device is flagged as down. Adjusting either value will widen or narrow this window.

Adjusting the Heartbeat Interval

1. Navigate to either the individual router's configuration tab or the group configuration template in need of adjusting.
2. Looking at the router settings, expand **System > Log**.
3. Change the **Heartbeat interval** -- increasing or decreasing its value from the current number will adjust the delay in reporting a device as down accordingly.
4. Click **Save** to finalize the configuration change.

The screenshot shows a configuration interface for a router. At the top, there is a tab labeled 'System' with a dropdown arrow. Below this, there are several expandable sections: 'Name', 'Contact', 'Location', and 'Banner', each with a dropdown arrow and a text input field. Below these is a section labeled 'Scheduled tasks' with a plus icon and a dropdown arrow. Under 'Scheduled tasks' are two more expandable sections: 'Time' and 'Log', both with plus icons and dropdown arrows. The 'Log' section is currently expanded, showing a 'Heartbeat interval' dropdown menu set to '5m'.

In the example above, the router will check in over syslog every 5 minutes. If the device fails to check in, aView will flag the device as down if it does not check back in before the **Grace Period Duration** expires. Because the **Grace Period Duration** default value is 109 minutes, if the **Grace Period Duration** is left unchanged, this means the device will be flagged as down 114 minutes after the last time the device checked into aView.

Adjusting the Grace Period

1. Navigate to either the individual router's configuration tab or the group configuration template in need of adjusting.
2. Note that the **Grace Period Duration** is blank by default; its value is 109 minutes.

3. Increasing or decreasing this value from 109 will adjust the delay in reporting a device as down accordingly.
4. Click **Save** to finalize the configuration change.

Cellular 6350-SR

Reports ▾ Actions ▾ Commands ▾ SMS ▾ Pages ▾

Device Details

Configuration

Settings

Associated Devices

Cellular Details

Tunnels

Group Configuration

SR Default (Trade) ▾ **↑ Inherit All**

Edit group configuration: SR Default (Trade)

Last checked at Mar 29 2018 17:10:07 (EDT)

Firmware ▾

17.8.128.64 ▾

Options highlighted in blue denotes non-production firmware

Grace Period Duration ▾

5m  

In the example above, if the device misses fails to check in, aView will wait 5 minutes before flagging the device as down. Because the **Heartbeat Interval**, which determines how long the device waits to check in, defaults to 30 minutes, if the **Heartbeat Interval** is left unchanged, this means the device will be flagged as down 35 minutes after the last time the device checked into aView.

Creating new organizations

Goal

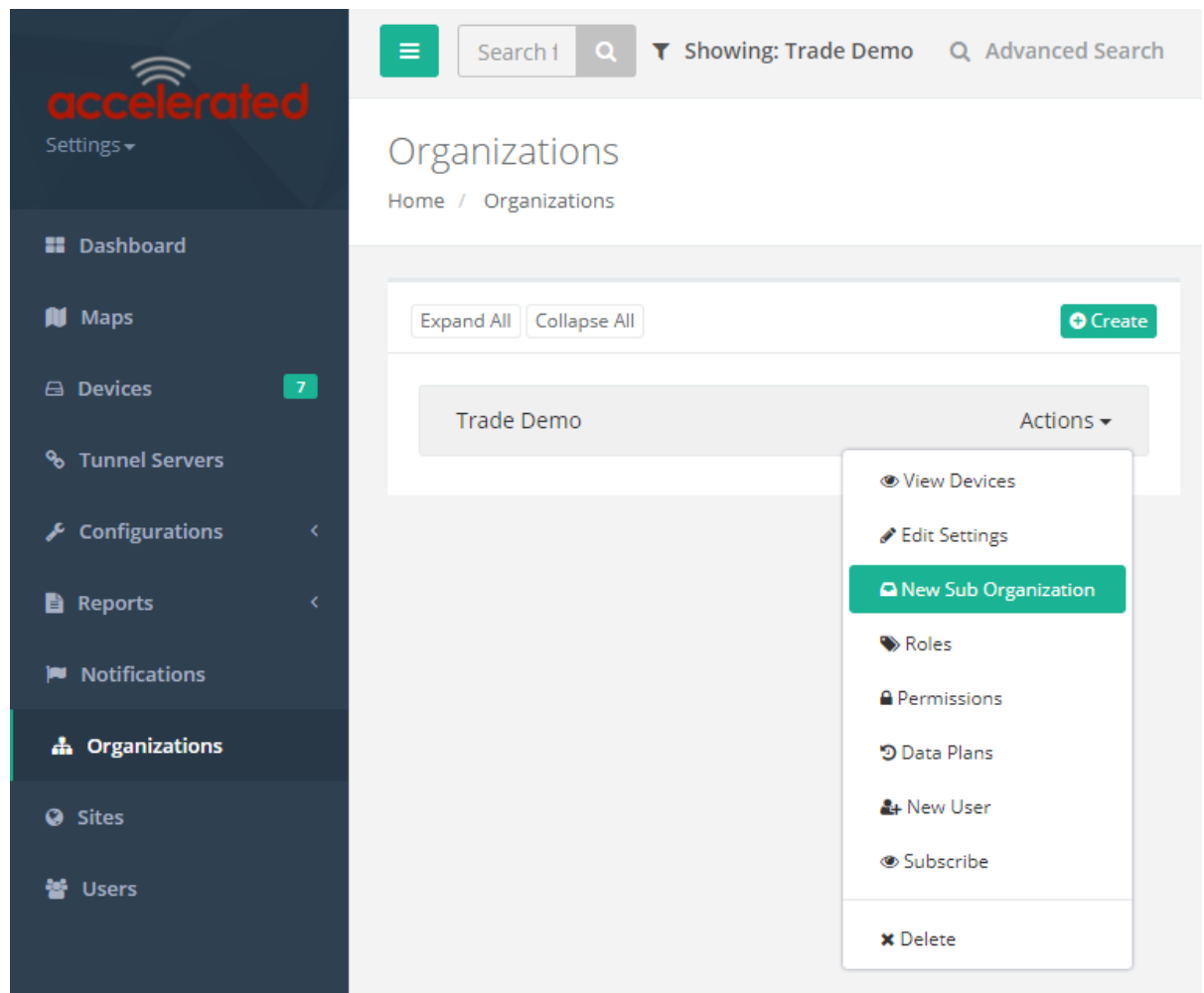
To create a new organization in aView.

Setup

New organizations in aView require that administrative permissions are set and group configurations are copied over. Once both are lined up, the organization is ready to be populated with devices and users.

Add a new Sub Organization

1. Navigate to the **Organizations** screen using the main menu.
2. Select **New Sub Organization** from the **Actions** menu.



3. Name the new organization and enter any other relevant information.

4. Click **Create Organization** to finalize the new entry.

New Organization ×

Name *	Organization Name
Parent *	Trade Demo
Description	
Service Name	
Abilities	All <input checked="" type="button" value="None"/> Custom ⊕ Expand
Logo	Choose File Upload
Footer	?

Grant admin permissions

1. Select **Roles** from the new organization's **Actions** menu.

Note that only the Admin role is listed by default, and it lacks any abilities other than View Only.

Name	Description	Abilities	Edit	Delete
Admin	Has all abilities	View Only	Edit	Delete

Showing 1 to 1 of 1 entries

2. Click the **Edit** button.

3. Define permissions by selecting the relevant checkboxes.

Edit Role

Name

Admin

Description

Has all abilities

Modify Sites

☐ ?

Modify Devices

☐ ?

Modify Organizations

☐ ?

Modify Users

☐ ?

Modify Configurations

☐ ?

Replace Devices

☐ ?

Modify Device Configurations

☐ ?

View Configuration History

☐ ?

Close

Update Role

4. Click **Update Role** to finalize any edits made to the selected Role.

You can create additional roles to define alternative levels of system access.

Populate the new organization

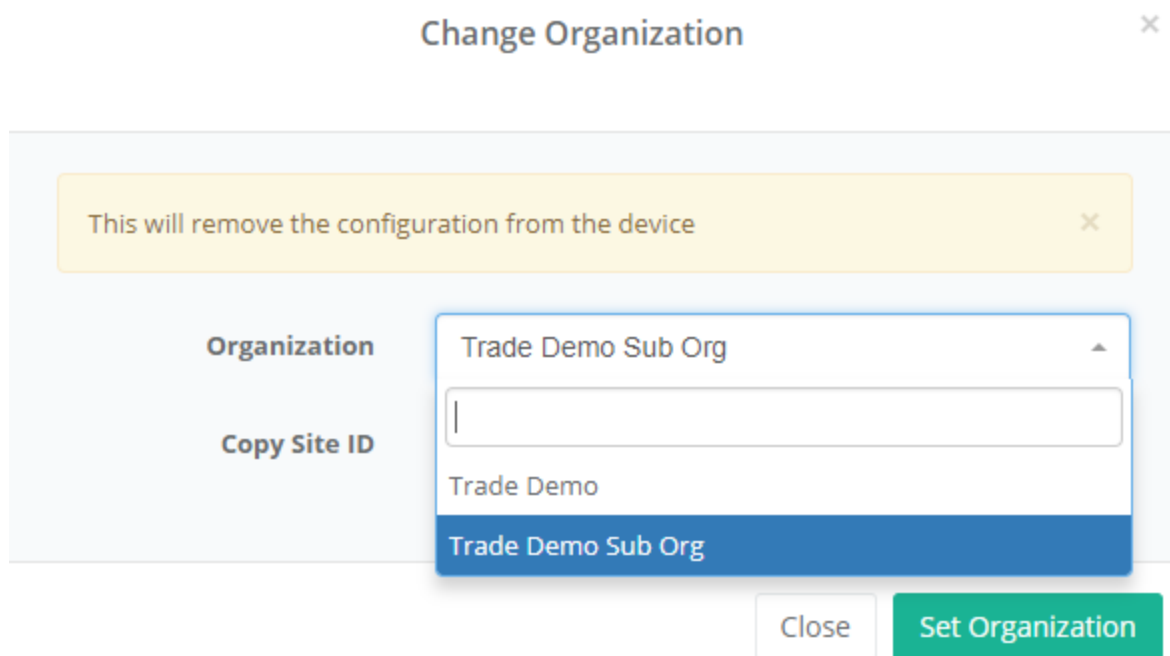
Move Devices

1. Browse to a device by searching for its MAC address or selecting it from the **Cellular Devices** list accessible from the main menu.
2. Navigate to the **Settings** tab.

The screenshot shows the 'Cellular 6350-SR' settings page. On the left is a sidebar menu with options: Device Details, Configuration, Settings (highlighted), Associated Devices, Cellular Details, Tunnels, Networks, Location, Contacts, and Netflow. The top right of the page has navigation links: Reports, Actions, Commands, SMS, and Pages. The main content area is titled 'Settings' and contains the following fields:

- Organization:** Trade Demo, with a green 'Change' button.
- Site ID:** Default, with a text input field and a link 'View devices at site: Default'.
- Data Plan:** -- No Plan --, with a dropdown arrow and a green 'Create' button.
- A green 'Update Settings' button at the bottom.

3. Select the **Change** button next to the **Organization** field and choose the newly created sub org from the corresponding pull-down menu.

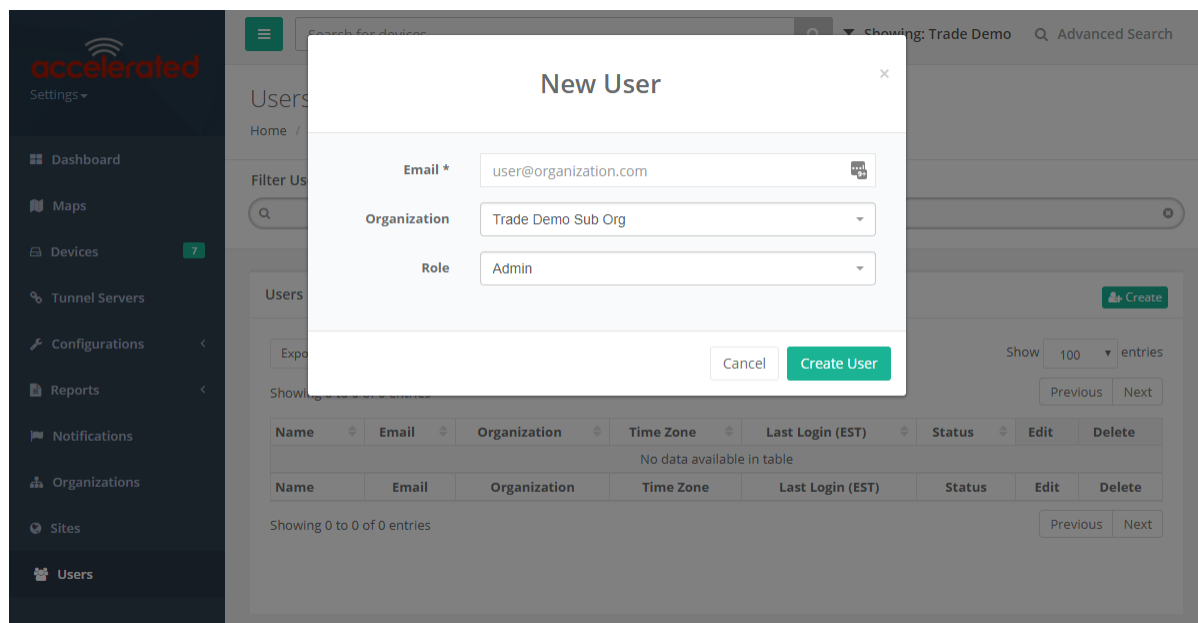


The image shows a 'Change Organization' dialog box. At the top, there is a yellow warning box that says 'This will remove the configuration from the device'. Below this, there are two labels: 'Organization' and 'Copy Site ID'. The 'Organization' label is next to a dropdown menu that is currently open, showing 'Trade Demo Sub Org' as the selected option. Below the dropdown is a text input field. At the bottom of the dialog, there are two buttons: 'Close' and 'Set Organization'.

4. Click the **Set Organization** button to finalize the device's move to its new organization.

Invite users

1. Navigate to the **Users** screen using the main menu.



The image shows the 'New User' dialog box. It has a title bar 'New User' with a close button. Inside, there are three fields: 'Email *' with the value 'user@organization.com', 'Organization' with a dropdown menu showing 'Trade Demo Sub Org', and 'Role' with a dropdown menu showing 'Admin'. At the bottom right, there are two buttons: 'Cancel' and 'Create User'. The background shows the 'Users' screen with a table of users and a sidebar menu.

- Click the green **Create** button.
- Select the intended **Organization** and **Role**.
- Click **Create User** to send out an automated invitation to the specified email address.

When a new user is created, aView will send a welcome email to the user's email address with instructions on setting up their user's password and account.

Note When creating a new user, the user must setup their account and password within 72 hours (3 days) after the email has been sent. After this time, the user will need to be recreated.

Duplicating device configurations

- Navigate to the **Configurations** screen using the main menu.

Cellular Configurations New

Showing 1 to 1 of 1 entries

Name	Organization	Category	Model	Firmware Version	Updated	Updated By	Edit	Delete
6350 Default Trade Demo	Trade Demo	Cellular	6350-SR	17.5.108.6	Aug 16 2017 13:56:19 (EDT)	jeremy.fields@accelerated.com	Edit	Delete

Showing 1 to 1 of 1 entries

- Browse to the configuration selected for duplication by clicking on the hyperlink in the entry's **Name** column.
- Click the blue **Copy** button and follow the prompt to name the new group configuration. Be sure to enter a distinct label for group configs, including a reference to the device model and organization.

Device Configurations Edit Copy Delete

Name	6350 Default Trade Demo
Organization	Trade Demo
Category	Cellular
Model	6350-SR
Firmware	17.5.108.6

Blue highlight denotes non-production firmware

- Once the new configuration has been duplicated, select the green **Edit** button.

5. Select the newly created sub org from the **Organization** pull-down menu.

Device Configurations New Link Devices Delete

Name6350 Default Trade Demo (Sub Org)

OrganizationTrade Demo Sub Org

Category

ModelTrade Demo

FirmwareTrade Demo Sub OrgVZW DemoVZW Demo2

6. Click the **Update** button at the bottom of the page after making any other configuration changes via the Settings field.
7. Browsing back to the **Configurations** screen using the main navigation menu, the newly duplicated group configuration should be listed.

Cellular Configurations New

Showing 1 to 2 of 2 entries

Showing 1 to 2 of 2 entries

Name	Organization	Category	Model	Firmware Version	Updated	Update
6350 Default Trade Demo (Sub Org)	Trade Demo Sub Org	Cellular	6350-SR	17.5.108.6	Dec 27 2017 15:03:40 (EST)	
6350 Default Trade Demo	Trade Demo	Cellular	6350-SR	17.5.108.6	Aug 16 2017 13:56:19 (EDT)	jeremy.fields@

Showing 1 to 2 of 2 entries

Be sure that the duplicated configuration is listed under the correct organization.

Linking Devices to Configuration Profiles

1. Navigate to the newly duplicated group configuration.
2. Scroll down to the bottom of the page and click the **Link Devices** button located on the right side of the screen.

Devices

Show 100 entries

Showing 1 to 1 of 1 entries
Previous 1 Next

☐	Status	MAC	Primary IP	Category	Model	Organization	Site	Firmware	Country
☐	●	0027042BB024	172.31.176.36	Cellular	6350-SR	Trade Demo Sub Org	Default	17.8.128.63	US

Showing 1 to 1 of 1 entries
Previous 1 Next

Link Selected Devices
Link All Devices
Cancel

3. Using the checkboxes found in the left-most column, select any and all devices that should be linked to this group configuration profile. The list includes all devices matching the group configuration's model (within that particular organization).

When a device is linked to a configuration, that configuration profile is automatically populated in the Group Configuration pull-down menu by default. Additional configurations can be selected from the pull-down menu if necessary, but keep in mind that the field will only show group configs associated with that device's organization.

Permissions between organizations

Goal

To grant an organization limited access to a peer organization.

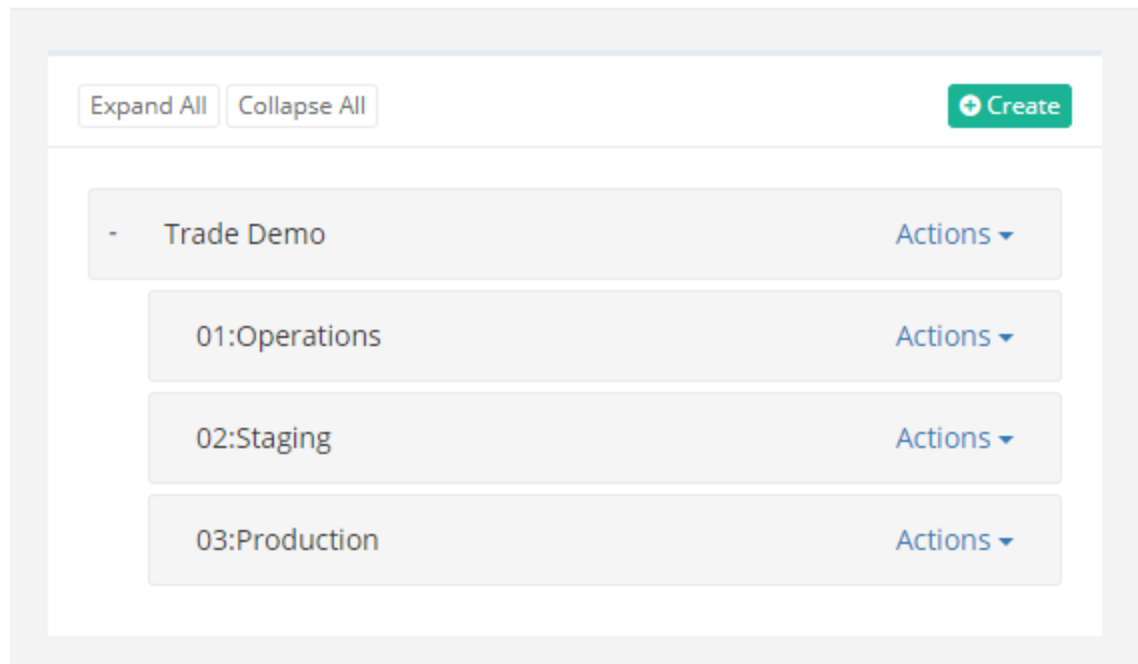
Setup

User accounts can be configured for restricted access to peer organizations by assigning a custom permission profile. This avoids the need to nest organizations in a parent/ child dynamic, which would grant full administrative access to user accounts in the parent organization.

Overview

Organizations

Home / Organizations



The following example refers to sub-organizations of "Trade Demo," as depicted above. User accounts belonging to the "Operations" organization require limited access to devices in "Staging" and "Production" -- they need to be able to move routers between orgs as routers leave the configuration lab (staging) and go out for deployment (production), but access to other aView features should be disabled.

After adding roles with the relevant abilities to each target organization (e.g. Staging and Production), selective access can be granted to users in the "Operations" org based off of the shared permissions.

For assistance with creating new Organizations in aView, see [Creating new organizations](#).

Roles with Limited Abilities

Organizations are populated with an administrative role by default. Admins should have access to all aView abilities, which isn't always the appropriate level of access for a given set of tasks.

Additional roles can be created to provide selective account permissions for users. To do so:

1. Navigate to the **Organizations** screen using the main menu.
2. Select **Roles** from the **Actions** menu of the organization intending to grant selective access. This will be either "Staging" or "Production" per the example outlined in the overview.

02:Staging

Home / Organizations / 02:Staging / Edit

02:Staging

Information

Roles

Permissions

Device Settings

Data Plans

New User

Create

Name	Description	Abilities	Edit	Delete
Admin	Has all abilities	Modify Sites Modify Devices Modify Organizations Modify Users Modify Configurations Replace Devices Modify Device Configurations View Configuration History View Admin Panel Deploy Devices Send Device Commands	Edit	Delete
Ops		Modify Sites Modify Organizations	Edit	Delete

Showing 1 to 2 of 2 entries

3. Click the **Create** button to add a new role -- be sure to only include abilities that are relevant toward the limited access.

Note The screenshot above has a secondary role, called "Ops," which will be used to grant limited access to users in other peer organizations.

Permissions for Other Organizations

After creating custom access to an organization by defining a limited role, the permissions can be granted to other organizations.

1. Navigate to the **Organizations** screen using the main menu.
2. Select **Permissions** from the **Actions** menu of the organization intending to receive selective access. This will be "Operations" per the example outlined in the overview.

3. Click the **Create** button to add new permissions to the organization.

New Permission

Organization 02:Staging

Description Ops
Admin

Abilities Ops Sites ?
Modify Organizations ?

Close Create Permission

4. Using the **Organization** pull-down menu, select the organization that is granting limited access.
5. Select the new role -- created in the first section of this document -- via the Description pull-down.
6. Verify the relevant Abilities are listed and click Create Permission to finalize the configuration change.

01:Operations

Home / Organizations / 01:Operations / Edit

01:Operations New User

Information

Roles

Permissions

Device Settings

Data Plans

Organization	Role	Abilities	Edit	Delete
01:Operations	Admin	Modify Sites Modify Devices Modify Organizations Modify Users Modify Configurations Replace Devices Modify Device Configurations View Configuration History View Admin Panel Deploy Devices Send Device Commands Assign Non-Production Firmwares	Edit	Delete
02:Staging	Ops	Modify Sites Modify Organizations	Edit	Delete

Showing 1 to 2 of 2 entries

Permissions for the "Staging" org have been added to "Operations"

Assigning Permissions to Users

Once an organization has been granted permission to a peer organization, its users can be granted access to the peer organization.

1. Navigate to the **Users** screen using the main menu.
2. Select the intended user account by clicking on its email address or the **Edit** button.
3. Browse to the **Permissions** tab of the user account.
4. Click **Create** to add access to the peer organization, selecting the relevant **Organization** and **Role** per the intended scope of access.
5. Select **Create Permission** to finalize the configuration change. The user is now able to interface with the peer organization per the **Abilities** that correspond to the organization's entry in the permissions table.

User

Home / Users

Information

Permissions

Notification Subscriptions

Notification Profiles

Organization

Role

Abilities

Edit

Delete

Create

01:Operations	Admin	Modify Sites Modify Devices Modify Organizations Modify Users Modify Configurations Replace Devices Modify Device Configurations View Configuration History View Admin Panel Deploy Devices Send Device Commands Assign Non-Production Firmwares	<a>Edit <a>Delete
02:Staging	Ops	Modify Sites Modify Organizations	<a>Edit <a>Delete

Showing 1 to 2 of 2 entries

Access to the "Staging" org is now available to this user account

Offline cellular connectivity test

Background

Our 63xx-series line of routers utilize the SureLink feature to perform connectivity tests on live Internet connections, both wired and cellular, to determine failover conditions. However, these tests are only performed when the WAN connection is up. In the case of cellular WAN interfaces, the connection could be offline or connecting, in which case the scheduled SureLink tests are not executed.

In some scenarios, the cellular modem may be stuck connecting due to a registration error, the cellular network throttling the connection, a stale activation, or the modem may be stuck on the wrong CNTI. Any of the above issues are typically fixed by resetting the embedded modem inside the 63xx-series router. This can be automatically done via a custom script on the 63xx-series router to perform a cellular connectivity test on the modem, regardless of whether it's offline or online, and then resetting the modem if that test fails a specified number of times.

See example setup below. This script, when setup in the configuration profile as shown below, will perform a connectivity test once every 20 minutes, regardless of whether the cellular modem has an Internet connection or not. If those connectivity tests fail four times in a row, then the script will automatically reset the cellular modem inside the 63xx-series router, and start its connection process over again.

Config Setup

Minimum firmware: 18.1.29

Note For firmware versions prior to 20.2.x, Digi SureLink is named Active Recovery.

Create a new custom script under System -> Scheduled tasks -> custom scripts, and enter in the following. Adjust the Interval to the desired interval you would like this script to run.

```
#!/bin/sh

# Test the cellular connection with a ping test. Keep a count of failed tests.
# If this test fails for four times in a row, then reset the modem.

# Adjustable settings
test_server='128.136.167.120' # where we perform the ping tests to
fail_count_file='/tmp/custom_cell_test_fail_count.txt'
fail_count_limit='4' # number of concurrent failures that can occur before
resetting

test_failed() {
    try=$((try+1))
    echo "$try" > "$fail_count_file"
    accns_log w config "custom: cell test failed ($1 - try $try)"
}

test_passed() {
    rm -f "$fail_count_file"
    try=0
    # Note: uncomment the following line if you want to log successful tests
    accns_log w config "custom: cell test passed"
}

try=$(cat "$fail_count_file" 2> /dev/null)
try=${try:-0}

# make sure $try is an integer. set to zero if not
case $try in
    ''|*[!0-9]*)
        try=0
    ;;
esac

# do the connectivity test
if ! modem cli 2>&1 | grep -q "connected"; then
    test_failed "Modem does not have cell connection"
elif ping -q -c 1 -W 10 -s 1 "$test_server" > /dev/null; then
    test_passed
else
    test_failed "ping failure to IP $test_server"
fi

# reset if failed test count is greater than specified limit
if [ "$try" -ge "$fail_count_limit" ]; then
    # note, that we don't reset the fail count. If we fail next attempt, try to
    reset again.
    modem reset
fi
```

Note The threshold for resetting the modem is determined by the script's fail_count_limit multiplied by the Interval set in the device configuration.

The screenshot displays the 'Scheduled tasks' configuration page in the Digi aView interface. The page is organized into a sidebar with expandable sections: Central management, Modem, Network, VPN, Firewall, Services, Authentication, and System. The 'System' section is expanded, showing fields for Name, Contact, Location, and Banner. Below these is the 'Scheduled tasks' section, which includes a 'Reboot time' field and a 'Custom scripts' section. The 'Custom scripts' section lists a script named 'cell_test_and_reset', which is highlighted by a red arrow. The script configuration includes an 'Enable' checkbox (checked), a 'Label' field (cell_test_and_reset), a 'Run mode' dropdown (Interval), an 'Interval' field (20m), an 'Once' checkbox (unchecked), and a 'Commands' text area containing the following text: '# Test the cellular connection with a ping test. Keep a count of failed tests. # If this test fails for four times in a row, then reset the modem. # Adjustable settings'. At the bottom of the 'Custom scripts' section is an 'Add Script' button with an 'Add' label. Below the 'Scheduled tasks' section are 'Time' and 'Log' expandable sections, and at the very bottom is a 'Monitoring' section.

Scheduled testing of inactive SIM slot

Design

Our 63xx-series line of routers provide SIM failover connectivity using the 1002-CM plug-in LTE modem. Scheduled Testing of inactive SIM Slot

However, the 63xx-series routers can only connect with one SIM at a given time. If both SIM slots of a 1002-CM connected to an Digi router are occupied, the user may want to periodically test the connection of that second SIM and report the results of that test and the stats of that modem to aView.

This feature is implemented using a custom script. See example setup below. This script will temporarily switch the 63xx-series router to use the secondary SIM slot, syslog to aView whether that SIM is able to establish a cellular connection (PASS/FAIL), send signal strength/connection details for that SIM to aView, perform a speed test, and then switch back to the previous SIM slot.

Config Setup

Minimum firmware: 18.1.29

Create a new custom script under System -> Scheduled tasks -> custom scripts, and enter in the following. Adjust the Run time to the desired time of day you would like to test the inactive SIM.

```
# test inactive SIM slot and report pass/fail along with modem stats to aView

run_speed_test() {
    server=$(config get config.aview.speedtest_server)
    if [ "$(expr "$server" : '[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}$' )" -eq 0 ]; then
        server=$(resolveip $server)
    fi
    if [ "$server" ]; then
        accns_log speed $(/bin/speedtest $server | tr '\n' '~' | sed 's/~$//')
    else
        accns_log w speed "Speed test failed: invalid server"
    fi
}

run_speed_test
sim1=$(sim | grep -o '[0-9]*')
sim2=$((1 + (sim1 % 2)))
case "$(runt get modem.sim.$sim2.present)" in
    ""|true)
        sim $sim2
        sleep 300
        if [ "$(runt get modem.sim.$sim2.present)" != "true" ] || ! modem cli 2>&1 |
grep -q "connected"; then
            ( sleep 90; event create info config "SIM $sim2 - check FAIL") &
        else
            event create info config "SIM $sim2 - check PASS"
        fi
        ubus call eventd reset
        trigger event status
        run_speed_test
        sim $sim1
        ;;
    *)
        event create info config "SIM $sim2 - no SIM present"
        ;;
esac
```

The screenshot shows the aView configuration interface. The left sidebar contains a navigation menu with the following items: Central management, Modem, Network, VPN, Firewall, Services, Authentication, and System. The main content area is divided into several sections: Name, Contact, Location, Banner, Scheduled tasks, System maintenance, and Custom scripts. The 'Custom scripts' section is expanded, showing a list of scripts. The first script, 'inactive_sim_test', is selected and its configuration is displayed. A red arrow points to the 'inactive_sim_test' entry in the list. The configuration for 'inactive_sim_test' includes: Enable (checked), Label (inactive_sim_test), Run mode (Set time), Run time (02:00), and Commands (a shell script). The 'Commands' field contains the following script:

```
# test inactive SIM slot and report pass/fail along with modem stats to aView
sim1=$(sim | grep -o "[0-9]*")
sim2=$((1 + (sim1 % 2)))
case "$(run get modem.sim.$sim2.present)" in
  true)
    sim $sim2
    sleep 300
    if [ "$(run get modem.sim.$sim2.present)" = "true" ] || [ modem < 2>=1 | grep -q "connected" ]; then
      / clean 00; agent create info result "SIM $sim2 - check F&B %". &
    fi
  *)
    / clean 00; agent create info result "SIM $sim2 - check F&B %". &
  fi

```

At the bottom of the 'Custom scripts' section, there is an 'Add Script' button and an 'Add' button.

aView tunnel alternatives

Overview

All of our devices by default establish an IPSec tunnel to remote.accns.com. This tunnel is used to send remote commands to a device and for the Terminal on Unit link in aView. However, due to the number of devices establishing a tunnel to this single endpoint, we have run into congestion and the result is unstable tunnel connections, which leads to poor remote interaction with a device.

We have two separate endpoints that can be used instead of the remote.accns.com tunnel: ipsec.accns.com and an AT&T SIG. See option a and option b sections below, respectively. The ipsec.accns.com endpoint is a scalable IPSec endpoint that can handle any number of devices tunneling to it. Each of the three AT&T SIG endpoints can support up to 8,000 concurrent tunnels before encountering load congestion. Therefore, our suggestion is to use the ipsec.accns.com endpoint listed in option a, and only fallback to option b if needed.

Option A - ipsec.accns.com

This is a mirror image of remote.accns.com, with some added security enhancements, load-balancing, and scalability improvements implemented under the hood. It also leverages a dynamic pool of IP address instead of the static MAC-address-to-IP allocation we have on remote.accns.com. Devices can expect to get a NAT'd DHCP tunnel IP address when tunneling to the ipsec.accns.com server. This tunnel IP is used by the aView site to send remote commands to the device, and for accessing the

device via the Terminal on Unit link in aView.

To utilize this tunnel instead of the default remote.accns.com tunnel, make the following config changes to the aView tunnel in the config settings of the device:

- set Remote endpoint -> hostname to ipsec.accns.com
- Set Remote endpoint -> ID -> IPv4 ID value to ipsec.accns.com
- Set Policies -> Policy -> Local network -> Type to Request a network
- Set Management priority to 10, which tells aView to use the tunnel IP as the primary IP to contact the unit.
- Set System > Log > Event categories > Network interfaces > Status interval interval to 1m
- Under Services -> Web administration ensure the following options are set:
 - Enable is selected
 - Port is set to 443
 - Access control list -> Zones includes IPSec

Note This zone is included in the Web administration service's ACL by default, but it's mentioned here for the user to verify that it is still present in case the device is running settings that deviate from the default config

The screenshot displays the 'VPN' configuration page in aView, specifically the 'IPsec' section. The 'Accelerated View' is enabled. The configuration includes the following fields and settings:

- NAT keep alive time:** 40s
- Tunnels:**
 - Accelerated View:**
 - Enable:** ☒
 - Zone:** IPsec
 - Mode:** Tunnel mode
 - Protocol:** ESP
 - Pre-shared key:** [Redacted]
 - Management priority:** 10
 - XAUTH client:**
 - Enable MODECFG client:** ☐
 - Local endpoint:** [Empty]
 - Remote endpoint:**
 - Hostname:** ipsec.accns.com
 - ID:**
 - ID Type:** IPv4
 - IPv4 ID value:** ipsec.accns.com
 - Policies:**
 - 1. Policy:**
 - Local network:**
 - Type:** Request a network
 - Remote network:** 192.168.211.50/32
 - IKE:** [Empty]
 - Dead peer detection:** [Empty]
 - NAT:** [Empty]
 - Active recovery:** [Empty]

At the bottom, there is an 'Add IPsec tunnel' section with a text input 'IPsec tunnel' and an 'Add' button. Below this are tabs for 'OpenVPN', 'Firewall', 'Services', 'Authentication', 'System', and 'Monitoring'.

Option B - AT&T SIG

This is one of three SIG servers residing inside our peak10 datacenter, which is where our aView application lives. This tunnel hands out dynamic IP addresses as well, in the 1.1.32.1/19 range

To utilize this tunnel instead of the default remote.accns.com tunnel, you will need to disable the default VPN -> IPsec -> Accelerated View tunnel, and create a new IPsec tunnel entry with settings matching the following configuration screenshot. You can replace the 128.136.162.23 IP address of the SIG with either of the other two SIG servers. I've listed all three below for reference.

- 128.136.162.22
- 128.136.162.23
- 128.136.162.24

```
# config dump vpn.ipsec.peak10SIG
auth.secret=AUTH0R1ZE0R5400RM
auth.type=secret
connection_monitor.attempts=3
connection_monitor.enable=true
connection_monitor.interval=15m
connection_monitor.reboot=false
connection_monitor.restart=true
connection_monitor.success_condition=one
connection_monitor.target.0.dns_server=
connection_monitor.target.0.dns_server6=
connection_monitor.target.0.http_url=
connection_monitor.target.0.http_url6=
connection_monitor.target.0.ping_host=10.0.2.50
connection_monitor.target.0.ping_host6=
connection_monitor.target.0.ping_size=20
connection_monitor.target.0.ping_size6=20
connection_monitor.target.0.test=ping
connection_monitor.timeout=15s
dpd.delay=60
dpd.enable=true
dpd.timeout=90
enable=true
ike.initiate=true
ike.mode=aggressive
ike.pad=true
ike.phase1_proposal.0.cipher=aes128
ike.phase1_proposal.0.dh_group=modp768
ike.phase1_proposal.0.hash=sha1
ike.phase2_proposal.0.cipher=aes128
ike.phase2_proposal.0.dh_group=modp768
ike.phase2_proposal.0.hash=sha1
local.id.fqdn_id=
local.id.ipv4_id=
local.id.ipv6_id=
local.id.keyid_id=RM5400_GROUP
local.id.raw_id=
local.id.rfc822_id=
local.id.type=keyid
local.interface=
local.type=defaultroute
mgmt=20
mode=tunnel
modecfg_client.enable=false
nat.0.dst=10.0.0.0/15
policy.0.local.address=
policy.0.local.custom=
policy.0.local.network=
policy.0.local.type=request
policy.0.remote.network=10.0.0.0/15
remote.hostname=128.136.162.23
remote.id.fqdn_id=
remote.id.ipv4_id=128.136.162.23
remote.id.ipv6_id=
```

```
remote.id.keyid_id=  
remote.id.raw_id=  
remote.id.rfc822_id=  
remote.id.type=ipv4  
type=esp  
xauth_client.enable=true  
xauth_client.password=alluse  
xauth_client.username=atap.v2vl1010  
zone=ipsec
```

VPN

IPsec

Accelerated View

peak10SIG

Enable

Zone

Mode

Protocol

Pre-shared key

Management priority

XAUTH client

Enable MODECFG client

Local endpoint

Remote endpoint

Policies

IKE

Dead peer detection

NAT

Active recovery

Enable

Zone

Mode

Protocol

Pre-shared key

Management priority

Enable

Username

Password

Enable MODECFG client

Local endpoint

Remote endpoint

Policies

IKE

Dead peer detection

NAT

Active recovery

1. Policy

Local network

Add Policy

1. Phase 1 Proposal

Phase 2 Proposals

Add Phase 2 Proposal

1. 10.0.0.0/15

Add NAT destination

1. Active recovery

You also need to ensure the Ipsec zone is added to the ACL for the Web admin, SSH, and Remote control services, which allows aView to access the device through the SIG on the appropriate ports/services for sending remote commands and using the Terminal on Unit link. See screenshot below for reference.

Central management

Serial

Modem

Network

VPN

Firewall

Services

Web administration

Enable

Access control list

IPv4 Addresses

IPv6 Addresses

Interfaces

Zones

1. Zone

2. Zone

3. Zone

Internal

IPsec

Setup

SSL certificate

View

Legacy port redirection

SSH

Enable

Port

Access control list

IPv4 Addresses

IPv6 Addresses

Interfaces

Zones

1. Zone

2. Zone

3. Zone

Internal

IPsec

Setup

Private key

Telnet

DNS

Remote control

Enable

Port

Access control list

IPv4 Addresses

IPv6 Addresses

Interfaces

Zones

1. Zone

Add Zone

Add

IPsec

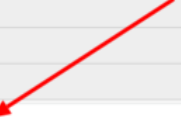
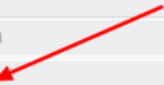
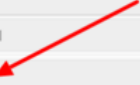
SNMP

Multicast

Authentication

System

Monitoring



Custom script for fixing primary interface on aView

The aView application determines the primary interface for a device by looking for a network syslog with default set to pri and then parses out the intf value as the primary interface. However, if I set an interface or tunnel to have a management priority, such as the case when we want to have aView treat the tunnel IP as the primary IP address to access the device, then the device never sends a syslog where the default key is set to pri and also includes an intf key/value. The result is the primary IP address for the device in aView gets updated, but not the Primary Interface. See screenshot below for reference.

Below is a sample syslog of what is currently sent

```
cnt=93~type=mgmt~default=pri~ip0=192.168.64.26~name0=ipsec-tunnel-aview
```

What should be sent is this, where the intf value that the management priority is tied to is using. Meaning, if a tunnel has the highest management priority, I still want to know which WAN interface is the primary interface.

```
cnt=93~type=mgmt~default=pri~ip0=192.168.64.26~name0=ipsec-tunnel-aview~intf=wwan0
```

The screenshot shows the aView web interface for a device named 'Cellular 6350-SR'. The 'Device Details' section is expanded, showing various fields. The 'UpLink IP Address' is highlighted with a red box, and an arrow points to it with the text 'This updates if management priority is set'. The 'Primary Interface' is highlighted with a red box, and an arrow points to it with the text 'This does not update if management priority is set'.

Device Details	
Organization:	Livonny
Site ID:	Default
Configuration:	6350 Default - Last checked at Apr 18 2018 16:24:37 (EDT)
MAC Address:	0027042CAFED
Serial:	6350010305091705
Status:	Device is up
Model:	6350-SR
UpLink IP Address:	192.168.64.67
Terminal:	Terminal on Unit
Firmware Version:	18.1.29.41
Primary Interface:	wan
Activated At:	Apr 17 2018 09:27:48 (EDT)
Last Heartbeat:	Apr 18 2018 16:54:40 (EDT)
Last Restart:	Apr 18 2018 16:24:37 (EDT)
Last Configuration Check:	Apr 18 2018 16:24:37 (EDT)
Data Plan:	N/A

This issue is tracked with our developers in ACL-160, and will be fixed in a future firmware update.

In the meantime, you can add the following custom script to a device to have it update its Primary Interface in aView properly when it's using an alternate aView tunnel. To do so, click Add under System -> Scheduled tasks -> Custom scripts. Select the Enable checkbox, add a 5-minute interval, then copy/paste the script below into the Commands field.

```
#!/bin/sh

# workaround for devices on firmware 18.4.54.22 or lower to log their primary
# WAN interface to aView when they have a mgmt priority set

send_mgmt_intf_update() {
    pri=$(run get network.mgmt.log.default)
    if [ "$pri" = 'pri' ]; then
        default_net=$(run dump network.route.default | grep -m 1 -o "interface_.*")
```

```

| cut -f2 -d'_' | tr -d '=')"
    if [ -n "$default_net" ]; then
        default_intf="$(runt get network.interface.${default_net}.device)"
        runt set network.mgmt.log.intf "$default_intf"
    fi
    log=$(runt log network.mgmt.log)
    accns_log network_mgmt "${log:+type=mgmt~}$log"
fi
}

reset_tunnel() {
    accns_log w config "custom: aView IPSec tunnel dropping incoming traffic.
Restarting tunnel..."
    cat /var/log/messages > /var/log/messages.0
    echo '' > /var/log/messages
    /sbin/ipsec stop
    sleep 5
    /sbin/ipsec start
    sleep 10
    accns_log w config "custom: aView IPSec tunnel restarted"
    send_mgmt_intf_update
}

send_mgmt_intf_update

# workaround for a rare issue where the device doesn't update it's local
# tunnel IP address, resulting in device dropping incoming packets from the
# aView tunnel IPSec server

ip_addr_string='[0-9]\{1,3\}.[0-9]\{1,3\}.[0-9]\{1,3\}.[0-9]\{1,3\}'
dropped_tunnel_dst=$(grep -m 1 "DROP.*SRC=192.168.211.50" /var/log/messages |
grep -o "$ip_addr_string" | cut -f2 -d'=')
aview_tunnel_ip=$(/sbin/ipsec status | grep -om1 "aview.*$ip_addr_string ===" |
grep -o "$ip_addr_string")

route_exists='y' #assume the route is there, then check
[ "$aview_tunnel_ip" ] && ! ip addr | grep -q "$aview_tunnel_ip" && route_
exists='n'
[ "$route_exists" = 'n' ] && reset_tunnel

if [ -n "$dropped_tunnel_dst" ] && [ "$dropped_tunnel_dst" = "$aview_tunnel_ip"
]; then
    reset_tunnel
fi

```

Notes on the username/password prompt in aView

aView looks at two specific config settings within the device's config profile to determine if it needs to prompt the user for a username/password to send a remote command to the device:

1. VPN -> IPSec -> (Tunnel - in 18.4.54 or greater firmware) -> Accelerated View -> Remote endpoint -> hostname
2. Services -> Remote control -> Enable

If option 1 is set to anything other than remote.accns.com, that triggers aView to show the username/password prompt. If option 2 is de-selected, that also triggers the prompt.

Cellular signal strength threshold test

Goal

To periodically check the cellular signal strength of the cellular modem in the 63xx-series router, and reset the cellular connection if the signal strength is below a specified threshold percentage.

Background

Cellular connections can grow stale over time, due to various environmental factors such as the modem sticking to a particular LTE band, the modem switching from one nearby cellular tower to another, or bandwidth saturation from other cellular devices in the area. Restarting the cellular connection when this occurs allows the modem to re-register with the nearby cellular towers and networks, perform PRL updates, receive OTA updates, and various other improvements that could result in improved signal strength and bandwidth.

The following script, when setup in the configuration profile as shown below, will check the cellular signal strength once every 20 minutes, regardless of whether the cellular modem has an Internet connection or not. If the signal strength falls below the specified threshold percentage four times in a row, then the script will automatically reset the cellular modem inside the 63xx-series router, and start its cellular connection process over again. The default threshold percentage is 20%, and can be adjusted by changing the `signal_threshold_percentage` variable in the script below.

Config Setup

Minimum firmware: 18.4.54

Create a new custom script under System -> Scheduled tasks -> custom scripts, and enter in the following. Adjust the Interval to 20m, or the desired interval you would like this script to run.

```
#!/bin/sh

# Check the signal strength of the modem. If it's below the specified
# percentage,
# mark it as a failure. Keep a count of failed signal strength thresholds. If
# the signal is below the threshold for four consecutive checks, then reset the
# modem.

# Adjustable settings
signal_threshold_percentage='20'
fail_count_file='/tmp/custom_signal_test_fail_count.txt'
fail_count_limit='4' # number of concurrent failures that occur before resetting
# modem

test_failed() {
    try=$((try+1))
    echo "$try" > "$fail_count_file"
    accns_log w config "custom: signal below threshold ($1 - try $try)"
}

test_passed() {
    rm -f "$fail_count_file"
    try=0
    # Note: uncomment the following line if you want to log successful tests
    #accns_log w config "custom: signal above threshold ($1)"
}


```

```
try=$(cat "$fail_count_file" 2> /dev/null)
try=${try:-0}

# make sure $try is an integer. set to zero if not
case $try in
  ''|*[!0-9]*)
    try=0
    ;;
  *)
    ;;
esac

# do the signal strength test
current_signal_pct="$(runt get mm.modem.$(modem idx).status.per)"
current_signal_pct=${current_signal_pct:-0}
if [ "$current_signal_pct" -ge "$signal_threshold_percentage" ]; then
  test_passed "current=$current_signal_pct~threshold=$signal_threshold_
percentage"
else
  test_failed "current=$current_signal_pct~threshold=$signal_threshold_
percentage"
fi

# reset modem if failed count is greater than specified limit
if [ "$try" -ge "$fail_count_limit" ]; then
  # note that we reset the fail count, to give the modem time to reconnect and
  # improve signal before we reset it again
  rm -f "$fail_count_file"
  modem reset
fi
```

Note The threshold for resetting the modem is determined by the script's `fail_count_limit` multiplied by the Interval set in the device configuration.

Central management

Modem

Network

VPN

Firewall

Services

Authentication

System

Name

Contact

Location

Banner

Scheduled tasks

Reboot time

System maintenance

Custom scripts

1. cell_test_and_reset

Enable

Label

Run mode

Interval

Once

Commands

Add Script:

Add

Time

Log

Monitoring

API

aView provides a RESTful API that can be used to obtain a list of details for one or more devices a user has access to. Full documentation on using the API can be found at the following link:

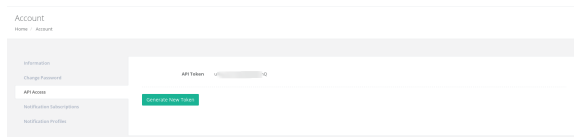
<https://aview.accns.com/apidocs>

Managing your token

Authenticated use of the API is accomplished by the use of a per-user unique token ID. You can view your user's token ID by clicking the **Settings** drop-down at the top of the left navigation panel, select the **Account** link, then click the **API Access** tab. This token never expires as long as the user has access to the aView application. You can generate a new token at any time for your user by clicking the **Generate New Token** button.

Limitations

The API limits each user to 100 requests every 15 minutes.



Release notes

Version 3.16.1	165
Version 3.14.1	165
Version 3.12.1	166
Version 3.12.0	167
Version 3.10.0	167
Version 3.9.2	168
Version 3.9.1	168
Version 3.9.0	169
Version 3.7.8	170
Version 3.7.1	171
Version 3.6.12	172

Version 3.16.1

Release date: 2019-05-01

- Digi branding update to login logo, favicon, email notifications, and documentation
- Custom settings for SNMP polling interval and alerts per organization/account for monitoring VPN Gateway devices
- Added tunnel up/down notifications for VPN Gateway devices
- Include cellular details when Exporting device index pages
- Added cellular detail columns to the Dashboard and VPN Gateway index pages
- Track the cellular provider in addition to the carrier for Cellular devices
- Added help text to Intelliflow and IDS tabs for devices, outlining the information presented in the graphs and charts on these tabs
- Added message on the IDS and Intelliflow tabs when the service is not enabled
- Added device site name to Data Plan overage notifications
- Added a reboot reason code and title to the event created when a VPN Gateway reboots
- Improved phone number formatting on the Contacts tab
- Fixed bug where 6300-CX units with serial numbers starting with 630001 were sometimes mistaken as SRs
- Fixed bug where inactive/old cellular locations were listed on the Maps page
- Fixed bug where devices couldn't be imported if serial numbers contained lower-case characters
- Changed default VPN Gateway model from 8200 to U110
- Removed phone number constraint for sending SMS commands

Version 3.14.1

Release date: 2019-02-05

- Added support for new ConnectIT4 serial range
- Added support for EX15 models
- Added organization name to the API-version2 results
- Added the device status (up/down/etc) to the API-version4 results
- Increased API rate limit from 100 to 300 requests per 15 minutes
- Increased number of supported outbound tunnels per VPN Gateway from 4 to 6
- For each group configuration profile on the **Configuration** index page, show a count of devices associated to that configuration profile
- Save and display the **VPN Service IP** address for each tunnel of a VPN Gateway. The **VPN Service IP** is the IPv4 or IPv6 address the VPN Gateway received as its local IP address for the tunnel the VPN Gateway is establishing the tunnel to
- Enable Intelliflow collection and display metrics for VPN Gateway devices
Intelliflow must be enabled on the VPN Gateway for it to post Intelliflow metrics to aView. See [VPN Gateway device Intelliflow tab](#).

- Enhanced tracking of tunnels for a VPN Gateway
 - The status of the tunnel is now used to determine what remote commands are available to interact with that particular tunnel
 - User-controlled, disabled, or down tunnels will now remain listed to allow users to send a **Tunnel Up** remote command if needed. If the device reboots or is power cycled, all old tunnels will be removed after VPN Gateway comes back online and syncs its list of configured tunnels
- Save the **config** and **port** values reported by Digi Linux (DAL) devices, such as the 6310-DX and 6350-SR, and display them for each modem entry on the **Cellular Details** tab

These new values are reported by DAL devices running on firmware version 18.4.54 and higher
- Fixed bug where duplicate entries were created on the **Cellular Details** tab for devices with multiple active cellular modems/connections
- Save the cellular module temperature reported by DAL devices and display it for each modem entry on the **Cellular Details** tab

These new values are reported by DAL devices running on firmware version 18.4.54.22 and higher
- Implemented new, scalable service for monitoring VPN Gateway devices via SNMP
- Fixed bug where Data Plan metrics would include usage from devices that were offline for over a month
- Fixed rare bug where the **Create** button on the **Roles** tab of the Edit Organizations page was not clickable in certain browsers
- Fixed bug where users could input invalid characters into the phone number of a contact under the **Contacts** tab for a device
- Fixed bug where DAL devices with previously-overridden settings would still list their configuration profile name as **mac_address Config** even though the device was inheriting all settings from its group configuration profile
- Disabled the cleanup of empty organizations by the automated import task used for syncing VPN Gateways between Service Manager and aView

Version 3.12.1

Release date: 2018-11-02

- Reduced timing of device event processing by pre-calculating heartbeat timers, bulk-inserting events to our database, and caching device heartbeats to once per minute per device
- Fix validation bug in ACL device configuration profiles using firmware versions 18.10.x or higher
- Dynamically updated the clock when a user changes timezone
- Enhanced the error messages displayed if a remote command to an ACL device fails
- Updated Admin import tool to automatically disassociate old configuration profiles from a device if the import moves the device to a different organization
- Added task to update the **Management IP** for a device after successfully sending a remote command to it
- Updated **Terminal on Unit** link to use the **Management IP** to reach the device

Version 3.12.0

Release date: 2018-10-25

- Add real-time clock under the logo of the left navigation bar (disabled by default)
Users can enable this on their **Account** page
- Support for the new SNMP MIB OIDs included in VPN Gateway firmwares 7.0+
- Reduced timing of device event processing by pre-calculating heartbeat timers and bulk-inserting events to our database
- Updated colorization, naming, and help-text of WAN Utilization charts for VPN Gateways
- Updated WAN Utilization charts to handle new information sent by VPN Gateways on firmware version 7.0+
- Optimized **Maximum Used** and **High Water Mark** metrics on WAN Utilization charts
- Exclude values of **0** from the **Average Used** line on WAN Utilization charts
- Updated colors used for noting VPN Gateway tunnel health on the device index page
VPN Gateway must be running firmware version 7.0 or higher for aView to retrieve this tunnel health
- Improved validation of the device before sending remote commands to it
 - If the device has an aView tunnel built, aView will query a DNS service running on the aView tunnel server to ensure that the IP address used to send the command to the device is the active tunnel IP for the device
 - aView will also perform an HTTP query to the device at the given IP address to ensure that it is sending the command to the correct device
 - Because of these added validations, we no longer require the user to input username and password to authenticate directly with the device, as they are already authenticated through aView
- The aView tunnel IP address for the device (used for sending remote commands) is now stored in a separate **Management IP** field on the Device Details page.
Users with permissions to edit devices in aView will be able to update this Management IP directly from the Device Details page if needed.

Version 3.10.0

Release date: 2018-08-16

- Added maintenance message to login page. Admins can control the message displayed from the Admin page
- Added support for new CX Access command options for VPN Gateway devices
- Added ability for users to export Data Plans
- Added support for ACL device configuration profiles on 18.8.14.0 or higher
- Added a Feedback button to the default footer, which can be used to provide suggestions or comments on the portal. Device or portal issues should still be directed to support
- Updated notifications for Data Plan overages to include a breakdown of usage per device.

- Updated supported list of SNMP informs to match the new informs added in firmware 7.0 of the VPN Gateway
- Updated cookie policy
- Updated bulk email notification subject to include the timestamp of when the notification was generated and how many unique devices are included in the bulk notification
- Enhanced tracking of VRRP state of VPN Gateway units by looking at the VRRP statuses for any/all VLANs
- Fixed bug with generating Availability and Cellular Utilization reports
- Fixed bug with missing cellular utilization chart if no cellular data was present for the past 24 hours
- Fixed bug where VRRP state would still be displayed for devices no longer enabled with VRRP
- Fixed bug where the timestamp for when a device last synced its central config settings would not be cleared out when applying a new group configuration to the device.

Version 3.9.2

Release date: 2018-07-23

Version 3.9.2 fixes the following bugs present in version 3.9.1 of aView

- Remote commands to devices with tunnels to ipsec.accns.com weren't working
- SMS commands weren't working
- Red and Pause icons were showing as question marks

Version 3.9.1

Release date: 2018-07-20

- Added new SIM switch remote commands for ACL devices
- Add ability to migrate arrays in device configurations for firmware versions 18.4.54 or higher
- Added link to Site ID on device show page
- Enhanced tunnels column for Gateway devices to show active versus expected tunnels count and status
- Status column on Gateway index page now only reflects the WAN status of the device
Requires Gateway device to be on firmware version 7.0 or higher
- Added ability to search API for devices by serial
- Added new **Comment** field to device index and show pages messages once a user logs into the site
- Added new **CX Access** remote command for VPN Gateway devices
- Include tunnel name in tunnel-related events from VPN Gateway
- Removed requirements for serial numbers to be exactly 16-digits
- Removed requirement for users to click **OK** button of Privacy/Cookie policies before they could login to the site.
- Removed **VRRP Master** from VPN Gateway device statuses

- Removed **Category** column from device-specific index pages. Category is still included on **All** index page
- Categorized and grouped remote commands listed under **Commands** dropdown
- Allow individual ACL device configurations to span the whole row
- Updated footer links to add Privacy and Cookie policies
- Improved speed and reliability of utilization charts and generating device reports
- Filter index page to always show undeployed devices at bottom of the list of devices, regardless of the up/down status of the undeployed device.
- Increased site-wide org typeahead search limit from 10 to 100 to account for search terms with common phrasing
- Changed manual tunnel up/down command to prepopulate interface fields with blank instead of zero
- Adjusted width of headers in pop-up modals so the text is not squished together
- Limit location postal code to 20 characters
- Updated device status filtering to not show undeployed devices when filtering by up/down status
- Fixed bug where modem with missing mcc/mnc/cid/lac values would show an incorrect cellular location
- Fixed bug where **Update Modem Firmware** remote command would fail when sent to an ACL device using the json_command
- Prevent duplicate modem records when device switches SIM slots
- Prevent **aview=purge** ipsec events from deleting the tunnel that the event updates.
- Fixed bug where bulk notification frequency was not honored
- Prevent Error on Page Load for Device Show Page for Legacy Cellular Devices
- Fixed bug where clicking in text box of site-wide org filter would make the dropdown unusable
- Renamed WR14 model to IX14

Version 3.9.0

Release date: 2018-07-18

- Added new SIM switch remote commands for ACL devices
- Add ability to migrate arrays in device configurations for firmware versions 18.4.54 or higher
- Added link to Site ID on device show page
- Enhanced tunnels column for Gateway devices to show active versus expected tunnels count and status
- Status column on Gateway index page now only reflects the WAN status of the device
- Added ability to search API for devices by serial
- Added new **Comment** field to device index and show pages messages once a user logs into the site
- Added new **CX Access** remote command for VPN Gateway devices
- Include tunnel name in tunnel-related events from VPN Gateway
- Removed requirements for serial numbers to be exactly 16-digits

- Removed requirement for users to click OK button of Privacy/Cookie policies before they could login to the site.
- Removed **VRRP Master** from VPN Gateway device statuses
- Removed **Category** column from device-specific index pages. Category is still included on **All** index page
- Categorized and grouped remote commands listed under **Commands** dropdown
- Allow individual ACL device configurations to span the whole row
- Updated footer links to add Privacy and Cookie policies
- Improved speed and reliability of utilization charts and generating device reports
- Filter index page to always show undeployed devices at bottom of the list of devices, regardless of the up/down status of the undeployed device.
- Increased site-wide org typeahead search limit from 10 to 100 to account for search terms with common phrasing
- Changed manual tunnel up/down command to prepopulate interface fields with blank instead of zero
- Adjusted width of headers in pop-up modals so the text is not squished together
- Limit location postal code to 20 characters
- Updated device status filtering to not show undeployed devices when filtering by up/down status
- Fixed bug where modem with missing mcc/mnc/cid/lac values would show an incorrect cellular location
- Fixed bug where **Update Modem Firmware** remote command would fail when sent to an ACL device using the json_command
- Prevent duplicate modem records when device switches SIM slots
- Prevent **aview=purge** ipsec events from deleting the tunnel that the event updates.
- Fixed bug where bulk notification frequency was not honored
- Prevent Error on Page Load for Device Show Page for Legacy Cellular Devices
- Fixed bug where clicking in text box of site-wide org filter would make the dropdown unusable

Version 3.7.8

Release date: 2018-05-25

- Show a device's cellular location pin even if no user-entered location is present.
If available and if setting is enabled on user's account in aView
- Removed **Order By** option when creating Reports. Reports can be sorted and ordered after they are generated.
- Remove tunnel down status (purple color) from available list of statuses for a VPN Gateway.
- Replace site-wide organization filter with type-ahead filter
- Clear out device's Tunnels tab for Digi (non-VPN Gateway) devices when "aview=purge" event is received.
This event is sent by Digi devices running firmware version 18.1.29 or higher a few minutes after they are powered up and are online.

- Added ability to delete device modems from the Cellular Details tab of a device.
- Added a disclaimer to speed test results from Digi (non-VPN Gateway) devices.
- Grammar and typo fixes on the Device Details page for VPN Gateways.
- Fixed rare bug where a device would be considered undeployed due to a timezone mismatch in SNMP informs.
- Fixed event creation logic when processing modem-related details from a Gateway SNMP probe
- Fixed bug where devices connected to the HSDPA cellular network would be marked as unknown networks instead of 3G.
- Fixed bug where Location tab for a device would be shown after a user de-selected the Enable Maps option in their Account settings.
- Fixed bug rendering Dashboard and Maps page on IE11 browser
- Fixed datapoint offset when viewing various charts (cellular usage, IDS, WAN utilization, etc.). Datapoints are now shown in UTC time.
- Show appropriate status for VPN Gateways in Dual WAN mode.
 - Green – both up
 - Orange – WAN1 up, WAN2 down
 - Blue – WAN1 down, WAN2 up
 - Red – WAN1 down, WAN2 down
- Collect and store Gateway primary VRRP status with SNMP probes.
- Get tunnel name from SNMP probe and display it on the Tunnels tab
- Add missing TunnelDown reason codes to device events
- Added a disclaimer to the IDS chart when a user hovers over a datapoint, clarifying the timeframe the data pertains to.
- Hide WAN Toggle remote commands from 8200 and older VPN Gateways, as they don't support the command.
- Added **status** option to WAN toggle command
- Added state drop-down list to the Location tab for a device when the Country is set to United States. Any other country will display a standard text field where the user must type in the state/province.
- Added support for ACL device configurations on firmware version 18.4.54 or higher
- Add support for WR14 device model
- Add support for 5402-RM device model
- Add support for non-standard device serial formats
- Collect and store Gateway SNMP tunnel status fields
- Add Privacy and Cookie policy links to the footer (aView only)
- Let individual and group ACL device configuration span the whole row
- Prevent duplicate modem records when device switches SIM slots

Version 3.7.1

Release date: 2018-01-12

- Optimized device details page for faster loading and rendering.
Each tab on the page is now loaded when selected, as opposed to all at once.
- Optimized searching and device indexing to deliver faster page load and search results.
- Allow admins to set the Activation date through the Admin Importer.
- Fixed bug when saving the history of who edited a device configuration.
- Auto-undeploy VPN Gateway devices if Digi aView hasn't heard from them within 30 days.
- Auto-deploy VPN Gateway devices once they sync with Digi aView.
- Added support for tracking the cellular band reported by a VPN Gateway's cellular modem.
Requires VPN Gateway firmware version 6.5 or higher
- Added support for tracking data send/received on each individual LAN port of a VPN Gateway.
Rx/Tx values can be seen by hovering your mouse over a LAN port on a VPN Gateway's device details page.
- Updated Emergency SMS message event to always show the encrypted SMS string.
- Added a new **WAN Toggle** command to enable/disable a VPN Gateway's WAN port for a specified amount of time.
- Added support for processing and displaying backup tests performed by VPN Gateway devices.
Results are displayed under a new **Connectivity Tests** tab on the device details page.
- Added a new **Backup WAN Test** command to manually trigger a backup test on a VPN Gateway device.
- Removed **Default** site IDs. Users can now leave site IDs blank if desired.
- Fixed rare bug where users couldn't apply a new group configuration to a device after overriding group config settings and subsequently removing the group config from a device.
- Fixed bug where duplicate network entries could appear on the Networks tab for a device.

Version 3.6.12

Release date: 2017-12-21

- Support for the 6310-DX model
- Fixed bug validating new contacts for a device
- Allow location details for a Gateway device to be cleared from Service Manager