6300-CX

Table of Contents

User Manual

Configuration Examples

Solution Guides

Supplemental Information

Antenna Notes and Solutions

Package Contents

6300-CX Unit

Cellular Antennas (2x)

Ethernet Cable

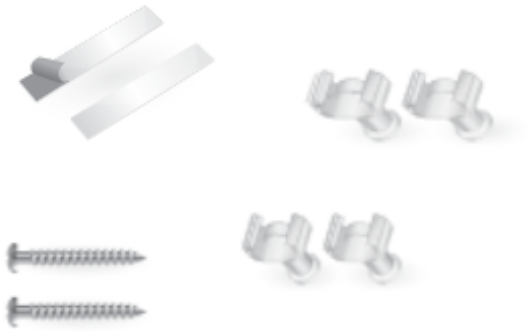
Power Supply Unit

Power-over-Ethernet (PoE) Injector

Temporary Battery Pack

Mounting Bracket

Mounting Accessories

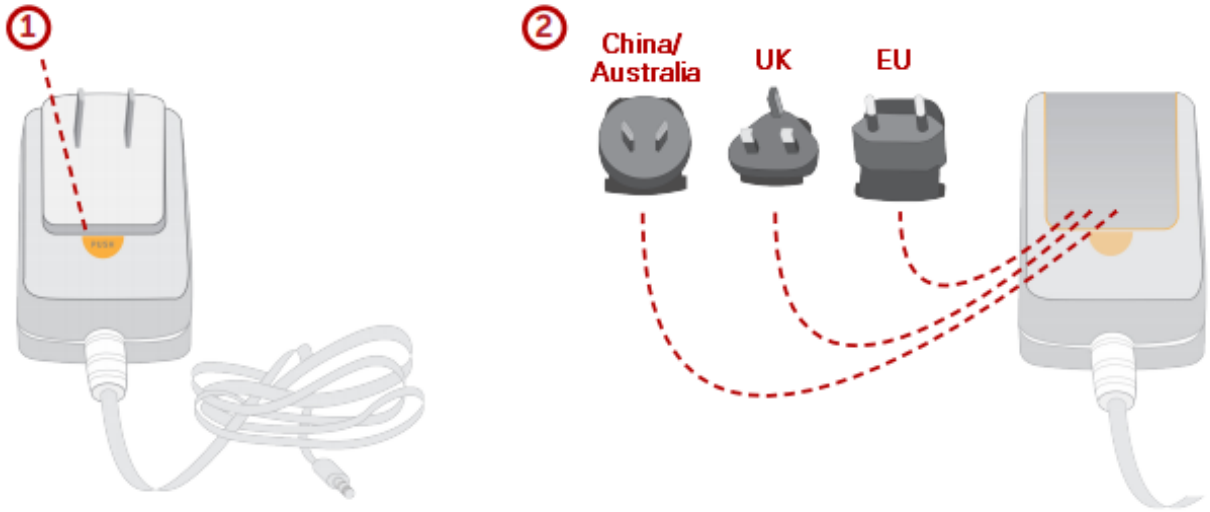


Exchanging Power Tips

The 6300-CX router may include four interchangeable plug tips that allows the Power Supply Unit (PSU) to operate in most countries. The PSU comes with the United States style plug installed.

To change the plug tip:

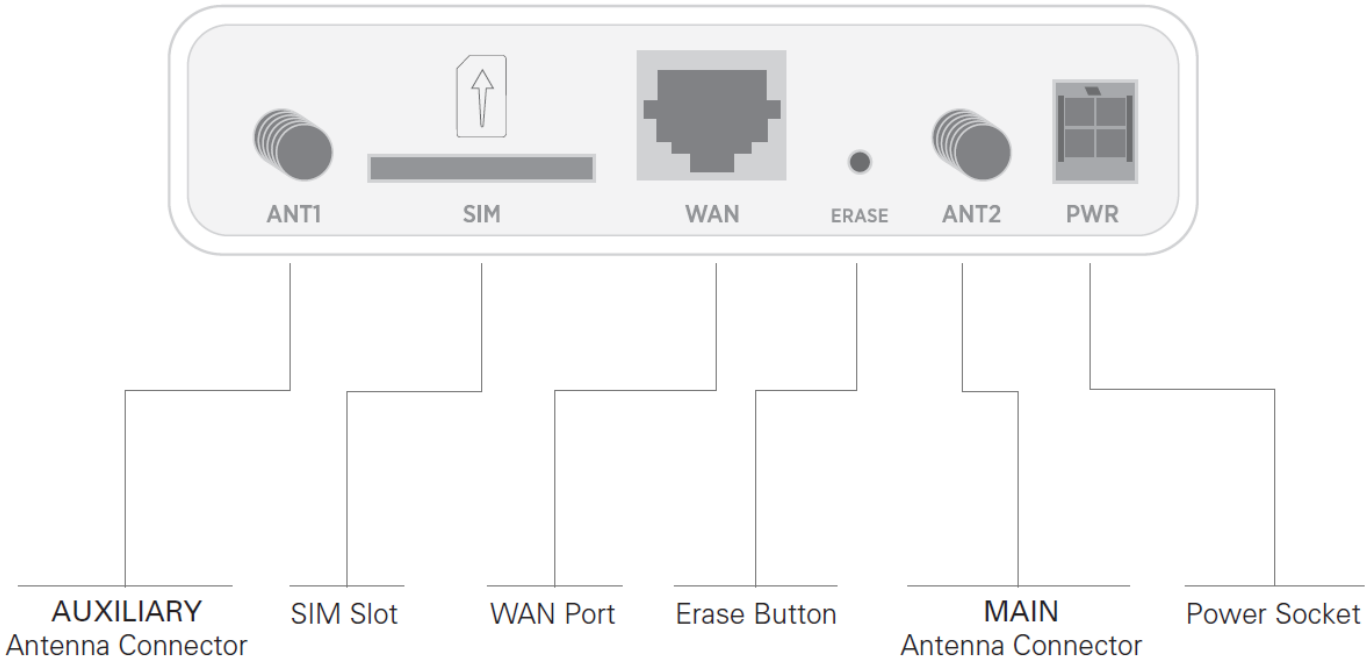
- While holding down the "PUSH" button, slide the current plug tip forward.
- Pull off the attached plug tip.
- Slide the new tip down into place until it clicks.



NOTE: For more information regarding power-tip compatibility with global deployments, please click here.

Ports and Connectors

Back of 6300-CX



LTE Signal Status

Once powered on with its plug-in modem connected (including the activated SIM card), the 6300-CX will boot up and attempt to join its cellular network. Initialization may take 30-60 seconds.

LEDs on the **Signal Strength Indicator** show the quality of cellular reception.

The **Network Status LED** displays the cellular network connection's status (i.e. whether it is on a 3G or 4G connection, or unable to connect to either).

Please refer to the following tables for more information:

Network Status LED

Solid Yellow Initializing or starting up.	**Solid Green** Connected to 2G or 3G and also has a device linked to a LAN port.
Flashing Yellow In the process of connecting to the cellular network and to any device on its LAN port(s).	**Flashing Blue** Connected to 4G LTE and in the process of connecting to a device on its LAN port(s).
Flashing White Established LAN connection(s) and is in the process of connecting to the cellular network.	**Solid Blue** Connected to 4G LTE and also has a LAN connection.
Flashing Green Connected to 2G or 3G and is in the process of connecting to any device on its LAN port(s), or nothing is connected to the port.	**Alternating Red/ Yellow** Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Signal Strength LEDs

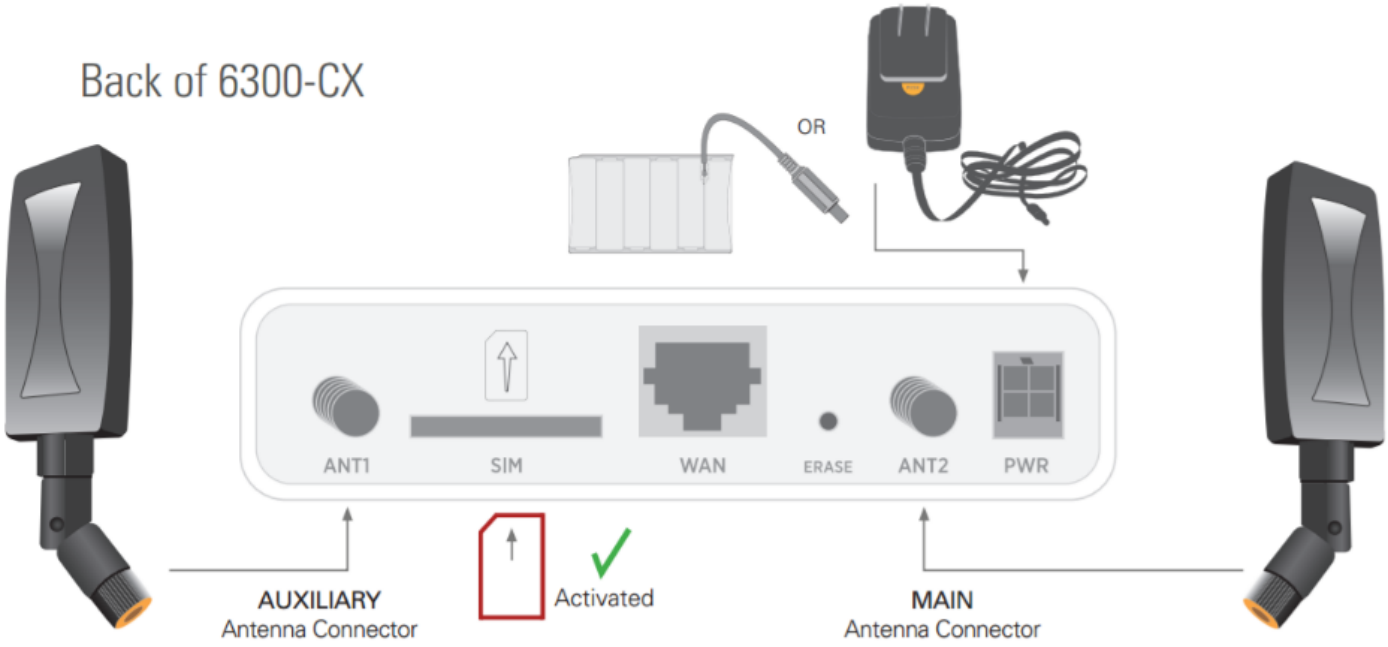
Signal Bars	Weighted dBm	Signal Strength %	Quality
	-113 to -99	0 - 23%	Bad
	-98 to -87	24 - 42%	Marginal
	-86 to -76	43 - 61%	OK
	-75 to -64	62 - 80%	Good
	-63 to -51	81 - 100%	Excellent

These measurements are negative numbers, meaning the smaller negative values denote a larger number. So, for example, a -85 is a better signal than -90.

NOTE: For more information regarding how signal strength is calculated and subsequently displayed via the LED indicators, refer to this explanation.

Initial Setup

1. Insert your activated SIM card provided by your cellular network operator. The metal contacts should be facing down. You should hear a click sound once the SIM is completely inserted.
2. For maximum performance, attach both of the included antennas. While gripping the metal connector section with your thumb and forefinger, tighten until the antenna is secure. Do not tighten the antenna by holding any part of the plastic housing.
3. Connect the power supply unit or Ethernet cable (for PoE), or if doing a site survey, attach the temporary battery pack and follow the instructions in the Site Survey section.

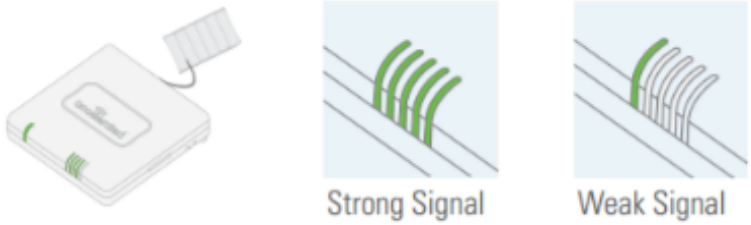


* If a single antenna solution is required, it must be attached to the main antenna port labeled 'ANT2'

Site Survey

A cellular site survey is not necessary if your anticipated installation location is known to have strong cellular signal strength. If you are unsure of available cellular signal strength or are choosing between several installation locations, follow the below instructions to perform a site survey to determine your best possible installation location. After the optimal location has been determined, setup the 6300-CX with either the power supply unit or the POE injector cable.

1. Follow the steps in the “Initial Setup” section above. During a site survey it is useful to use the included battery pack instead of the power supply unit to power the Accelerated 6300-CX. The battery pack will power your device for approximately two hours while you perform your site survey. The battery pack is not rechargeable and should be properly disposed of after use.
2. Move the Accelerated 6300-CX to different locations within your site to determine the best compromise between signal strength and installation constraints. Since cellular signal strength may fluctuate, it is important to wait at each location for 1 minute while observing the signal strength indicator on the front of the device. Minimum cellular signal strength for proper operation is 2 bars.
3. After the optimal location has been determined, remove the battery pack and connect either the main power supply unit or POE injector cable (see section labeled Using Remote Power for more information).



After the optimal location has been determined, setup the 6300-CX with either the power supply unit or the POE injector cable.

Site Survey Troubleshooting

If you are unable to verify a location with a strong cellular signal:

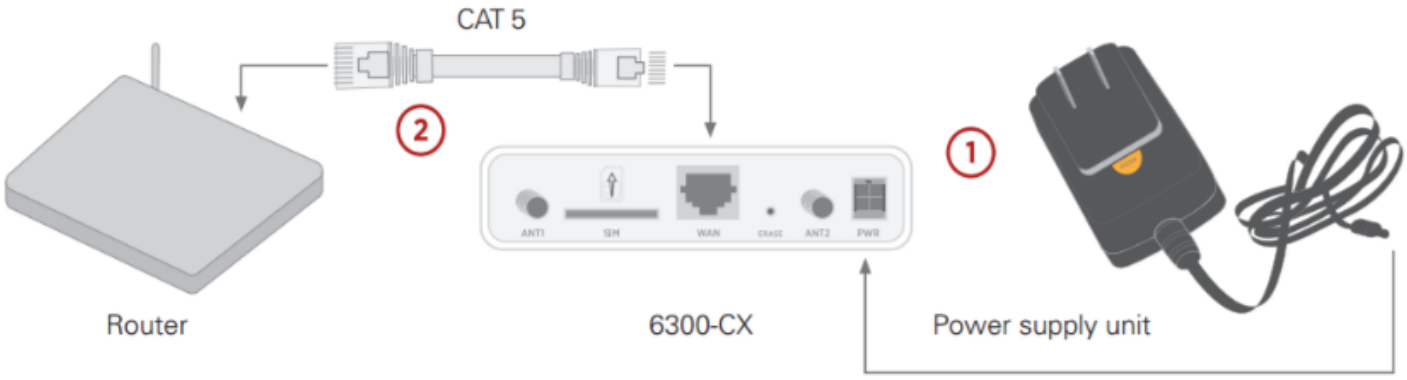
- Verify your SIM has been activated with your cellular operator.
- If cellular signal isn’t indicated on the Accelerated 6300-CX indoors, then take the device outdoors to verify that your cellular network operator has coverage in your location.

- If the outdoor cellular signal strength is less than 2 bars, it may be necessary to connect using a different cellular network operator. This requires an activated SIM from the alternate cellular network operator.
- Try the device/antennas in different orientations and away from other nearby electronic equipment at each test location. Note: LTE requires the use of both antennas & antennas will usually give better performance when vertical.
- Refer to the Device Status section to use Accelerated 6300-CX indicator lights to aid in diagnosis.

Physical Installation

Connecting to the Site Network with Local Power

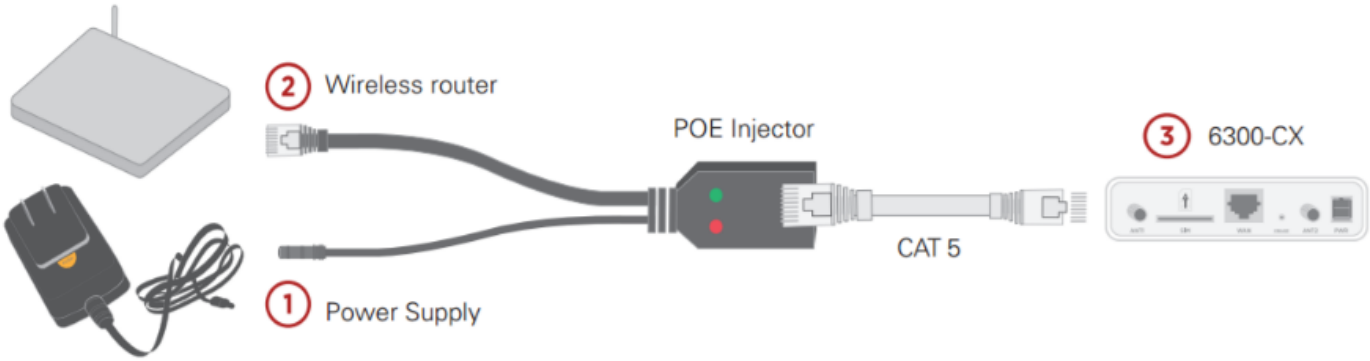
Using an Ethernet cable, connect the WAN port on the Accelerated 6300-CX to your site Gateway. By default a DHCP request will be sent to the WAN Ethernet network.



1. Plug the power supply unit into an AC power outlet and connect to the 12V DC lead (4 pin connector) of the POE injector cable.
2. Using the include CAT5 cable or a customer provided CAT5 cable connect to your site router or gateway and the WAN port of the 6300-CX.

Connecting to the Site Network with Remote Power

If your device needs to be positioned some distance from either the nearest AC power outlet or site network equipment/router using the included passive Power-Over-Ethernet (POE) injector cable will usually simplify the installation cabling and allow for improved cellular signal strength. The POE injector cable allows the DC power and Ethernet connection to be run to the Accelerated 6300-CX via the Ethernet connection only.



1. Plug the power supply unit into an AC power outlet and connect to the 12V DC lead (4 pin connector) of the POE injector cable.

2. Connect the male RJ45 connector plug of the POE injector cable to the site network equipment/router.
3. Connect a standard Ethernet cable from the RJ45 socket/jack on the POE injector cable, (marked 'DC OUT'), to the Ethernet port of the device

Remote Power Trouble Shooting

On the end of the POE injector cable (see diagram) there are two LEDs. The Red LED marked DC IN will be

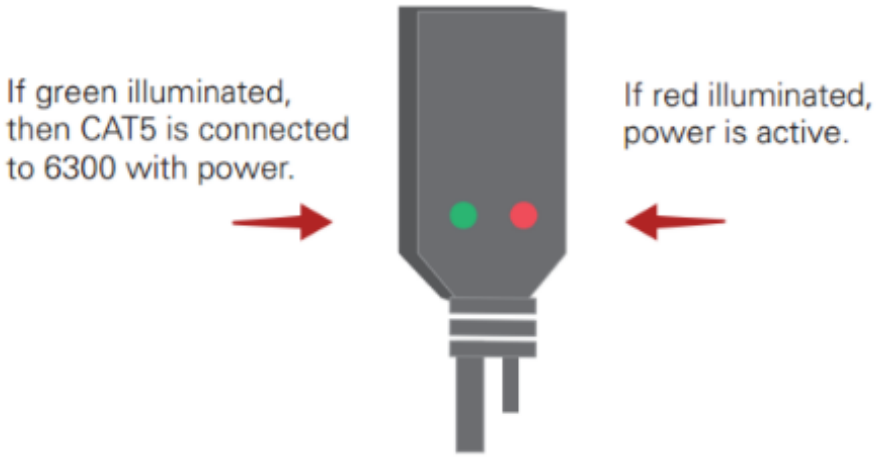
illuminated if the 6300-CX Power Supply Unit (PSU) in plugged into an AC power outlet and plugged into the POE Injector Cable. If the red LED is not illuminated check the following:

- Ensure that the PSU is plugged into an AC power outlet and is receiving power.
- Ensure that the PSU's power plug is correctly connected to the POE injector cable power input socket. The proper orientation is for the lock tab and clip to align. (See picture below)

Correct power supply connection

The Red LED marked DC IN and the Green LED marked DC OUT will both be illuminated on the POE injector cable (see diagram) if you have properly connected the PSU and you have connect a length of CAT5 cable properly to the POE injector cable and the 6300-CX. If the red LED is illuminated and the Green LED not illuminated check the following:

- Ensure that you have a good connection at both the ends of you CAT5 cable.
- Check your CAT5 cable.


If green illuminated,
then CAT5 is connected
to 6300 with power.
If red illuminated,
power is active.

Configuring Device

Network Managed Configuration

Your Accelerated 6300-CX has the capability to automatically sync and receive all settings from a centralized cloud management tool, Accelerated View™.

The Accelerated View management portal provides the following capabilities for your Accelerated 6300-CX.

- Monitoring details including signal strength, network connectivity details (RSRP, CNTI, RSRQ, Ec/Io, etc.), SIM card details (IMEI, IMSI, ESN, etc.), data transmitted/received, and more.
- Email notifications based on connectivity, device firmware, and signal strength.
- Remote control.
- Out of band SMS recovery.

Devices using Accelerated View typically require no additional configuration or set-up.

Local Configuration

If your Accelerated 6300-CX is not provisioned in Accelerated View, it will use a default local configuration profile which will enable basic cellular connectivity (primary or backup) to your router. Your device will operate as a transparent bridge and all traffic on all ports is passed directly to and from the client device connected to the device's Ethernet port.

To change any default settings for an Accelerated 6300-CX not provisioned in Accelerated View refer to Managing Device Locally section.

Troubleshooting

Resetting Your Device

While the settings are reset, the device's firmware version remains the same.

To reset the device to factory default settings, press and release the ERASE switch once on the rear of the device when the device is switched on. This will erase all device-specific settings (excluding the automatically generated keys/certificates) to their original state, and it will automatically reboot.

Establishing Backup Connectivity via Ethernet Port

If the device cannot connect using a cellular connection, use the following steps to use the Ethernet WAN connection:

1. Restore the device to its factory default settings.
2. Connect the Ethernet port of the device to the site network equipment/router. This may be done either directly with an Ethernet cable or via the POE injector cable (6). Refer to the section "Using the Passive POE Injector Cable" above. Check for solid LINK and flashing ACTIVITY LEDs on the device WAN Ethernet port.
3. Ensure the router connected to the Ethernet port of the device is configured with an IP address of 192.168.210.254/24. The device will try to use this as its gateway IP address for backup connectivity.
4. Observe the Status Indication LEDs & Signal Strength sections to aid in diagnosis.

Note: Backup Connectivity via Ethernet Port and WAN connectivity via Ethernet Port features cannot be used at the same time. If you use the steps listed here to set the device's Ethernet port as a backup connection for itself, the 6300-CX will not be able to provide WAN connectivity to client device(s).

Out of Band SMS Commands

A set of emergency remote commands can be sent via SMS to the device to provide out-of-band (OOB) recovery for the device. These SMS commands allow you to perform actions such as factory resets, reboot the device, and restore to the backup firmware partition, all without requiring the device to have an active cellular connection. Similar to the standard remote commands, these can be used to provide control over the device without any onsite interaction. To utilize this feature, SMS must be enabled for the SIM card used by the device. The complete

list of SMS commands is defined in the Accelerated View™ User's Guide. (https://aview-docs.accns.com)

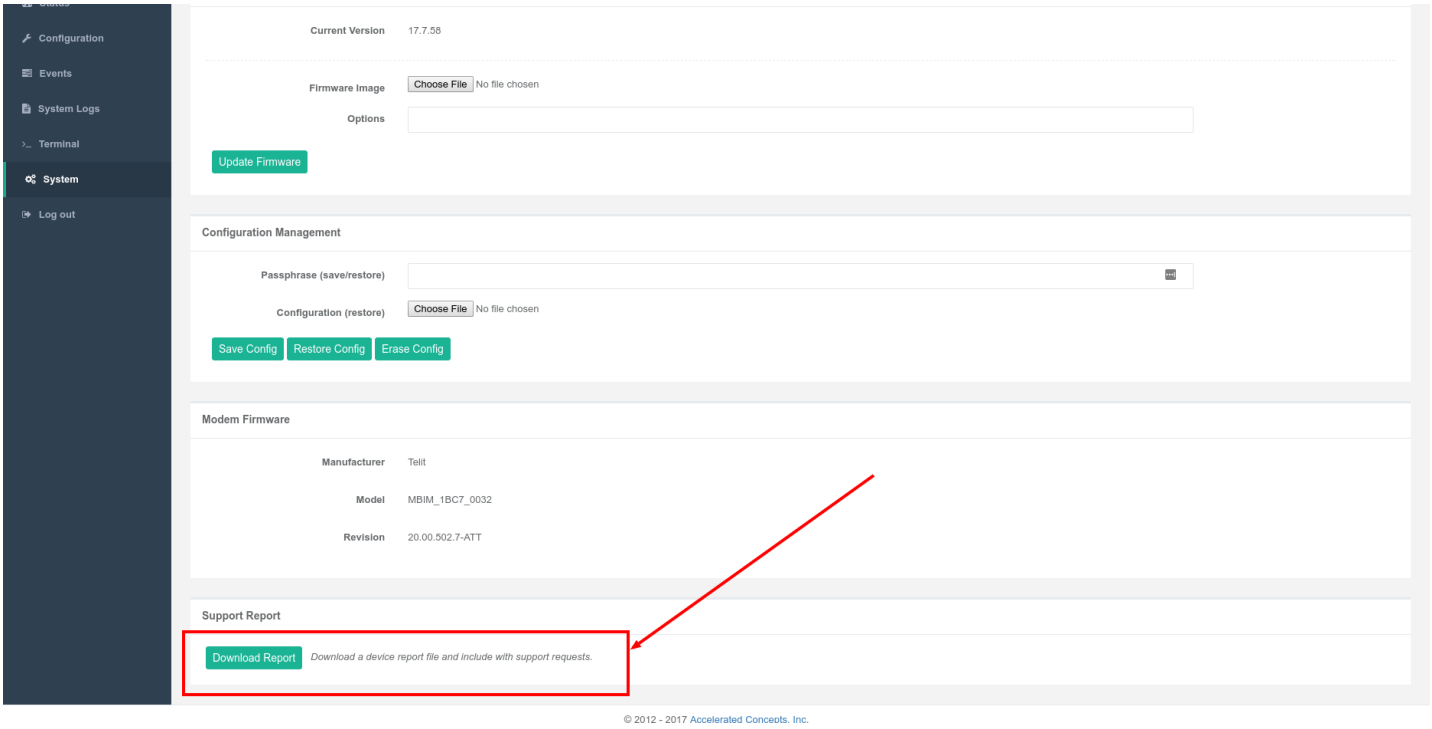
Support Report

Often times, it is beneficial to download a support report from the device to provide to technical support. This report is a zip file that contains all of the current details for the device's state, and a full record of the system logs from the device.

To obtain a support report from the device, login to the device's local web UI. To access the local web UI, the user must have a PC/laptop connected to the LAN Ethernet port of the 6300-CX and set the interface for a static IP per the instructions here. Once the PC/laptop has an IP address, open the following URL in a browser on the PC:

https://192.168.210.1

Next, go to the *System* page, then click the *Download Report* button at the bottom of the page.

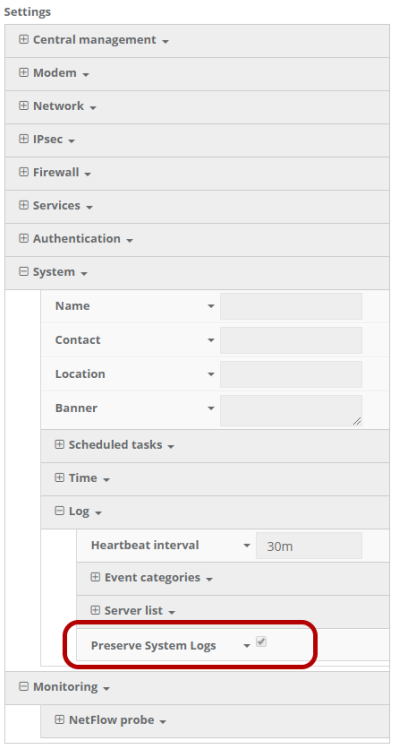


Persistent System Logs

As of December 6th, 2017, the default behavior for all Accelerated Routers is to have persistent system logs disabled. Information logged on the device will be erased when the router is powered off/ rebooted.

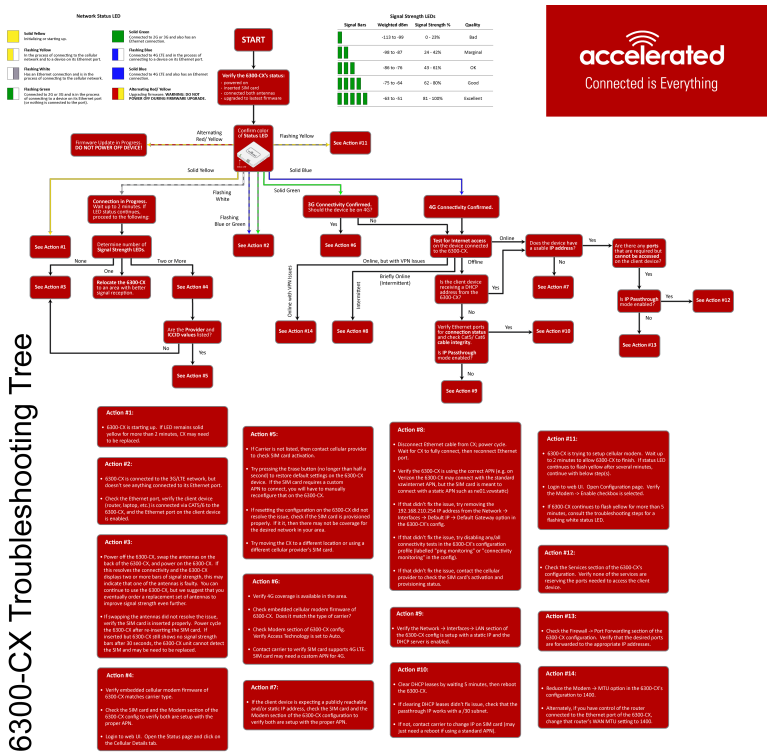
Logging can be configured to persist between power cycles by enabling the **Preserve System Logs** checkbox nested under the **System** → **Log** menu option.

NOTE: Logging across reboots should be enabled only to debug issues and then disabled ASAP to avoid unnecessary wear to the flash memory.



LTE Troubleshooting Tree

6300-CX_Troubleshooting_Flowchart.pdf



Network Status LED

Solid Yellow
Initializing or starting up.

Flashing Yellow
In the process of connecting to the cellular network and to any device on its LAN port(s).

Flashing White
Established LAN connection(s) and is in the process of connecting to the cellular network.

Flashing Green
Connected to 2G or 3G and is in the process of connecting to any device on its LAN port(s), or nothing is connected to the port.

Solid Green
Connected to 2G or 3G and also has a device linked to a LAN port.

Flashing Blue
Connected to 4G LTE and in the process of connecting to a device on its LAN port(s).

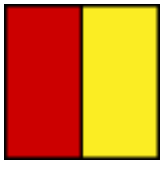
Solid Blue
Connected to 4G LTE and also has a LAN connection.

Alternating Red/ Yellow
Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Signal Strength LEDs

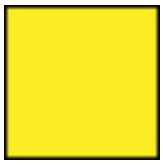
Signal Bars	Weighted dBm	Signal Strength %	Quality
	-113 to -99	0 - 23%	Bad
	-98 to -87	24 - 42%	Marginal
	-86 to -76	43 - 61%	OK
	-75 to -64	62 - 80%	Good
	-63 to -51	81 - 100%	Excellent

Alternating Red/ Yellow



Firmware Update in Progress: DO NOT POWER OFF DEVICE!

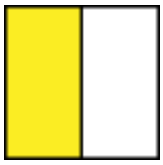
Solid Yellow



6300-CX is starting up.

If LED remains solid yellow for more than 2 minutes, CX may need to be replaced.

Flashing Yellow



6300-CX is trying to setup cellular modem. Wait up to 2 minutes to allow the process to finish. If status LED continues to flash yellow after several minutes, continue with below step(s):

1. Login to web UI. Open Configuration page. Verify the Modem -> Enable check box is selected.
2. If the 6300-CX continues to flash yellow for more than 5 minutes, consult the troubleshooting steps for a flashing white status LED.

Flashing White

Ethernet link detected, connection is in progress.

Wait up to 2 minutes. If LED status continues, determine the number of Signal Strength LEDs:

None

- Power off the 6300-CX, swap the antennas on the back of the 6300-CX, and power on the 6300-CX. If this resolves the connectivity and the 6300-CX displays two or more bars of signal strength, this may indicate that one of the antennas is faulty. You can continue to use the 6300-CX, but we suggest that you eventually order a replacement set of antennas to improve signal strength even further.
- If swapping the antennas did not resolve the issue, verify the SIM card is inserted properly. Power cycle the 6300-CX after re-inserting the SIM card. Wait 30 to 60 seconds. If the problem persists, the 6300-CX unit cannot detect the SIM and the router may need to be replaced.

One

Relocate the 6300-CX to an area with better signal reception.

Two or More

Verify that the embedded cellular modem firmware of the 6300-CX matches carrier type.

Check the SIM card and the Modem section of the 6300-CX config to verify both are setup with the proper APN.

Login to the web UI. Open the Status page and click on the Cellular Details Tab. Are the **Provider** and **ICCID** values listed?

No

- If the proper Carrier is not listed, contact the cellular provider to verify SIM card activation.
- Try pressing the Erase button (no longer than half a second) to restore default settings on the 6300-CX device. If the SIM card requires a custom APN to connect, you will have to manually reconfigure that on the 6300-CX
- If resetting the configuration on the CX did not resolve the issue, check if the SIM card is provisioned properly. If it is, then there may not be coverage for the desired network in your area.
- Try moving the CX to a different location or using a different cellular provider's SIM card.

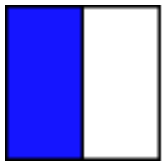
Yes

- Power off the 6300-CX, swap the antennas on the back of the 6300-CX, and power on the 6300-CX. If this resolves the connectivity and the 6300-CX displays two or more bars of signal strength, this may indicate that one of the antennas is faulty. You can continue to use the

6300-CX, but we suggest that you eventually order a replacement set of antennas to improve signal strength even further.

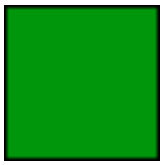
- If swapping the antennas did not resolve the issue, verify the SIM card is inserted properly. Power cycle the 6300-CX after re-insterting the SIM card. Wait 30 to 60 seconds. If the problem persists, the 6300-CX unit cannot detect the SIM and the router may need to be replaced.

Flashing Blue or Green



6300-CX is connected to the 3G/LTE network, but doesn't see anything connected to its Ethernet port. Check the Ethernet port, verify the client device (router, laptop, etc.) is connected via CAT5/6 to the 6300-CX, and the Ethernet port on the client device is enabled

Solid Green



3G connectivity confirmed

Should the device be on 4G?

Yes

- Verify 4G coverage is available in the area.
- Check embedded cellular modem firmware of 6300-CX. Does it match the type of carrier?
- Check Modem section of 6300-CX config. Verify Access Technology is set to Auto.
- Contact carrier to verify SIM card supports 4G LTE. SIM card may need a custom APN for 4G.

No

Test for Internet access on the device connected to the 6300-CX.

Online

Does the device has a usable IP Address?

- If no, see if the client device is expecting a publicly reachable and/or static IP address, check the SIM card and the Modem section of the 6300-CX configuration to verify both are setup with the proper APN.

Are there any ports that are required but cannot be accessed on the client device? Also check if the IP Passthrough has been enabled.

- If yes, check the Services section of the 6300-CX's configuration. Verify none of the services are reserving the ports needed to access the client device.
- If no, check the Firewall -> Port Forwarding section of the 6300-CX configuration. Verify that the desired ports are forwarded to the appropriate IP addresses.

Offline

Is the client device receiving a DHCP address from the 6300-CX?

- If yes, check if the IP Passthrough has been enabled.
  - If yes, are there any ports that are required but cannot be accessed on the client device? Also check if the IP Passthrough has been enabled.
    - If yes, check the Services section of the 6300-CX's configuration. Verify none of the services are reserving the ports needed to access the client device.
    - If no, check the Firewall -> Port Forwarding section of the 6300-CX configuration. Verify that the desired ports are forwarded to the appropriate IP addresses.
  - If no, see if the client device is expecting a publicly reachable and/or static IP address, check the SIM card and the Modem section of the 6300-CX configuration to verify both are setup with the proper APN.
- If no, verify Ethernet ports for connection status and check Cat5/ Cat6 cable integrity. Is IP Passthrough mode enabled?
  - If yes, clear DHCP leases by waiting 5 minutes, then reboot the 6300-CX. If clearing DHCP leases didn't fix issue, check that the passthrough IP works with a /30 subnet. If not, contact carrier to change IP on SIM card (may just need a reboot if using a standard APN).
  - If no, verify the Network → Interfaces→ LAN section of the 6300-CX config is setup with a static IP and the DHCP server is enabled.

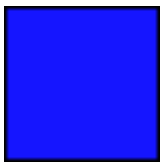
Online, but with VPN issues

Reduce the Modem → MTU option in the 6300-CX's configuration to 1400. Alternately, if you have control of the router connected to the Ethernet port of the 6300-CX, change that router's WAN MTU seting to 1400.

Briefly Online

1. Disconnect Ethernet cable from CX; power cycle. Wait for CX to fully connect, then reconnect Ethernet port.
2. Verify the 6300-CX is using the correct APN (e.g. on Verizon the 6300-CX may connect with the standard vzwinternet APN, but the SIM card is meant to connect with a static APN such as ne01.vzwstatic)
3. If that didn't fix the issue, try removing the 192.168.210.254 IP address from the Network → Interfaces → Default IP → Default Gateway option in the 6300-CX's config.
4. If that didn't fix the issue, try disabling any/all connectivity tests in the 6300-CX's configuration profile (labelled "ping monitoring" or "connectivity monitoring" in the config).
5. If that didn't fix the issue, contact the cellular provider to check the SIM card's activation and provisioning status.

Solid Blue



4G connectivity Confirmed

Test for Internet access on the device connected to the 6300-CX.

Online

Does the device has a usable IP Address?

- If no, see if the client device is expecting a publicly reachable and/or static IP address, check the SIM card and the Modem section of the 6300-CX configuration to verify both are setup with the proper APN.

Are there any ports that are required but cannot be accessed on the client device? Also check if the IP Passthrough has been enabled.

- If yes, check the Services section of the 6300-CX's configuration. Verify none of the services are reserving the ports needed to access the client device.
- If no, check the Firewall -> Port Forwarding section of the 6300-CX configuration. Verify that the desired ports are forwarded to the appropriate IP addresses.

Offline

Is the client device receiving a DHCP address from the 6300-CX?

- *If yes*, check if the IP Passthrough has been enabled.
  - If yes, are there any ports that are required but cannot be accessed on the client device? Also check if the IP Passthrough has been enabled.
    - *If yes*, check the Services section of the 6300-CX's configuration. Verify none of the services are reserving the ports needed to access the client device.
    - *If no*, check the Firewall -> Port Forwarding section of the 6300-CX configuration. Verify that the desired ports are forwarded to the appropriate IP addresses.
  - If no, see if the client device is expecting a publicly reachable and/or static IP address, check the SIM card and the Modem section of the 6300-CX configuration to verify both are setup with the proper APN.
- *If no*, verify Ethernet ports for connection status and check Cat5/ Cat6 cable integrity. Is IP Passthrough mode enabled?
  - If yes, clear DHCP leases by waiting 5 minutes, then reboot the 6300-CX. If clearing DHCP leases didn't fix issue, check that the passthrough IP works with a /30 subnet. If not, contact carrier to change IP on SIM card (may just need a reboot if using a standard APN).
  - If no, verify the Network → Interfaces→ LAN section of the 6300-CX config is setup with a static IP and the DHCP server is enabled.

Online, but with VPN issues

Reduce the Modem → MTU option in the 6300-CX's configuration to 1400. Alternately, if you have control of the router connected to the Ethernet port of the 6300-CX, change that router's WAN MTU seting to 1400.

Briefly Online

1. Disconnect Ethernet cable from CX; power cycle. Wait for CX to fully connect, then reconnect Ethernet port.
2. Verify the 6300-CX is using the correct APN (e.g. on Verizon the 6300-CX may connect with the standard vzwinternet APN, but the SIM card is meant to connect with a static APN such as ne01.vzwstatic)
3. If that didn't fix the issue, try removing the 192.168.210.254 IP address from the Network → Interfaces → Default IP → Default Gateway option in the 6300-CX's config.

4. If that didn't fix the issue, try disabling any/all connectivity tests in the 6300-CX's configuration profile (labelled "ping monitoring" or "connectivity monitoring" in the config).
5. If that didn't fix the issue, contact the cellular provider to check the SIM card's activation and provisioning status.

Advanced Configuration Using Accelerated View™

The following Accelerated View actions are typically only performed by your network administrator.

Using Accelerated View to centrally manage your device is recommended. If you are not using Accelerated View, you must manage and configure your device using the local interface. Refer to **Managing Device Locally** section for more information.

Viewing & Editing Configuration

To access the configuration for your device:

1. Login to Accelerated View and use the Search tool to search by MAC address.
2. Select the MAC address of your 6300-CX to bring up its Details page.
3. Select View Configuration in the Configuration section.
4. Select the Edit pencil icon at the top right of the page to make changes.

The 6300-CX will automatically support configuration updates after the next daily sync around 1AM UTC. To apply changes sooner than the next scheduled sync refer to the **Remote Commands** section for details on how to send a remote command.

Upgrading Firmware

To upgrade the firmware on your device:

1. Login to Accelerated View and use the Search tool to find the device by searching for its MAC address.
2. Select the MAC address of the device to bring up its details page.
3. Click on the **Settings** tab, then select the **View Configuration** link in the **Configuration** section of the page.
4. Once viewing the configuration profile, select the Edit pencil icon at the top right of the page.
5. Select the appropriate firmware version from the Firmware drop-down list.
6. Click the Update button.

Defining a Custom APN

If your device is unable to sync with Accelerated View because the device **cannot** establish a cellular connection without a custom APN refer to **Managing Device Locally** section.

1. Login to Accelerated View and use the Search tool to find the 6300-CX by searching for its MAC address.
2. Select the MAC address of the 6300-CX to bring up its details page.

3. Select the View Configuration link in the Configuration section of the page.
4. Once viewing the configuration profile, select the Edit pencil icon at the top right of the page.
5. Type in the custom APN into the APN entry located in the Modem section of the configuration.
6. Optional: If the custom APN requires a specific username and password, please input those into the Username and Password entries located in the Modem section of the configuration.
7. Click the Update button.

Using Remote Commands

The Accelerated View management portal allows you to send a specific set of remote commands to the device to provide control over the device without requiring any onsite interaction. These remote commands allow you to perform actions such as rebooting the device, triggering a configuration sync with Accelerated View, perform network speed tests, immediately probing the device for a real-time status, and more.

To send a remote command to an Accelerated 6300-CX:

1. Login to Accelerated View and use the Search tool to find the device by searching for its MAC address.
2. Select the MAC address of the device to bring up its details page.
3. Select the **Commands** drop-down list at the top-right of the page.

Immediately Update Device

1. Select Remote Commands.
2. Select Check Configuration option from the Commands drop-down.

Establishing WAN connectivity via Ethernet Port

In order to provide a cellular connection to client devices, the Accelerated 6300-CX can be configured either in the default Passthrough (i.e. bridge) mode or DHCP Server/Router mode.

Passthrough/Bridge Mode

In this default mode, the device operates as a transparent bridge and all traffic on all ports is passed directly to and from the client device connected to the device's Ethernet port. In Passthrough mode, a single IP address will be available through the device's Ethernet port. Only one client device can be connected to the Accelerated 6300-CX through its Ethernet port at a time.

1. Login to Accelerated View and use the Search tool to find the device by searching for its MAC address.

2. Select the MAC address of the device to bring up its details page.

3. Select the View Configuration link in the Configuration section of the page.

4. Once viewing the configuration profile, select the Edit pencil icon at the top right of the page.

5. Under the **Modem** section of the configuration, open the Passthrough section and set the following options inside that section:

a. Check **Enable**.

b. Change **Device** to **LAN**.

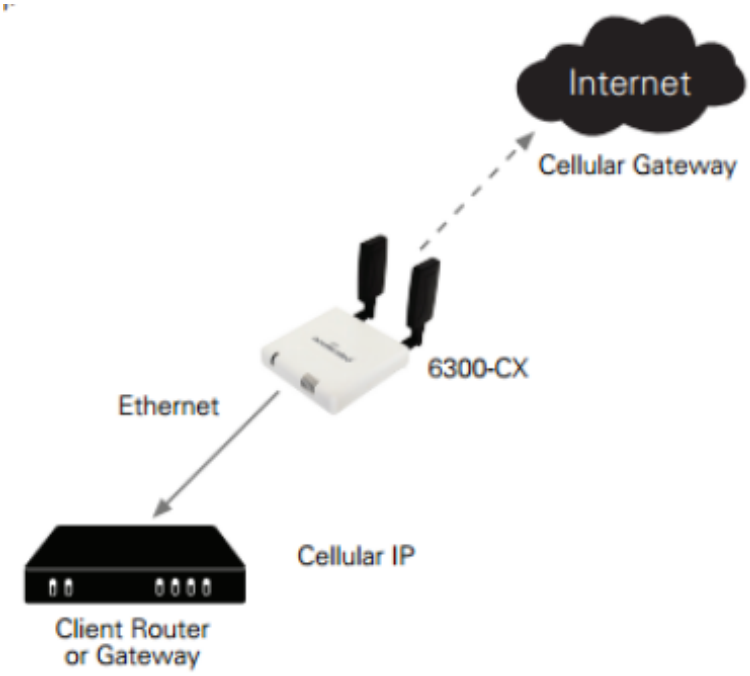
c. Change **Zone** to **Internal.**

6. Change the Interface Type under the **LAN** network section from **DHCP** to **Static IP Address**.

7. In the **Address**, enter in the IP address you wish to assign to the device for its LAN DHCP network (i.e. the gateway IP for the DHCP network).

8. Open the **DHCP Server** section and select **Disable**.

9. Click **Save** to apply the configuration changes.



Sample Diagram showing Passthrough Mode

Router Mode

In this mode, the device operates as a standard DHCP router. The device will be configured to hand out a range of LAN IP addresses to client devices connected on its Ethernet port. Standard router options are available in the device's configuration, including DHCP lease options, DNS options, firewall options, and port forwarding rules.

The following list of steps details how to setup a simple DHCP server on the device in router mode.

1. Login to Accelerated View and use the Search tool to find the device by searching for its MAC address.

2. Select the MAC address of the device to bring up its details page.

3. Select the View Configuration link in the **Configuration** section of the page.

4. Once viewing the configuration profile, select the green Edit pencil icon at the top right of the page.

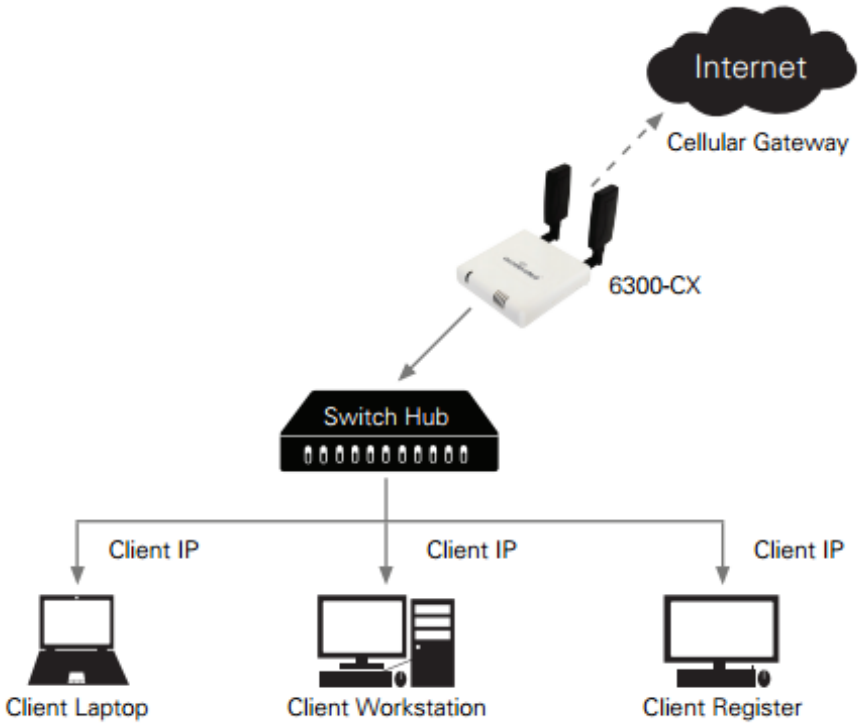
5. Open the **Modem** -> **Passthrough** section, de-select the **Enable** checkbox.

6. Change the **Network** -> **Interfaces** -> **LAN** -> **IPv4** -> **Interface Type** option from **DHCP** to **Static IP Address**.

7. In the **Network** -> **Interfaces** -> **LAN** -> **IPv4** -> **Address** option, enter in the IP address you wish to assign to the device for its LAN DHCP network (i.e. the gateway IP for the DHCP network).

8. Open the **Network** -> **Interfaces** -> **LAN** -> **IPv4** -> **Address** -> **DHCP Server** section and select **Enable**.

9. Click **Save** to apply the configuration changes.



Sample Diagram showing Router Mode

Learning More

In depth details on using Accelerated View can be found in the Accelerated View User's Guide.

AT Command Access

To gain AT command access through the 6300-CX, the tester must have a PC/laptop connected the LAN Ethernet port of the 6300-CX. They will need to configure a static IP on the PC/laptop of 192.168.210.2/24 with a gateway of 192.168.210.1

- Open a SSH session to the 6300-CX at 192.168.210.1. Default login credentials are:
  - *username:* root
  - *password:* default
- Select **a** to access the Admin CLI. If the SSH session immediately gives you the # prompt, you are already in the Admin CLI.
- Type **atcmd** and press Enter. Type **n** when the SR prompts you if you want exclusive access. This allows you to send AT commands to the device while still allowing the device to connect, disconnect, and/or reconnect to the Sprint network.
- Example AT command access below:

```
$ ssh root@192.168.210.1
Password:

Access selection menu:

a: Admin CLI
s: Shell
q: Quit

Select access or quit [admin] : a

Connecting now, 'exit' to disconnect from Admin CLI ...

# atcmd

Do you want exclusive access to the modem? (y/n) [y]: n
Starting terminal access to modem AT commands.
Note that the modem is still in operation.

To quit enter '~.' ('~~.' if using an ssh client) and press ENTER

Connected
ati
Manufacturer: Sierra Wireless, Incorporated
Model: MC7354
Revision: SWI9X15C_05.05.16.02 r21040 carmd-fwbuild1 2014/03/17 23:49:48
MEID: 35922505082765
ESN: 12803341918, 8032FE5E
IMEI: 359225050827658
```

```
IMEI SV: 11
FSN: J8513103240310
+GCAP:
```

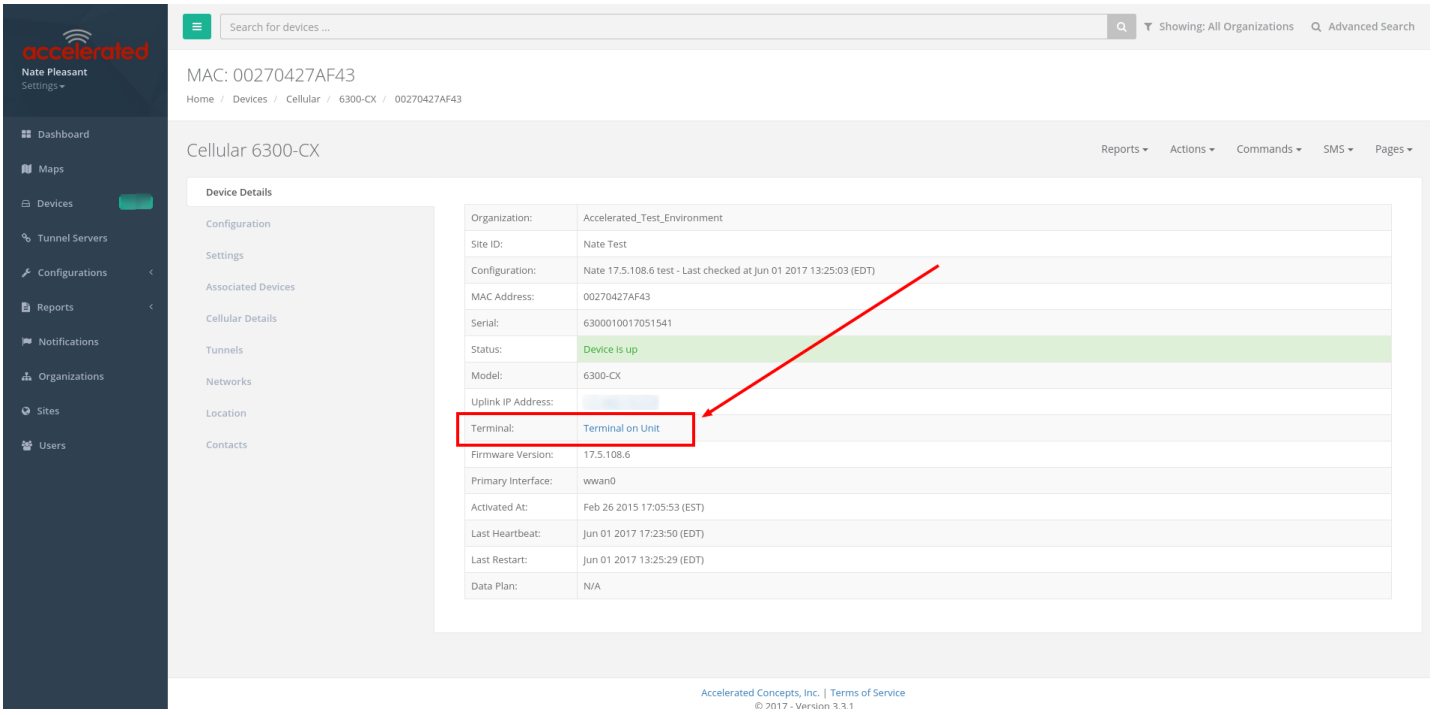
Terminal on Unit

Skill level: *Intermediate*

Goal

To access the console of an Accelerated LTE router using the *Terminal on Unit* link presented in Accelerated View for the device.

> The *Terminal on Unit* access leverages the management tunnel established between the 63xx-series router and Accelerated View. For details on the monthly data usage for this access, refer to the following article:
>
> Data Usage Estimates



Setup

For this setup, you will need access to Accelerated View, and a 63xx-series router online and syncing with Accelerated View. If you see the 63xx-series router listed as up (green status) in Accelerated View, you are good to go.

Details

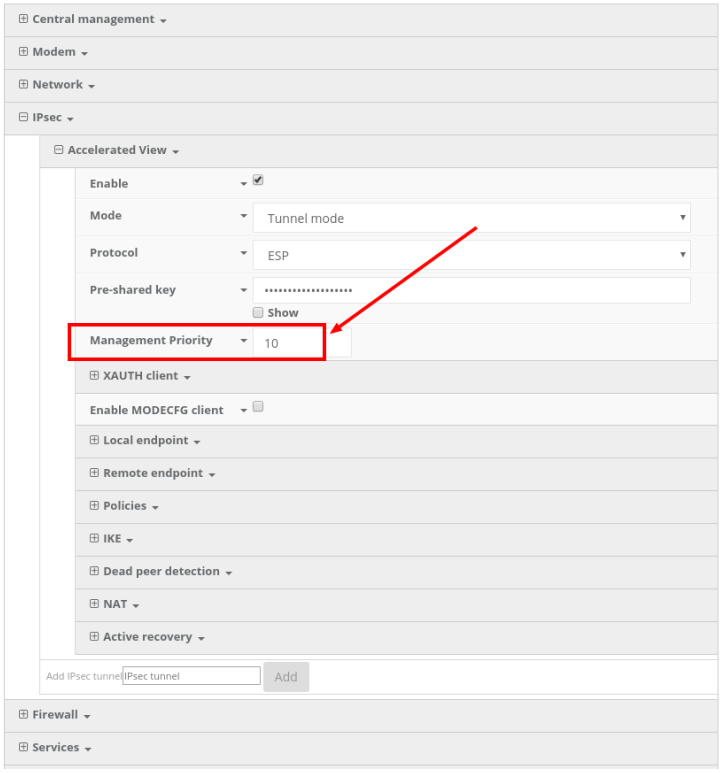
Accelerated View utilizes the IPSec tunnel the 63xx-series router establishes to remote.accns.com to provide terminal access to the console of the router.

For details on the monthly data usage for this access, refer to the following article:

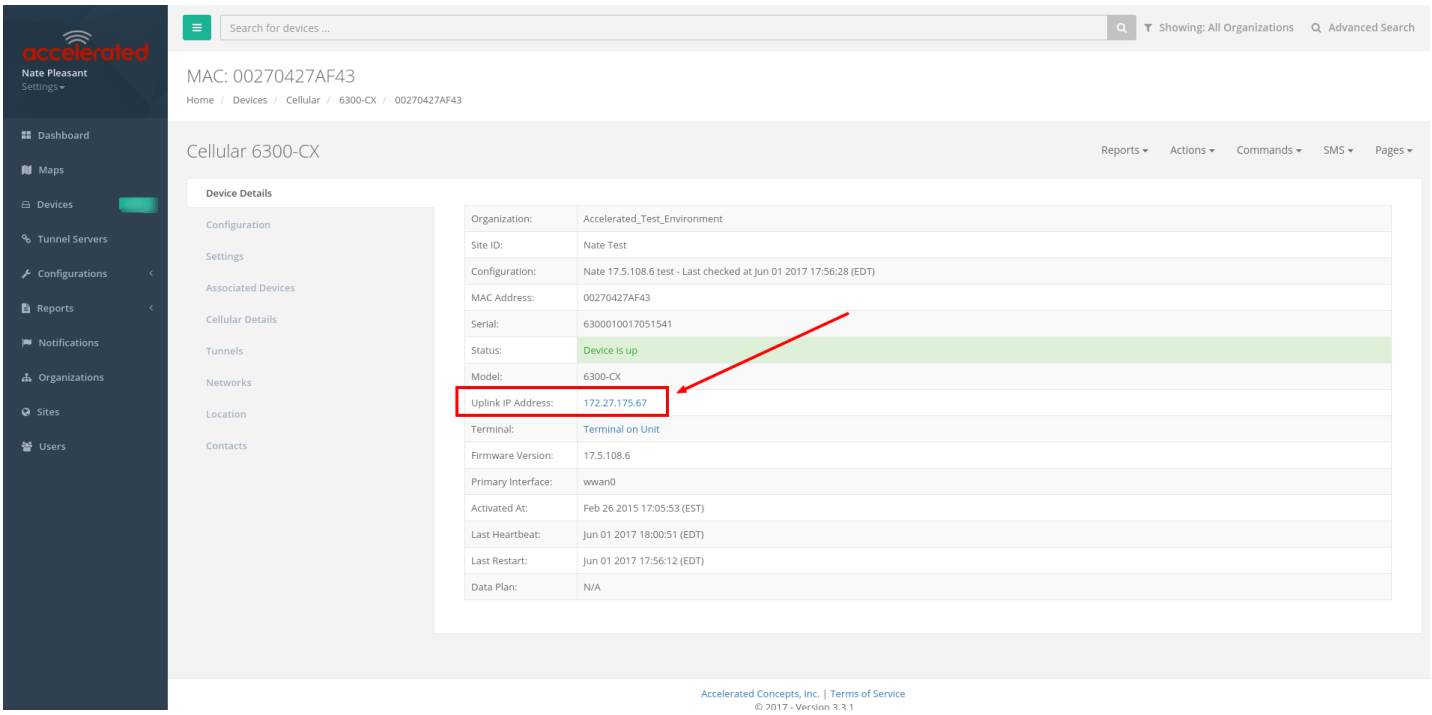
Data Usage Estimates

The following configuration settings will setup the 6300-CX to report its IPSec tunnel local IP address as the management IP that Accelerated View can then use to access its console.

Open the configuration profile for the 63xx-series router. Under *IPSec -> Accelerated View*, set the *Management priority* to *10*. This will tell the 63xx-series router to treat the AView IPSec tunnel as the highest priority management interface, which it then reports to Accelerated View as the IP that can be used to access its console.



Once you apply the new configuration to the 63xx-series router, reboot the 63xx-series device so it rebuilds the IPSec tunnel and reports the new IPSec local IP address to Accelerated View. You can verify that Accelerated View is using the IPSec local IP as the management IP by looking at the *Uplink IP address* on the *Device Details* tab. This value should be set to a 172.x.x.x IP address.



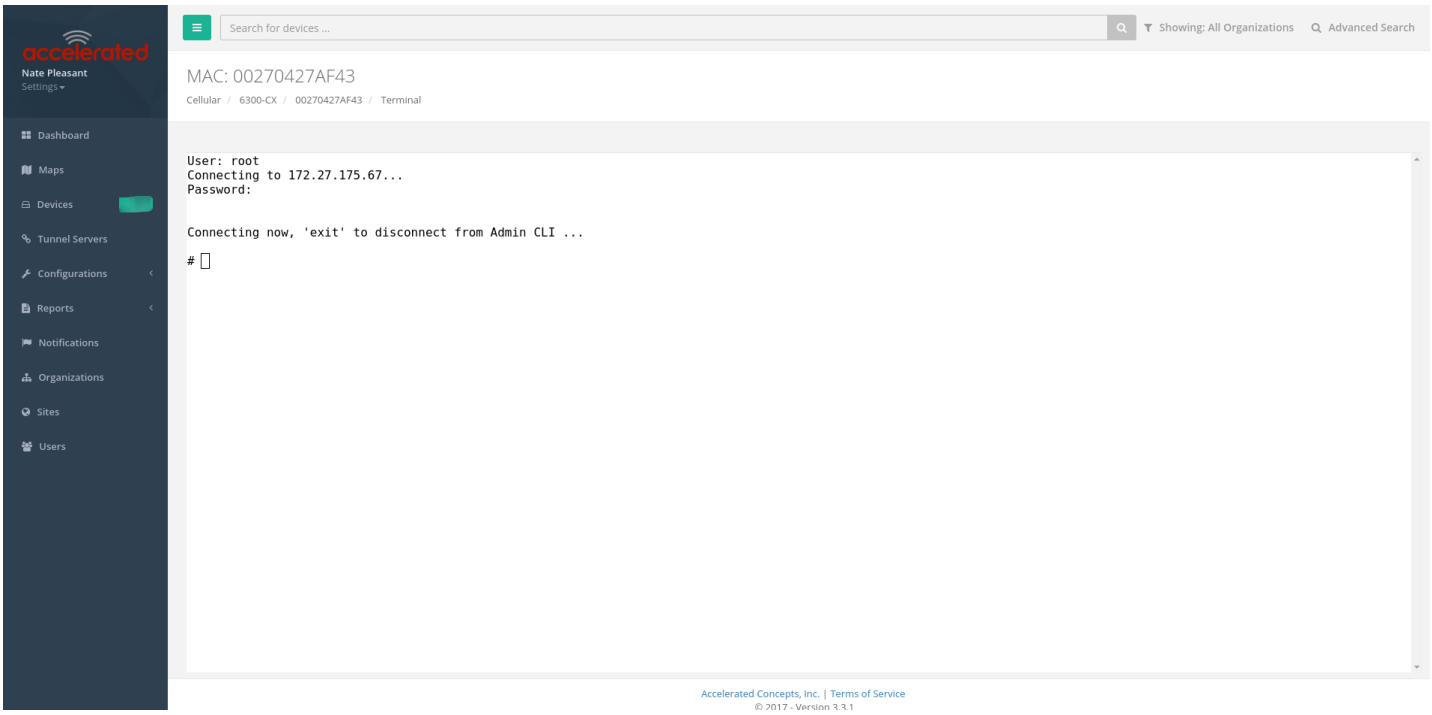
Using the Terminal on Unit link

Once the correct management IP is reported from the 63xx-series router to Accelerated View, clicking the *Terminal on Unit* will open a page on Accelerated View to provide the user access to the console of the 63xx-series router. Default login credentials are below.

User: root

Password: default

To create a different user or change the root user's password, refer to this article.



There is a known issue where the predictive/auto-correct feature of the Google keyboard renders it incompatible with the Terminal page. If you are access the above Terminal with an Android phone or tablet, you will need to use a different keyboard other than the native Google keyboard.

Managing Device Locally

The following Accelerated View actions are typically only performed by your network administrator. Note: Using Accelerated View to centrally manage your device is recommended. If you are not using Accelerated View, you must manage and configure your device using the local interface.

Connecting to the Device

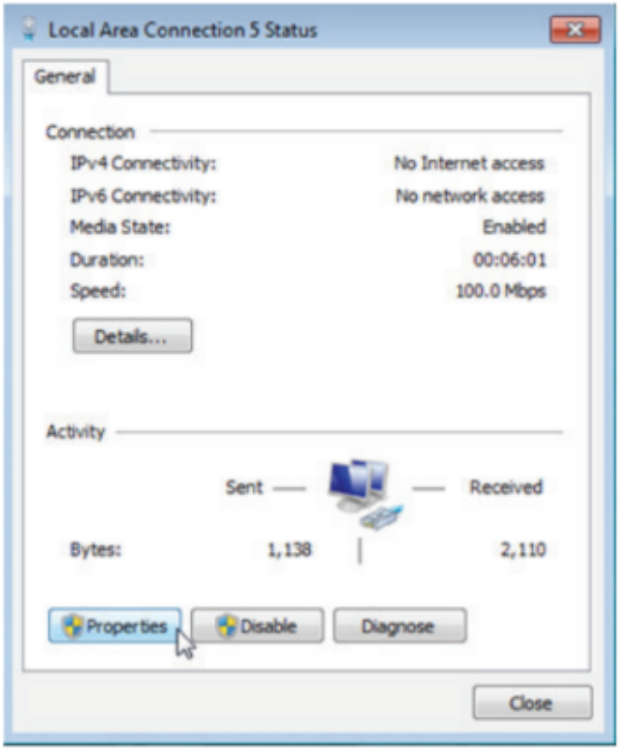
Communication with the device is typically via its Ethernet port. By default, you can connect to the device via its Ethernet port, at the IP address 192.168.210.1. You can access the device via this default IP address using a PC connected to its Ethernet port.

When connected to your site network, your Accelerated 6300-CX will attempt to use DHCP to establish a connection and obtain an IP address. If a DHCP server is operating on the site network then the device will receive an IP address configuration from the local network. You can also access the device using the IP address provided in the DHCP connection

Manually Configuring PC to Connect to Device

To manually connect to the device, you must manually set an IP address on your PC to be able to communicate with the Accelerated 6300-CX.

1. Select the Properties of the relevant network connection on the Windows PC.

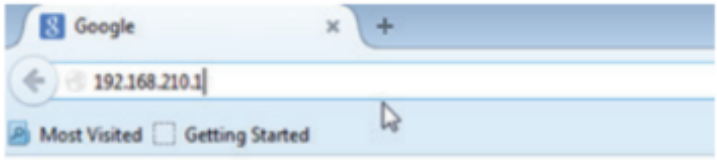


2. Click the Internet Protocol Version 4 (TCP/IPv4) parameter and select Properties and configure with the following details.

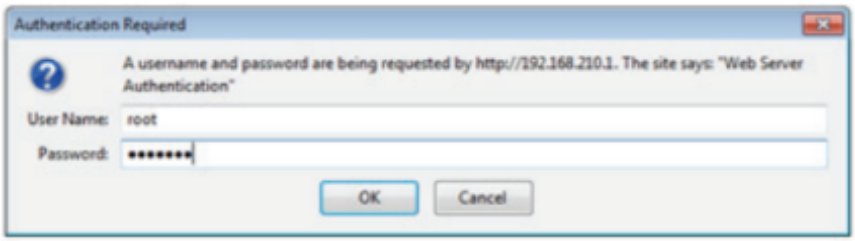
Logging into Device

To manually connect to the device, you must manually set an IP address on your PC to be able to communicate with the Accelerated 6300-CX.

1. Open the web browser on the PC and type in the address bar, the IP address of the Accelerated 6300-CX (192.168.210.1) and hit Enter.



2. When prompted Enter - User Name: **root** Password: **default**.



3. The Accelerated 6300-CX default web user interface will be shown.

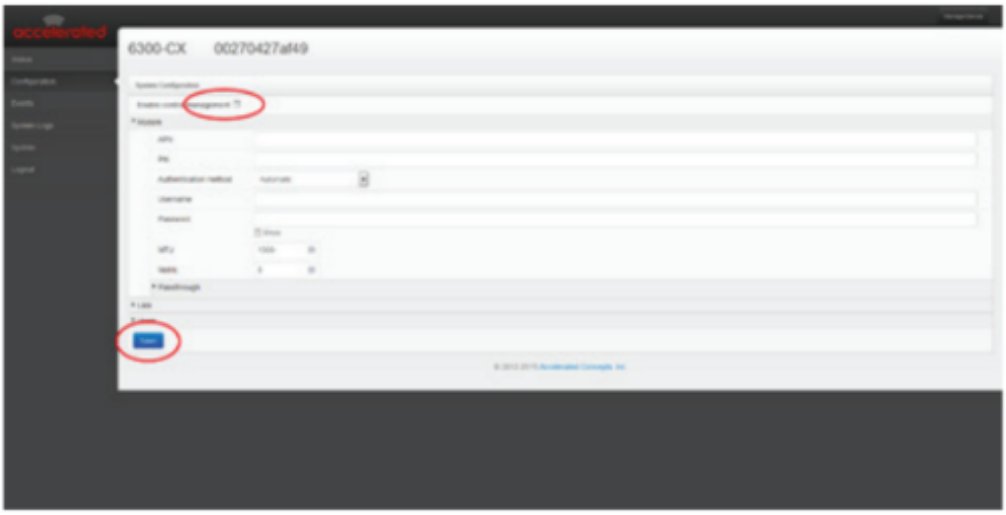
Advanced Local Configuration

Once logged in via the local web interface you must enable local management of the device to modify settings for the Cellular and Ethernet interfaces.

1. Uncheck box next to "**Enable central management**"

2. Click **Save**.

After saving the profile, the device will no longer attempt to sync with Accelerated View and a full range of available configuration options will be visible. 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.



Upgrading Firmware

1. Download the appropriate firmware file from Accelerated.
2. Connect to the device's web UI by connecting your PC to the WAN Ethernet port of the device and then going to http://192.168.210.1.
3. Select the System tab on the left side of the page.
4. Select the Browse button next to the Firmware image section.
5. Browse for and select the downloaded firmware file.

6. Click the Update Firmware button.

Do not turn off or unplug the device while it is upgrading its firmware. The upgrade process should take less than one minute.

Defining a Custom APN

1. Connect to the device's web UI by connecting your PC to the WAN Ethernet port of the device and then going to http://192.168.210.1. If the device does not give your PC an IP address via DHCP, you may need to configure your PC with the following static IP settings. IP address for PC: 192.168.210.2 Subnet: 255.255.255.0 Gateway: 192.168.210.1
2. Select the Configuration tab on the left side of the page.
3. Type in the custom APN into the APN entry located in the modem section of the configuration.
4. Optional: If the custom APN requires a specific username and password, please input those into the Username and Password entries.
5. Click the Save button.

FAQS

How do I factory reset the Accelerated 6300-CX?

1. Ensure that the device has been powered on for at least 30 seconds.
2. Briefly press the Erase button located on the back of the device.

What IP address does the Accelerated 6300-CX use?

By default, the Accelerated 6300-CX will use 192.168.210.1. You can access the device through its WAN Ethernet port using this IP address.

What size SIM card does the Accelerated 6300-CX use?

The Accelerated 6300-CX supports standard mini-SIMs (2FF).

How do I insert a SIM into the Accelerated 6300-CX?

With the power disconnected, the SIM card should be inserted notch-end first with the gold contacts face down. The SIM slot is located on the back of the Accelerated 6300-CX between the power connector and the USB port. The SIM will click into place when fully inserted.

Does the Accelerated 6300-CX fail back to 3G?

Yes, if the Accelerated 6300-CX doesn't recognize a 4G/LTE network available, the device will automatically fallback to the highest available 3G network. Supported networks include DC-HSPA+, HSPA+, HSPA, EDGE, GPRS, GSM and CDMA.

Does the Accelerated 6300-CX support IPv6?

Yes. In passthrough mode, when the 6300-CX receives an IPv6 prefix from the cellular network, it uses SLAAC to pass the prefix to the client device connected to its Ethernet port. The 6300-CX will also pass the IPv6 DNS server using the SLAAC RDNSS option and stateless DHCPv6.

Regulatory Guide

FCC

THIS EQUIPMENT HAS BEEN TESTED AND FOUND TO COMPLY WITH THE LIMITS FOR A CLASS A DIGITAL DEVICE, PURSUANT TO PART 15 OF THE FCC RULES. THESE LIMITS ARE DESIGNED TO PROVIDE REASONABLE PROTECTION AGAINST HARMFUL INTERFERENCE WHEN THE EQUIPMENT IS OPERATED IN A COMMERCIAL ENVIRONMENT. THIS EQUIPMENT GENERATES, USES, AND CAN RADIATE RADIO FREQUENCY ENERGY AND, IF NOT INSTALLED AND USED IN ACCORDANCE WITH THE INSTRUCTION MANUAL, MAY CAUSE HARMFUL INTERFERENCE TO RADIO COMMUNICATIONS. OPERATION OF THIS EQUIPMENT IN A RESIDENTIAL AREA IS LIKELY TO CAUSE HARMFUL INTERFERENCE IN WHICH CASE THE USER WILL BE REQUIRED TO CORRECT THE INTERFERENCE AT HIS OWN EXPENSE. INDUSTRY CANADA - CAN ICES-3(A)/NMB-3(A) THIS PRODUCT IS INTENDED FOR OPERATION IN A COMMERCIAL OR INDUSTRIAL ENVIRONMENT AND SHOULD NOT BE USED IN A RESIDENTIAL ENVIRONMENT. THIS PRODUCT HAS BEEN TESTED AND FOUND TO COMPLY WITH THE REQUIREMENTS OF: ICES-003 - INFORMATION TECHNOLOGY EQUIPMENT - LIMITS AND METHODS OF MEASUREMENT ISSUE 5, AUGUST 2012.

European Union

THIS PRODUCT MAY CAUSE INTERFERENCE IF USED IN RESIDENTIAL AREAS. SUCH USE MUST BE AVOIDED UNLESS THE USER TAKES SPECIAL MEASURES TO REDUCE ELECTROMAGNETIC EMISSIONS TO PREVENT INTERFERENCE TO THE RECEPTION OF RADIO AND TELEVISION BROADCASTS.

Supported Countries

FOR A FULL LIST OF CERTIFIED COUNTRIES GO TO: WWW.ACCELERATED.COM/COUNTRIES/6300-CX

End User Agreement

ACCELERATED CONCEPTS, INC. END USER AGREEMENT (v20160613.01)

USE OF THIS PRODUCT IS YOUR ACCEPTANCE TO THE ACCELERATED CONCEPTS, INC. END USER AGREEMENT FOUND AT: HTTPS://ACCELERATED.COM/ENDUSERAGREEMENT

LIMITED WARRANTY

Accelerated Concepts, Inc. (“ACI”) provides the Limited Warranty set forth herein on ACI’s VPN and Cellular products (“Product” or “Products”) to the original purchaser (hereinafter referred to as the “End User”) who purchased Products directly from ACI or one of its authorized resellers. This Limited Warranty does not apply to Products purchased from third-parties who falsely claim to be ACI resellers. Please visit our web site if you have questions about authorized resellers.

This Limited Warranty becomes invalid once the End User no longer owns the Product, if the Product or its serial number is altered in any manner, or if any repair or modification to the Product is made by anyone other than an ACI approved agent.

This Limited Warranty covers the Product against defects in materials and workmanship encountered in normal use of the Product as set forth in the Product’s Users Guide for one (1) year from the date of purchase. This Limited Warranty is not intended to include damage relating to shipping, delivery, installation, applications and uses for which the Product was not intended; cosmetic damage or damage to the Product’s exterior finish; damages resulting from accidents, abuse, neglect, fire, water, lighting or other acts of nature; damage resulting from equipment, systems, utilities, services, parts, supplies, accessories, wiring, or software applications not provided by ACI for use with the Product; damage cause by incorrect electrical line voltage, fluctuations, surges; customer adjustments, improper cleaning or maintenance, or a failure to follow any instruction provided in the Product’s Users Guide. This list is not intended to cover every possible limitation to this Limited Warranty. ACI does not warrant against totally uninterrupted or error-free operation of its Products.

In order to obtain warranty service under this Limited Warranty during the Limited Warranty period as set forth above, you must submit a valid claim through ACI’s return merchandise authorization (“RMA”) process as follows:

End User must request an RMA number either from Accelerated support or by sending an e-mail to RMA@accelerated.com with the following information:

1. Your name, address and e-mail address
2. The Product model number and serial number
3. A copy of your receipt
4. A description of the problem

ACI will review your request and e-mail you either an RMA number and shipping instructions or a reason why your request was rejected. Properly pack and ship the Product to ACI with the RMA number written on the outside of each package. ACI will not accept any returned Products which are not accompanied by an RMA number. ACI will use commercially reasonable efforts to ship a replacement device within ten (10) working days after receipt of the Product. Actual delivery times may vary depending on shipment location. Products returned to ACI must conform in quantity and serial number to the RMA request. End User will be notified by e-mail by ACI in the event of any incomplete RMA shipments.

Products presented for repair under this Limited Warranty may be replaced by refurbished goods of the same type rather than being repaired. Refurbished or used parts may be used to repair a Product covered by this Limited Warranty. If ACI, by its sole determination, is unable to replace a Product covered by this Limited Warranty, it will refund the depreciated purchase price of the Product.

LIMITED LIABILITY

EXCEPT AS PROVIDED IN THE LIMITED WARRANTY AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, UNDER NO CIRCUMSTANCES WILL ACI BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING, BUT NOT LIMITED TO, COMPENSATION, REIMBURSEMENT OR DAMAGES ON ACCOUNT OF THE LOSS OF PRESENT OR PROSPECTIVE PROFITS, EXPENDITURES, INVESTMENTS OR COMMITMENTS, WHETHER MADE IN THE ESTABLISHMENT, DEVELOPMENT OR MAINTENANCE OF BUSINESS REPUTATION OR GOODWILL, FOR LOSS OR DAMAGE OF RECORDS OR DATA, COST OF SUBSTITUTE PRODUCTS, COST OF CAPITAL, THE CLAIMS OF ANY THIRDPARTY, OR FOR ANY OTHER REASON WHATSOEVER.

ACI'S LIABILITY, IF ANY, AND THE END USER'S SOLE AND EXCLUSIVE REMEDY FOR DAMAGES FOR ANY CLAIM OF ANY KIND WHATSOEVER REGARDLESS OF THE LEGAL THEORY, SHALL NOT BE GREATER THAN THE PRODUCT'S ACTUAL PURCHASE PRICE.

THIS LIMITATION OF LIABILITY IS APPLICABLE EVEN IF ACI IS INFORMED IN ADVANCE OF THE POSSIBILITY OF DAMAGES BEYOND THE PRODUCT'S ACTUAL PURCHASE PRICE.

SOFTWARE LICENSE

ACI software is copyrighted and is licensed to the End User solely for use with the Product.

Some software components are licensed under the GNU General Public License, version 2. Please visit http://www.gnu.org/licenses/old-licenses/gpl-2.0.en. html for more details regarding GNU GPL version 2.

These GNU General Public License, version 2 software components are available as a CD or download. The CD may be obtained for an administration fee by contacting Accelerated support at support@accelerated.com.

VPN Access with IPSec tunnels

Skill level: ***Expert*** (requires knowledge of IPSec tunnel setup)

Goal

To build an IPSec tunnel through the 63xx router's WAN internet connection, and use that IPSec tunnel to access endpoints inside a VPN.

Setup

For this setup, the 63xx series router will need an active WAN internet connection (cellular for the 6300-series, cellular or Ethernet for the 635x-SR series).

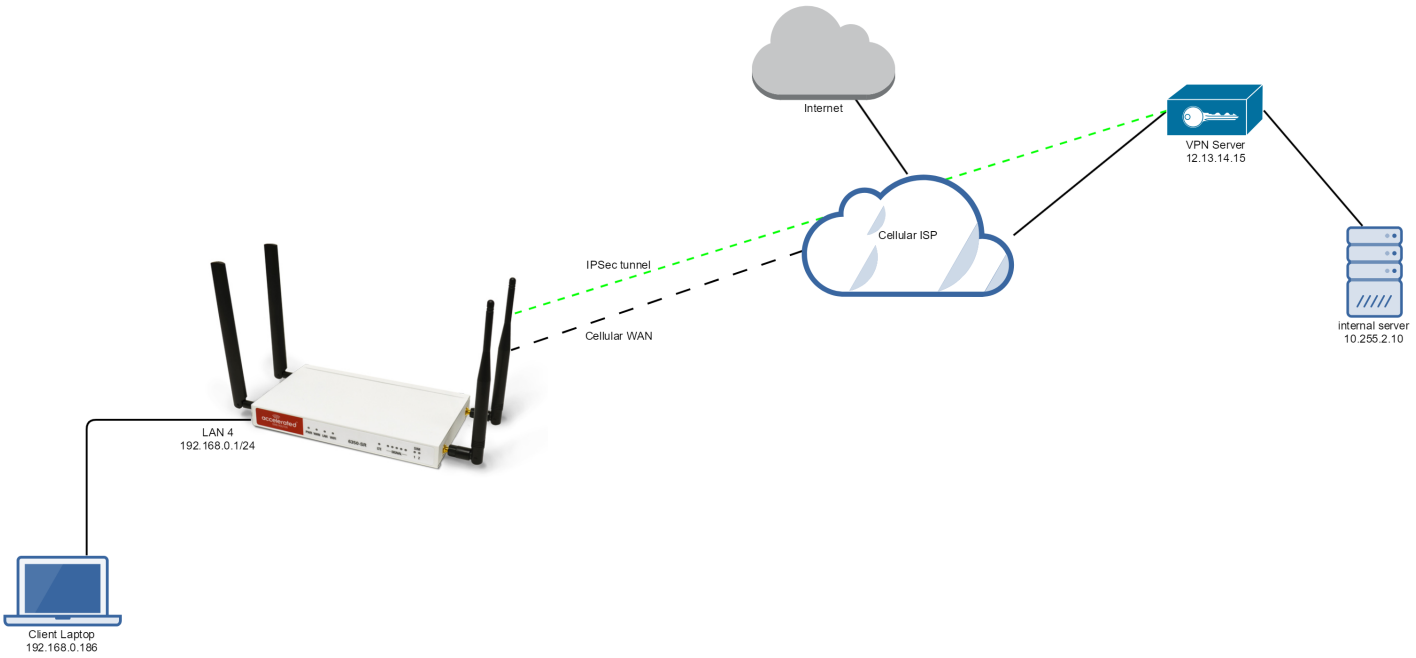
You will also need to know the IPSec credentials and settings needed to build a tunnel to the IPSec endpoint.

NOTE: the 63xx series of routers support building IPSec tunnels to the following endpoints:

- SonicWall routers
- strongswan IPSec servers
- OpenVPN IPSec servers
- other 63xx series routers. See the site-to-site tunnel article for an example.

Sample

The sample configuration below shows a 6350-SR building a tunnel to a VPN server at 12.13.14.15 through it's cellular modem. The client laptop connected to the LAN Ethernet port of the 6350-SR can then use that IPSec tunnel to access any IP address in the 10.255.0.0/16 range behind the IPSec server. Any traffic not destined for 10.255.0.0/16 will instead go through the cellular modem straight to the Internet.



Sample Configuration

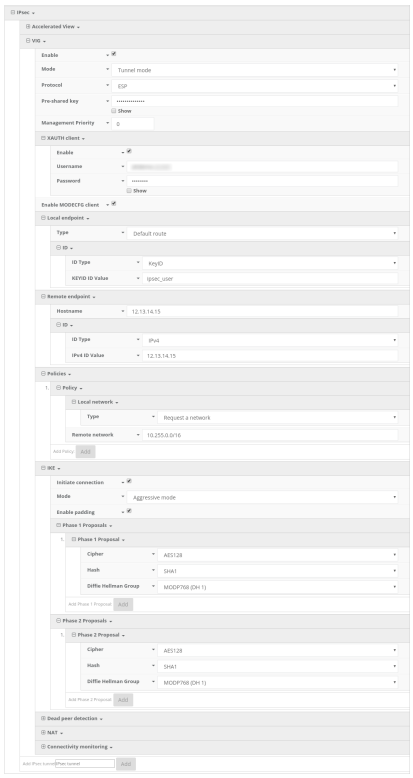
Open the configuration profile for the 6350-SR. Under *IPSec*, create a new entry titled *Tunnel*, and add your IPSec settings to the new entry. The following settings reflect the sample setup in the diagram above.

1. Enter in the PSK into the *Pre-shared key*.
2. (o*ptional*) In *XAUTH client*, check the *Enable* box and enter in the account, username, and password.
3. Check the *Enable MODECFG client* box.
4. Change *Local endpoint -> ID -> ID type* to *KeyID*
5. Set the local ID in *Local endpoint -> ID -> KEYID ID Value*
6. *(optional)* Set *Local endpoint -> type* to *Interface*,and set *Local endpoint -> Interface* to *Modem.* This configures the 63xx-series router to only build the tunnel through the cellular modem WAN interface. Leaving *Local endpoint -> type* to *Interface* as *Default route* will allow the tunnel to be built through any available WAN interface.
7. Change *Remote endpoint -> ID -> ID type* to *IPv4*
8. Set the IP address of the IPSec server in *Remote endpoint -> Hostname* and *Remote endpoint -> ID -> IPv4 ID Value*. In the example, this is 12.13.14.15
9. Set *IKE -> Mode* to *Aggressive mode*.
10. Set *IKE -> Phase 1 Proposals* and *IKE -> Phase 2 Proposals* to match the IKE settings required by the IPSec server. In this example, both proposals are set to AES128, SHA1, MOD768.

Under *Policies*, click *Add* to create a new policy, and enter the following settings:

1. Set *Policy -> Local network -> Type* to *Request a network.*
2. Set *Policy -> Remote network* to the IPv4 network you wish to access through the tunnel. In the sample, this is 10.255.0.0/16

(alternative) If you would instead like to have all outbound traffic go through this tunnel, set ***Policy -> Remote network*** to ***0.0.0.0/0***



VLAN Trunking

Skill level: *Moderate*

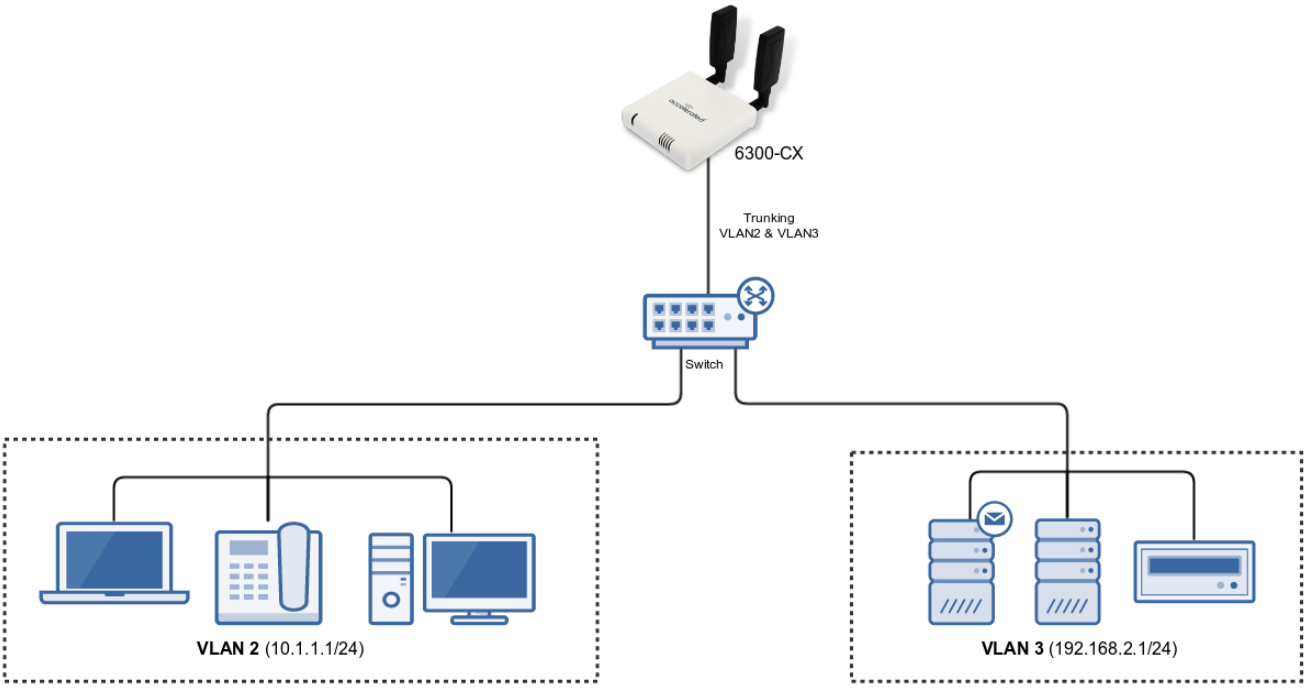
Goal

The primary benefit of the VLAN features on the 6300-CX is to provide multiple LAN networks on a single Ethernet port. This allows users to create a segmented network, where certain devices are sectioned off in their own network, for increased performance, improved manageability, simplified software configurations, and increased security options.

Technical Details

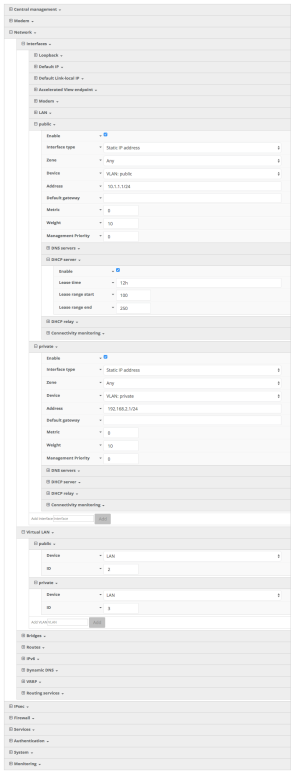
What the 6300-CX and 6300-LX supports is closest to a trunked VLAN behavior. That is, the 6300-CX supports multiple VLANs per Ethernet port, the packets arrive with tags already, and it doesn't add tags to the incoming packets. The difference is that since the 6300-CX acts as a router, we can't forward the tag on. The Ethernet header and VLAN tag are stripped before the packet enters the IP stack. So to the IP stack, it appears as the packet appeared on a virtual interface called "eth0.%d", and it needs to decide how to route the packet based on that. There's no concept of a trunk interface that sends and receives all VLAN tags. The outgoing packet will then only have a VLAN tag if it is being routed out one of these virtual interfaces, and this VLAN tag doesn't have to be the same as the VLAN tag on the incoming packet.

Example Setup



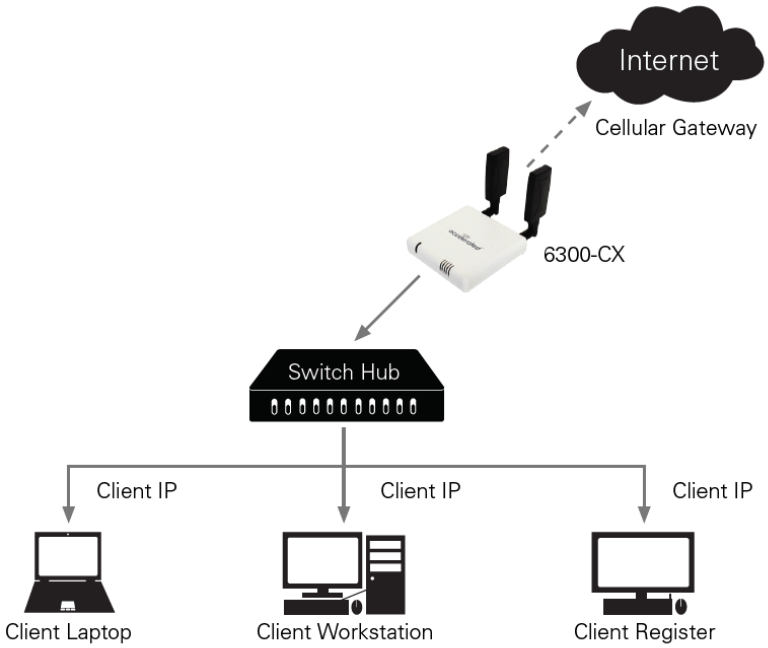
Sample Configuration

The following configuration reflects the VLAN trunking setup in the diagram, where we have two trunked VLAN interfaces on the 6300-CX's LAN Ethernet port. Also, please ensure that the **Modem** → *Passthrouth* → **Enabled** option is un-checked, as enabling passthrough mode will override any VLAN settings.


Central management
Modem
Network
Interfaces
Loopback
Default IP
Default Link-local IP
Accelerated View endpoint
Modem
LAN
public
Enable
Interface type
Static IP address
Zone
Any
Device
VLAN: public
Address
10.1.1.1/24
Default gateway
Metric
0
Weight
10
Management Priority
0
DNS servers
DHCP server
Enable
Lease time
12h
Lease range start
100
Lease range end
250
DHCP relay
Connectivity monitoring
private
Enable
Interface type
Static IP address
Zone
Any
Device
VLAN: private
Address
192.168.2.1/24
Default gateway
Metric
0
Weight
10
Management Priority
0
DNS servers
DHCP server
DHCP relay
Connectivity monitoring
Add interface
Add
Virtual LAN
public
Device
LAN
ID
2
private
Device
LAN
ID
3
Add VLAN/VLAN
Add
Bridges
Routes
IPv6
Dynamic DNS
VRRP
Routing services
IPsec
Firewall
Services
Authentication
System
Monitoring

Router Mode

In this mode, the device operates as a standard DHCP router. The device will be configured to hand out a range of LAN IP addresses to client devices connected on its Ethernet port. Standard router options are available in the device's configuration, including DHCP lease options, DNS options, firewall options, and port forwarding rules.



The following list of steps details how to setup a simple DHCP server on the device in router mode.

1. Login to Accelerated View and use the Search tool to find the device by searching for its MAC address.
2. Select the MAC address of the device to bring up its details page.
3. Select the View Configuration link in the **Configuration** section of the page.
4. Once viewing the configuration profile, select the green Edit pencil icon at the top right of the page.
5. Open the **Modem** -> **Passthrough** section, de-select the **Enable** checkbox.
6. Open the **Network** -> **Interfaces** -> **LAN** section and select the **Enable** checkbox.
7. Change the **Network** -> **Interfaces** -> **LAN** -> **IPv4** -> **Interface Type** option from **DHCP** to **Static IP Address**.
8. In the **Network** -> **Interfaces** -> **LAN** -> **IPv4** -> **Address** option, enter in the IP address you wish to assign to the device for its LAN DHCP network (i.e. the gateway IP for the DHCP network).
9. Open the **Network** -> **Interfaces** -> **LAN** -> **IPv4** -> **Address** -> **DHCP Server** section and select **Enable**.

10. Click **Save** to apply the configuration changes.

Site-to-Site VPN Access with two 63xx Series Routers

Skill level: *Expert* (requires knowledge of IPSec tunnel setup)

Goal

To build an IPSec tunnel through the 63xx router's cellular WAN Internet connection to another 63xx, and use that IPSec tunnel to access endpoints inside a VPN.

Setup

For this setup, you will need two 63xx series routers. Both 63xx routers must be on firmware version 17.5.108.6 or higher. The 63xx series routers will need an active WAN Internet connection.

The main site's 63xx series router will need a publicly reachable IP address, so the remote 63xx series router can reach the IP and build a tunnel.

You will also need to decide on the IPSec credentials and settings needed to build a tunnel between the 63xx series routers.

If configuring a 6300-CX for Site-to-Site VPN Access, it must be in router mode.

Sample

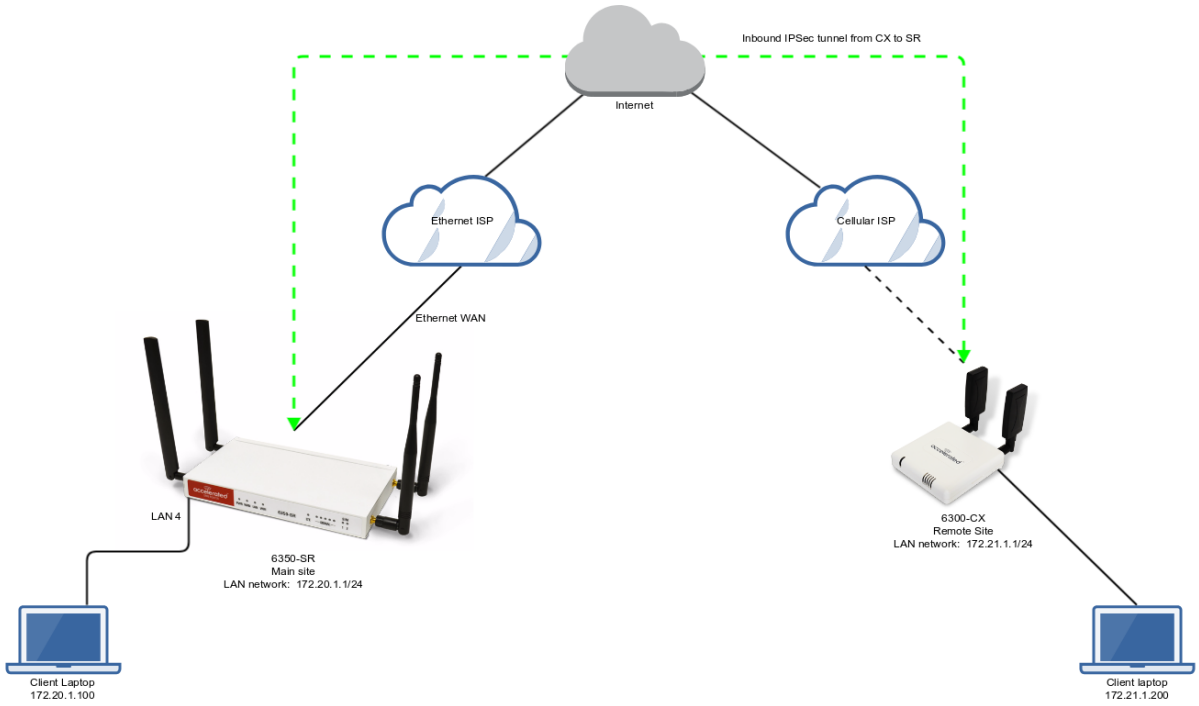
The sample configuration below shows a 6300-CX building a tunnel to a 6350-SR through its cellular modem. The client laptop connected to the LAN Ethernet port of the 6300-CX can then use that IPSec tunnel to access any IP address in the 172.20.1.1/24 range behind the 6350-SR. Any traffic not destined for 172.20.1.1/24 will instead go through the cellular modem straight to the Internet.

This tunnel will also allow the client laptop connected to the LAN 4 port of the 6350-SR to access any IP address in the 172.21.1.1/24 range behind the 6300-CX. Any traffic not destined for 172.20.1.1/24 will instead go through the Ethernet WAN of the 6350-SR straight to the Internet.

Both the 6350-SR and 6300-CX will need to be configured with a new IPSec tunnel, using matching authentication settings, in order for the 6300-CX to build the tunnel to the 6350-SR. Sample configuration settings for both devices are listed below.

Additional 63xx series routers can build IPSec tunnels to this 6350-SR. Each 63xx series router will need a unique local address range (e.g. 172.21.2.1/24 or 172.21.100.1/24) so the various remote sites do not conflict with each other. Also, the ***remote network*** and ***NAT*** settings of the main site's 6350-SR will need to be expanded to account for the additional ranges (e.g. 172.21.1.1/16).

NOTE: Be sure a value greater than 0 is specified for the local address ranges' fourth octet (i.e. X.X.X.1/24 is valid, X.X.X.0/24 is not).



6350-SR Sample Configuration

Open the configuration profile for the 6350-SR. Under ***IPSec***, create a new entry titled ***N6300*** (the name is arbitrary), and add your IPSec settings to the new entry. The following settings reflect the sample setup in the diagram above.

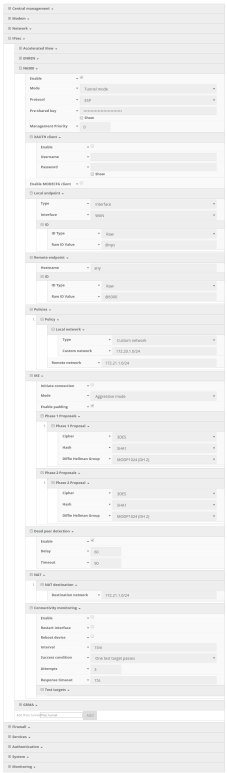
1. Enter in the PSK into the ***Pre-shared key***.
2. Change ***Local endpoint -> ID -> ID type*** to ***Raw***
3. Set the local ID in ***Local endpoint -> ID -> Raw ID Value***, e.g. *@nps*
4. Set ***Local endpoint -> type*** to ***Interface***,and set ***Local endpoint -> Interface*** to ***WAN***, or whichever interface you want to allow the inbound tunnel to connect through.
5. Change ***Remote endpoint -> ID -> ID type*** to ***Raw***
6. Set the remote ID in ***Remote endpoint -> ID -> Raw ID Value***, e.g. *@6300*.
7. Set the ***Remote endpoint -> Hostname*** to ***any***. This allows the 6300-CX to have any IP address. If you know the public IP address of the 6350-CX and wish to lock down the

6350-SR's settings so it only allows inbound tunnels from that IP, input the 6300-CX's public IP address here.

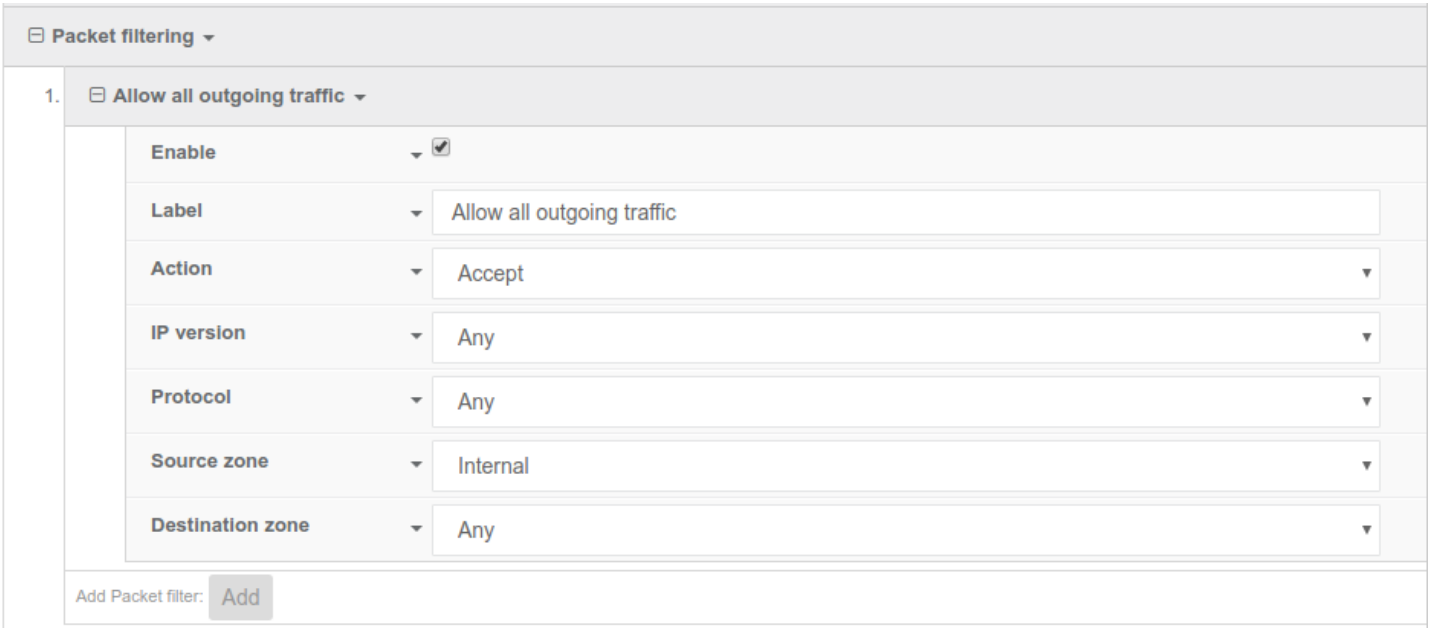
8. Set *IKE -> Mode* to *Aggressive mode*.
9. Uncheck the *IKE -> Initiate connection* option.
10. Set *IKE -> Phase 1 Proposals* and *IKE -> Phase 2 Proposals*. In this example, both proposals are set to 3DES, SHA1, MODP1024.
11. Under NAT, add a destination that corresponds to the local address range of the *remote* device. (In this example, it'd be 172.21.1.1/24.)

Under *Policies*, click *Add* to create a new policy, and enter the following settings:

1. Set *Policy -> Local network -> Type* to *Custom network.*
2. Set *Policy -> Local network -> Custom network* to the IPv4 network you wish to have on the LAN side of the 6300-CX. In the sample, this is 172.20.1.1/24
3. Set *Policy -> Remote network* to the IPv4 network you wish to access through the tunnel. (In the sample, this is 172.21.1.1/24)



Under *Firewall*, click *Packet Filtering* to ensure *Allow all outgoing traffic* item exists and enabled.



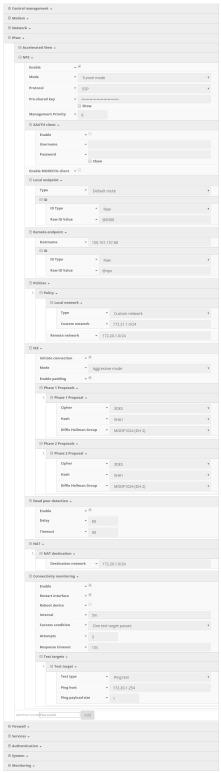
6300-CX Sample Configuration

Open the configuration profile for the 6350-SR. Under *IPSec*, create a new entry titled *NPS* (the name is arbitrary), and add your IPSec settings to the new entry. The following settings reflect the sample setup in the diagram above.

1. Enter in the PSK into the *Pre-shared key*.
2. Change *Local endpoint -> ID -> ID type* to *Raw*
3. Set the local ID in *Local endpoint -> ID -> Raw ID Value*, e.g. *@6300.*
4. *(optional)* Set *Local endpoint -> type* to *Interface*,and set *Local endpoint -> Interface* to *Modem.* This configures the 63xx-series router to only build the tunnel through the cellular modem WAN interface. Leaving *Local endpoint -> type* to *Interface* as *Default route* will allow the tunnel to be built through any available WAN interface.
5. Change *Remote endpoint -> ID -> ID type* to *Raw*
6. Set the remote ID in *Remote endpoint -> ID -> Raw ID Value*, e.g. *@nps*.
7. Set the *Remote endpoint -> Hostname* to the public IP address of the 6350-SR's WAN Ethernet.
8. Set *IKE -> Mode* to *Aggressive mode*.
9. Set *IKE -> Phase 1 Proposals* and *IKE -> Phase 2 Proposals* to match the IKE settings required by the 6350-SR. In this example, both proposals are set to 3DES, SHA1, MODP1024.

Under *Policies*, click *Add* to create a new policy, and enter the following settings:

1. Set *Policy -> Local network -> Type* to *Custom network.*
2. Set *Policy -> Local network -> Custom network* to the IPv4 network you wish to have on the LAN side of the 6300-CX. In the sample, this is 172.21.1.0/24
3. Set *Policy -> Remote network* to the IPv4 network you wish to access through the tunnel. In the sample, this is 172.20.1.0/24



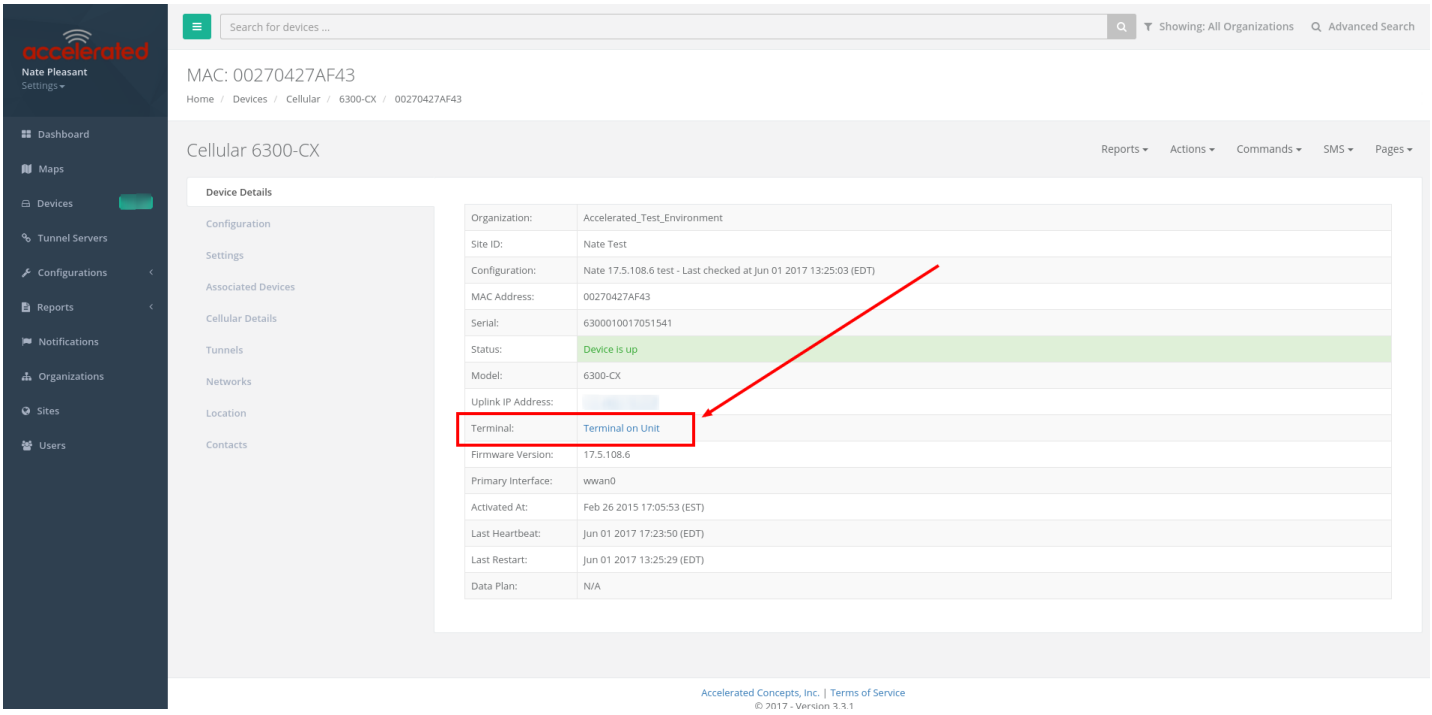
Terminal on Unit

Skill level: *Intermediate*

Goal

To access the console of an Accelerated LTE router using the *Terminal on Unit* link presented in Accelerated View for the device.

> The *Terminal on Unit* access leverages the management tunnel established between the 63xx-series router and Accelerated View. For details on the monthly data usage for this access, refer to the following article:
>
> Data Usage Estimates



Setup

For this setup, you will need access to Accelerated View, and a 63xx-series router online and syncing with Accelerated View. If you see the 63xx-series router listed as up (green status) in Accelerated View, you are good to go.

Details

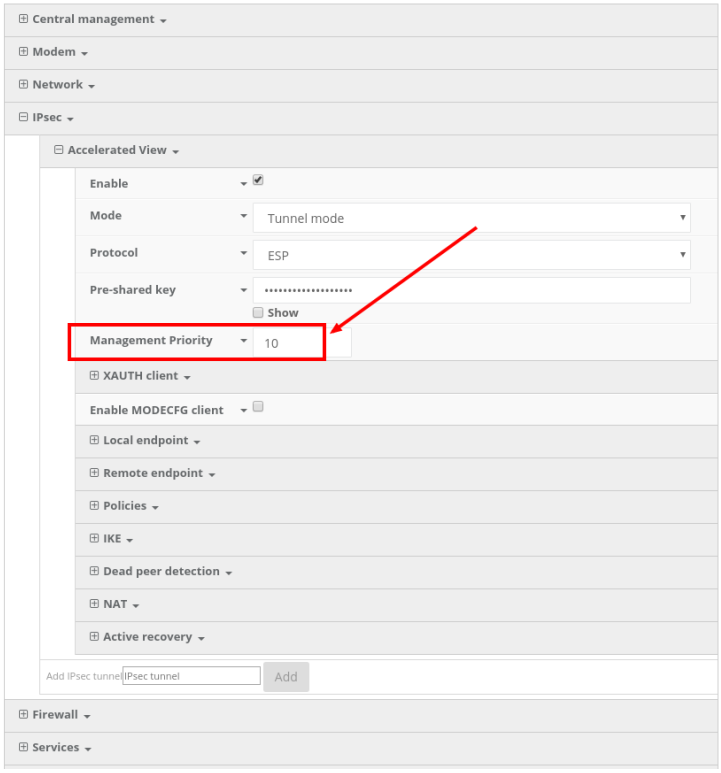
Accelerated View utilizes the IPSec tunnel the 63xx-series router establishes to remote.accns.com to provide terminal access to the console of the router.

For details on the monthly data usage for this access, refer to the following article:

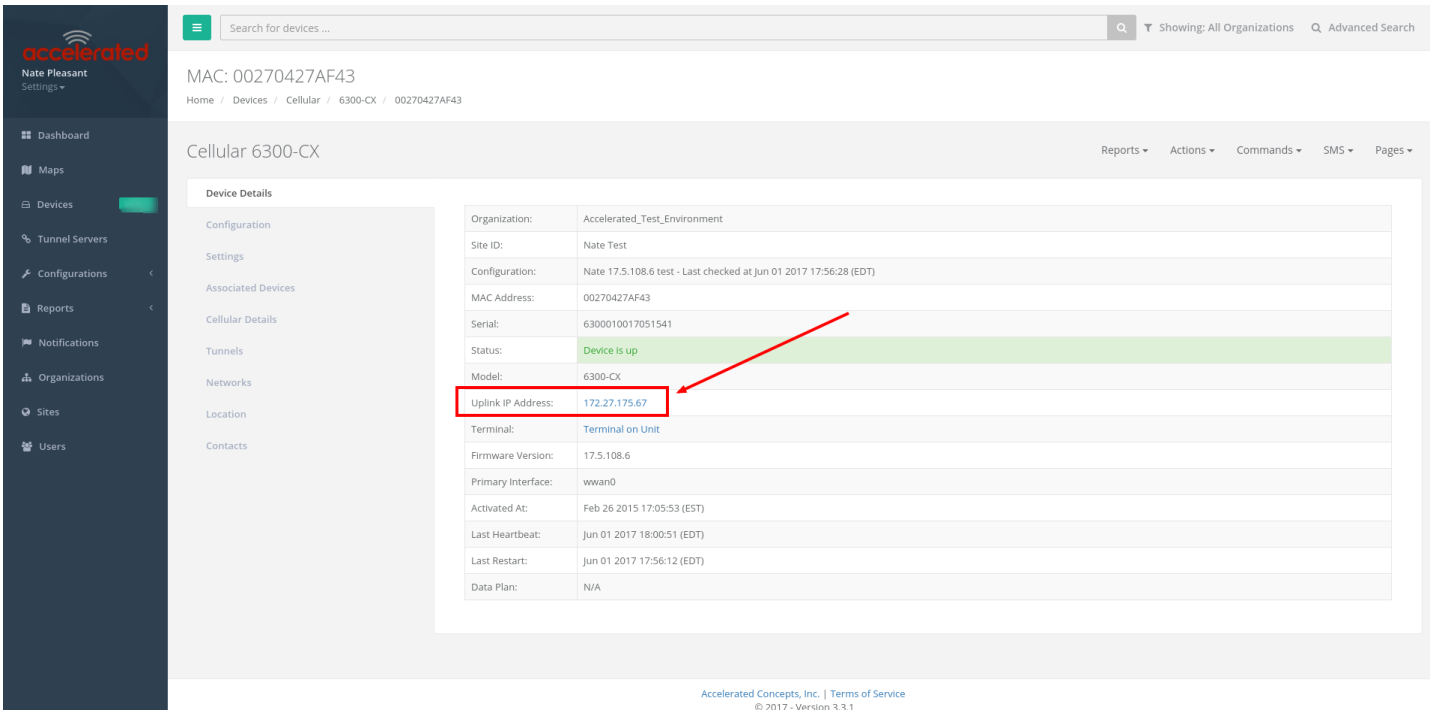
Data Usage Estimates

The following configuration settings will setup the 6300-CX to report its IPSec tunnel local IP address as the management IP that Accelerated View can then use to access its console.

Open the configuration profile for the 63xx-series router. Under *IPSec -> Accelerated View*, set the *Management priority* to *10*. This will tell the 63xx-series router to treat the AView IPSec tunnel as the highest priority management interface, which it then reports to Accelerated View as the IP that can be used to access its console.



Once you apply the new configuration to the 63xx-series router, reboot the 63xx-series device so it rebuilds the IPSec tunnel and reports the new IPSec local IP address to Accelerated View. You can verify that Accelerated View is using the IPSec local IP as the management IP by looking at the *Uplink IP address* on the *Device Details* tab. This value should be set to a 172.x.x.x IP address.



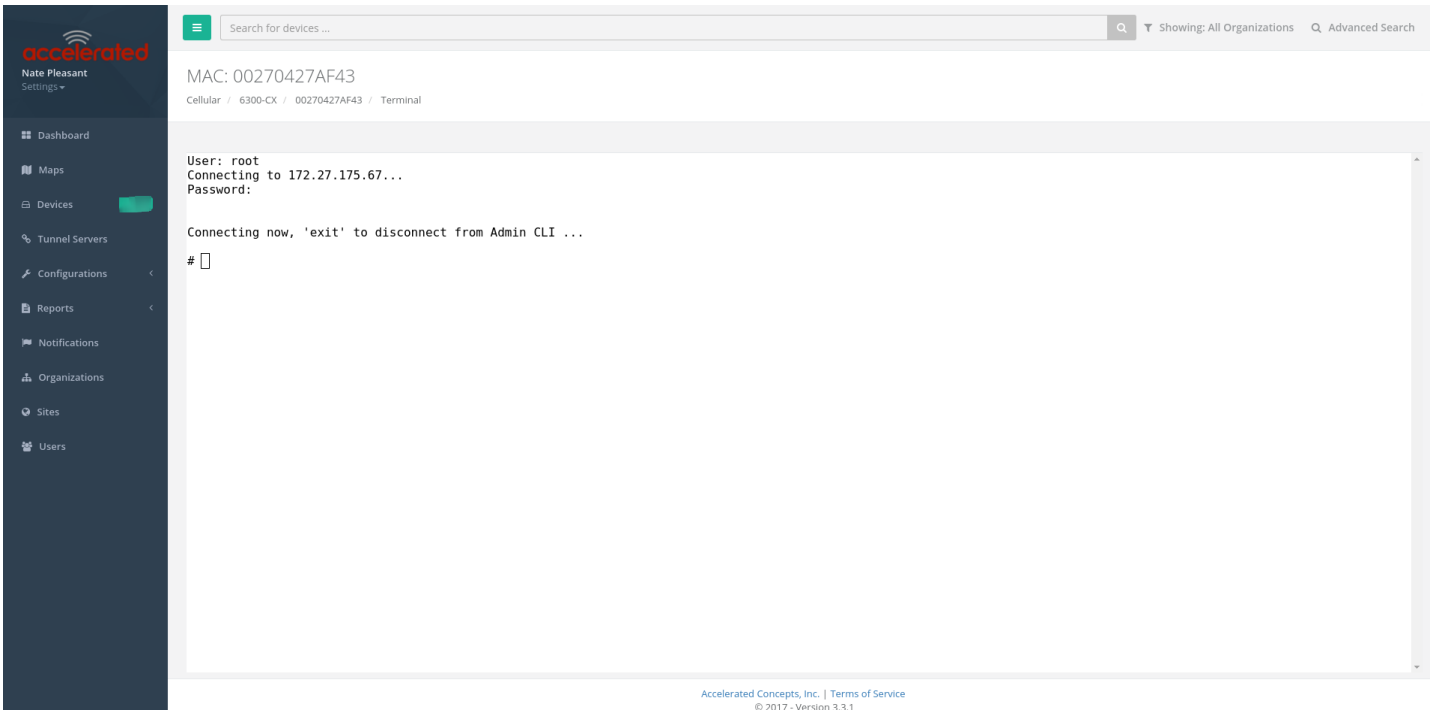
Using the Terminal on Unit link

Once the correct management IP is reported from the 63xx-series router to Accelerated View, clicking the *Terminal on Unit* will open a page on Accelerated View to provide the user access to the console of the 63xx-series router. Default login credentials are below.

User: root

Password: default

To create a different user or change the root user's password, refer to this article.



There is a known issue where the predictive/auto-correct feature of the Google keyboard renders it incompatible with the Terminal page. If you are access the above Terminal with an Android phone or tablet, you will need to use a different keyboard other than the native Google keyboard.

Custom Speed Test Server

Skill level: *Intermediate*

Goal

To setup a custom speed test server and have your Accelerated 63xx-series router perform speed tests to it.

The *Speed test* command leverages the management tunnel established between the 63xx-series router and Accelerated View. For details on the monthly data usage for this access, refer to the following article:

Data Usage Estimates

Setup

For this setup, you will need access to Accelerated View, and a 63xx-series router online and syncing with Accelerated View. If you see the 63xx-series router listed as up (green status) in Accelerated View, you are good to go.

Details

Accelerated View utilizes the IPSec tunnel the 63xx-series router establishes to remote.accns.com to send remote commands to the device. One of the available commands a user can run is the *Perform Speed Test* command. This will trigger the 63xx-series router to perform a speed test to the speedtest server specified in its configuration settings. The default speed test server is speedtest.accns.com.

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.

This article will detail setting up a separate speed test server that a 63xx-series router can use as an alternative to the default speed test server.

Speed Test server setup

The speed test server utilizes the nuttcp tool in Linux. This setup was tested using nuttcp version 6.1.2 on an Ubuntu 16.04 server with 1GB of RAM and a 30GB hard drive. The nuttcp tool used approximately 150kB of disk space, and consumed an average of 100MB of RAM.

Run the following command to install the nuttcp package.

```
sudo apt-get install nuttcp
```

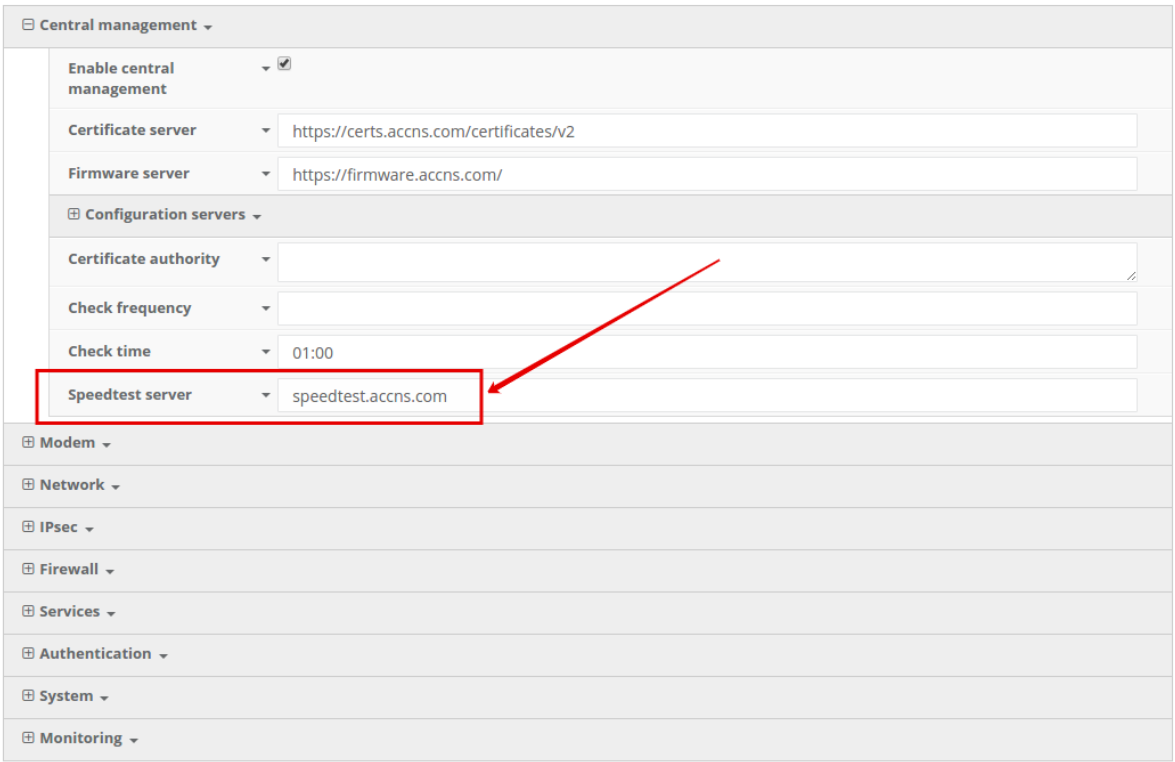
Then start the nuttcp speed test server with the following command:

```
nuttcp -S
```

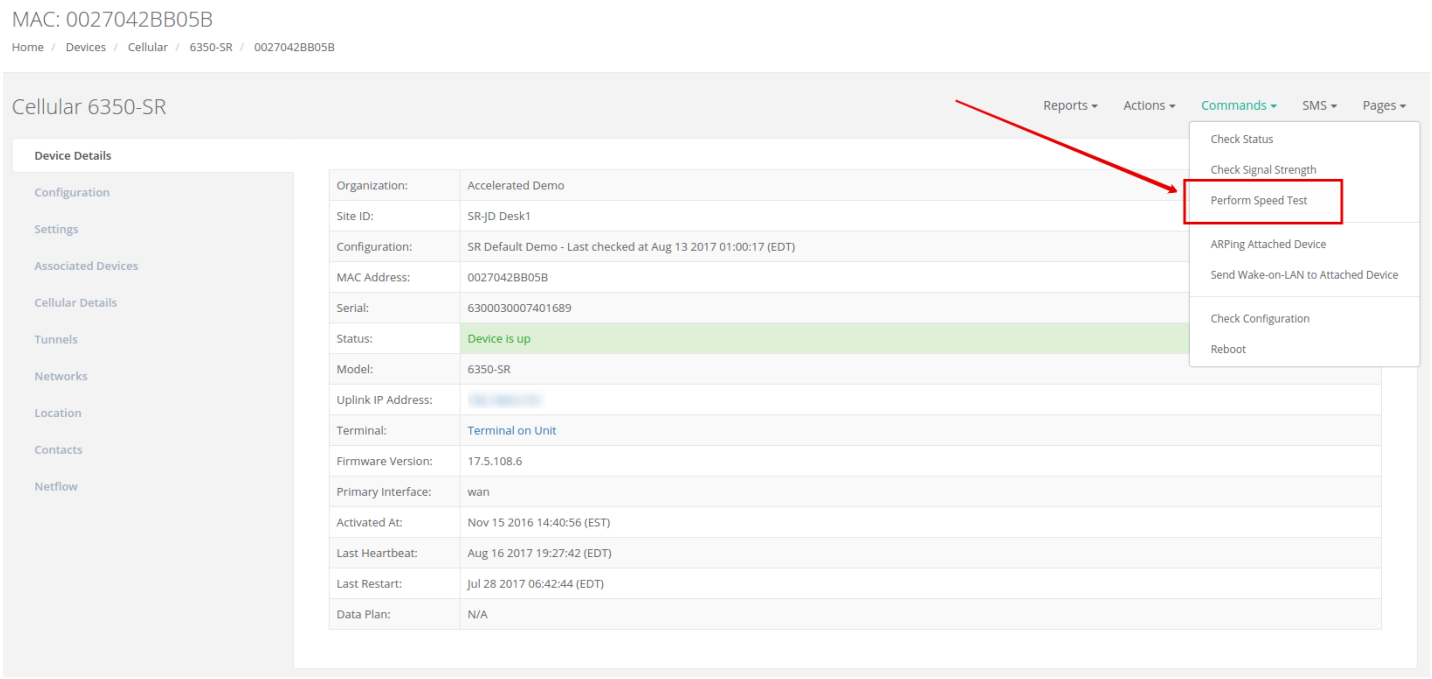
The 63xx-series router will need access to this server on UDP ports 5000 and 5001. Please ensure proper firewalls are opened to allow access to the IP address of the speed test server and its respective ports.

Using the new speed test server

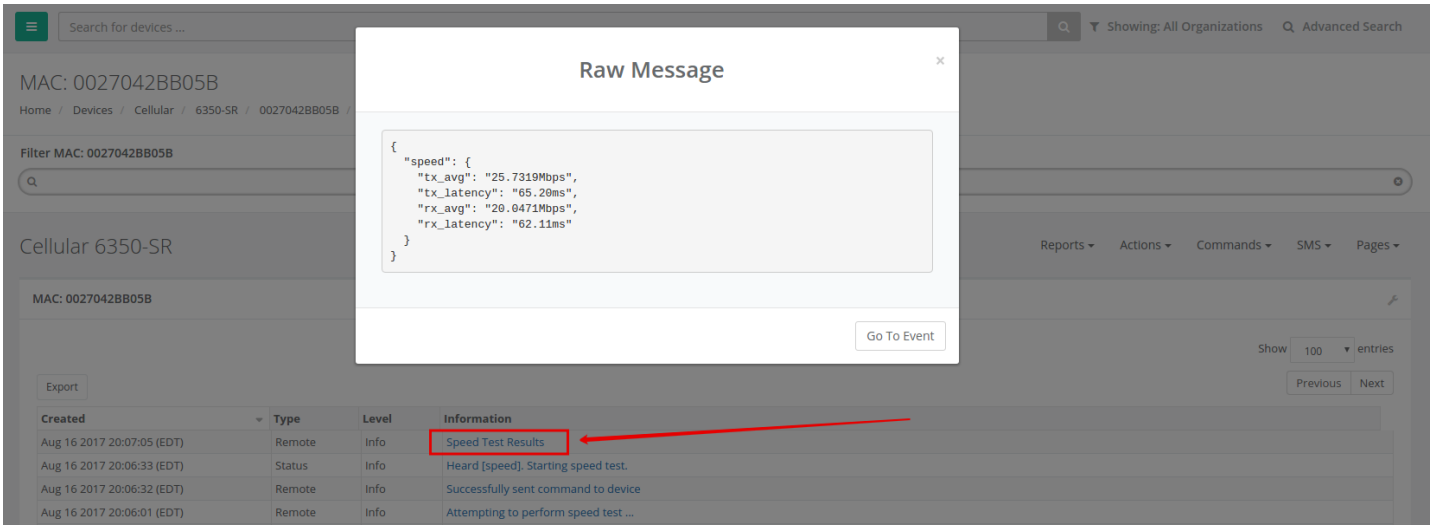
Once the new speed test server is running, add the IP address to the 63xx-series router's configuration profile under *Central management -> speedtest server* and apply the configuration to the device.



To run a speed test, select the *Perform Speed Test* option under the *Commands* drop-down listed on the device's details page in Accelerated View.



The 63xx-series router will acknowledge the request to perform the speed test, and will send another event to Accelerated View once the speed test completes. Clicking on the speed test results will display a window with the upload and downloads speeds observed in the test.



Remote Access

Skill Level: *Moderate* (assumes familiarity with SSH sessions)

Goal

To SSH into an Accelerated device remotely, using the terminal available via Accelerated View and a publicly reachable IP address.

If your device does not have a publicly reachable IP address, you can still leverage the Terminal on Unit via the Accelerated View IPSec Tunnel.

Setup

Devices can be managed over SSH so long as the external zone is enabled for remote SSH and web UI access.

The default credentials are:

Username: *root*

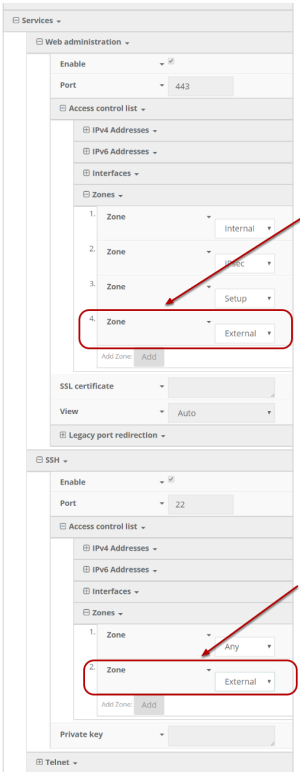
Password: *default*

NOTE: The configuration steps outlined below will open external access to your Accelerated device. It is imperative that the default password is changed to a more secure key to prevent intrusions.

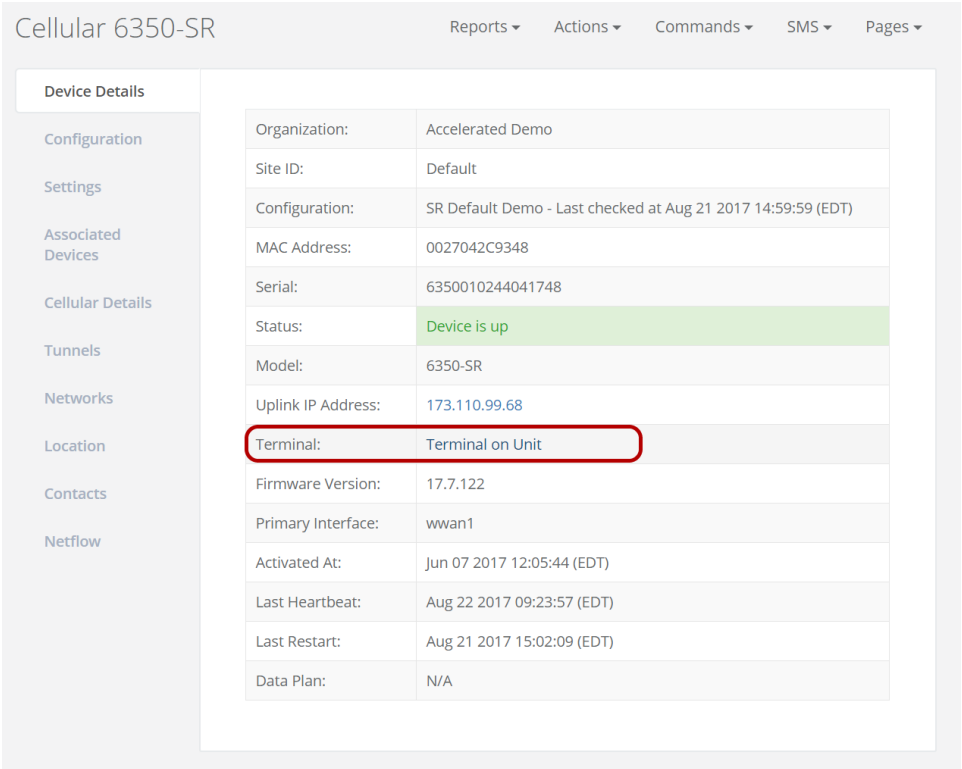
Sample Configuration

Open the configuration profile of the device and expand *Services*. Under *Web Administration*, expand *Access Control List* and *Zones* to create a new entry for "External." Repeat this process for the *Zones* associated with the *Access Control List* under the *SSH* menu heading. The following steps reflect the sample setup indicated in the screenshot below:

1. Under *Services -> Web Administration -> Access Control List*, expand *Zones*.
2. Add a new entry for "External."
3. Under *Services -> SSH -> Access Control List*, expand *Zones*.
4. Add a new entry for "External."



Once the configuration has been updated, click the *Terminal on Unit* hyperlink available from the *Device Details* screen.



Enabling intelliFlow

Difficulty level: *Beginner*

Goal

To enable Accelerated intelliFlow feature in compatible devices to allow the monitoring of system resource information and network traffic flow in the local management interface (WebUI)'s Dashboard page.

Setup

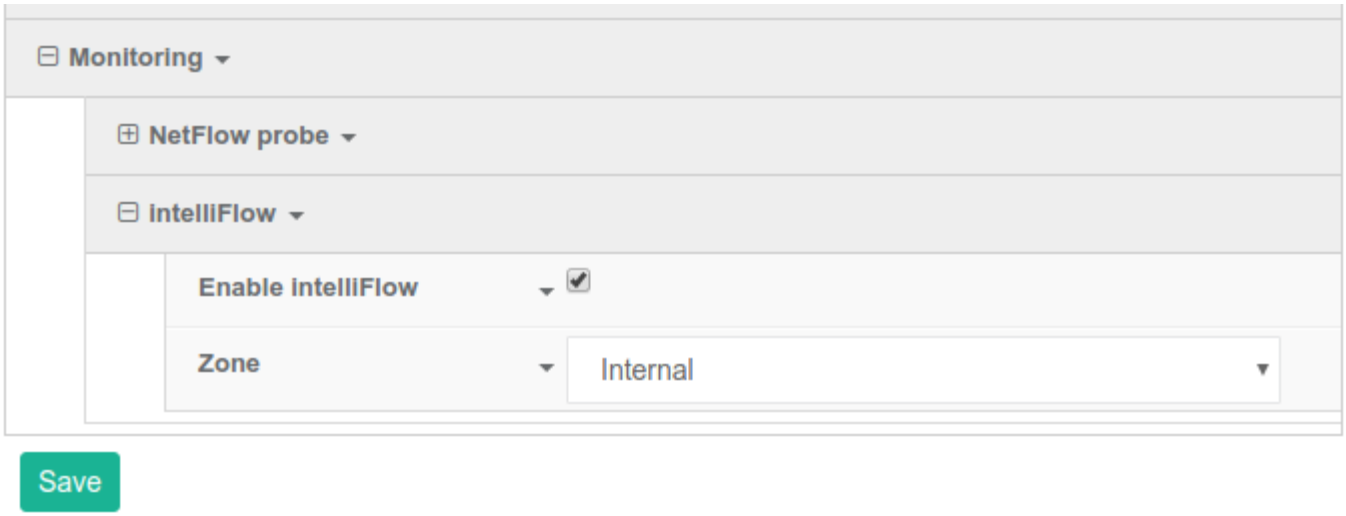
The purpose of intelliFlow is to keep track of the network data usage and traffic information, therefore the only requirement is that the device is powered on, and the local WebUI is accessible.

The comprehensive explanation of the Dashboard can be found in the User manual.

Sample Configuration

Open the configuration profile for the router device and make the following changes.

1. Under *Monitoring* > *intelliFlow,* check *Enable intelliFlow*.
2. Click *Save*.
3. To view intelliFlow data, select *Dashboard*. Once intelliFlow data is collected, relevant information will display in the Dashboard.



Enabling Shell Access

Difficulty: *Beginner*

Goal

To enable shell access to an Accelerated User Equipment (UE) via the SSH protocol.

Setup

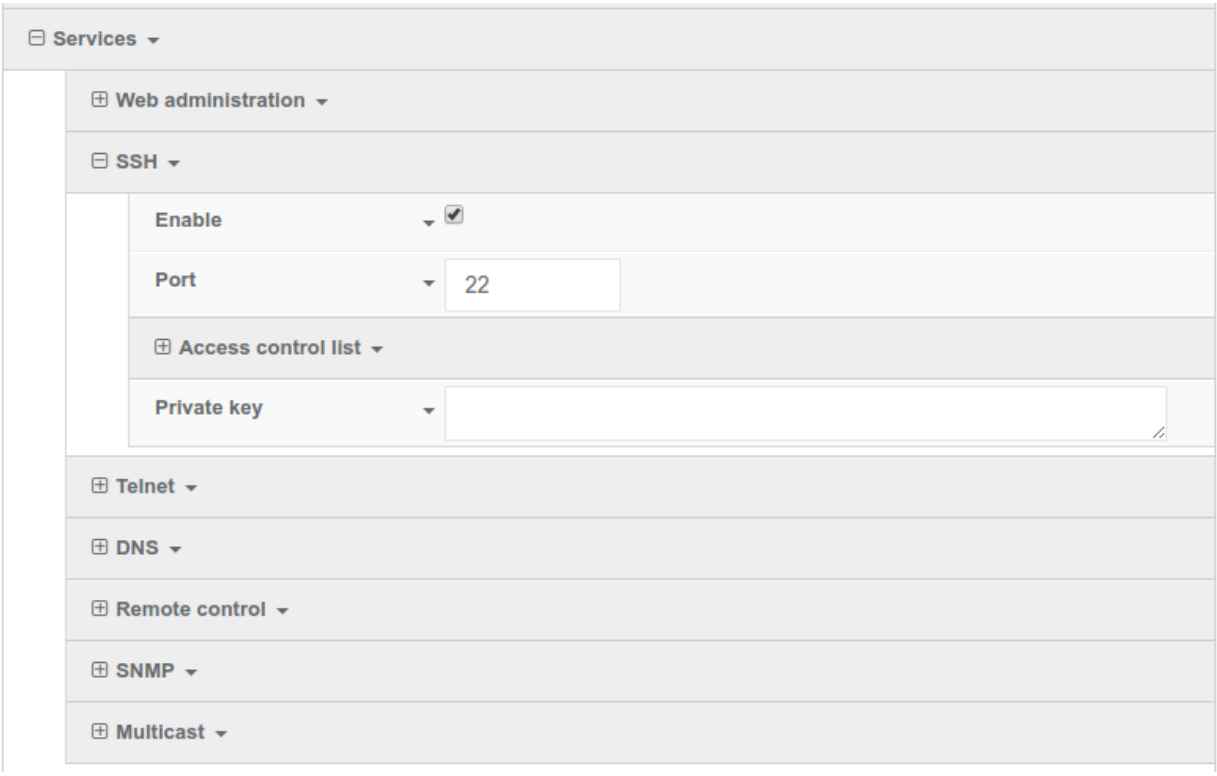
This article assumes the UE is running default configuration with the root password assignment, and central management disabled. Similar procedures apply if shell access is to be enabled in central management.

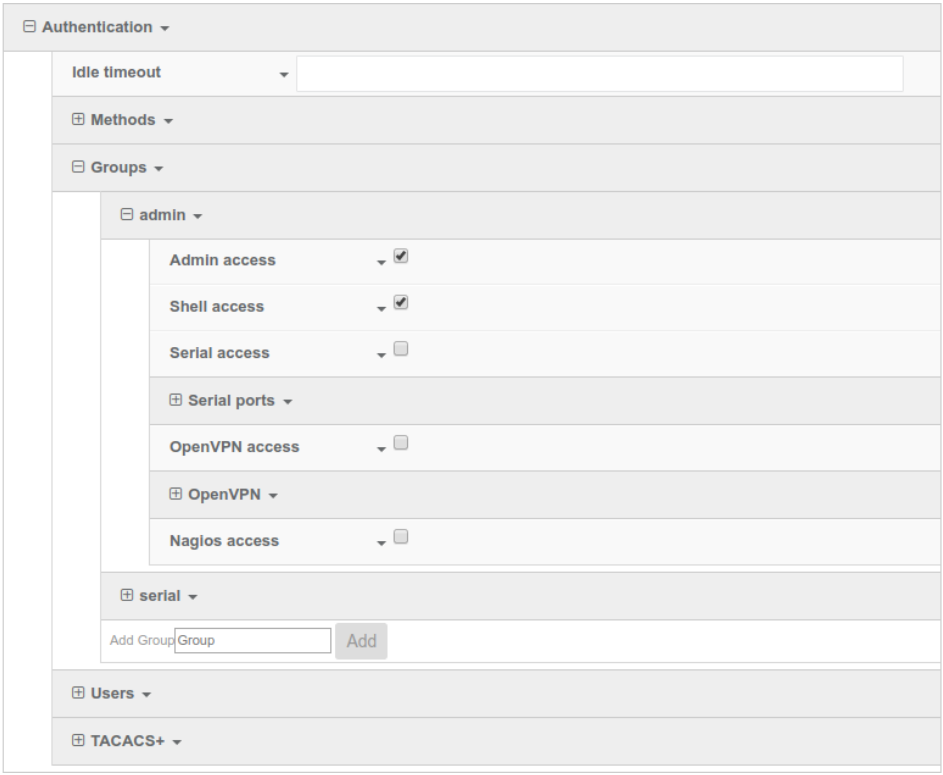
Configuration Steps

This configuration enables the local shell access for an existing root user. This procedure is applicable to any other users on the UE just the same.

Open the configuration page for the UE and make the following changes.

1. Ensure *Service -> SSH -> Enable* is checked.
2. Check the box under *Authentication -> Groups -> admin -> Shell access*.
3. Click *Save* to update configurations.





Once the configurations have been successfully saved, the UE's shell can be accessed via SSH. Below is an example shell login process:

```
$ ssh root@192.168.2.1
$ password
```

```
Access selection menu:

    a: Admin CLI
    s: Shell
    q: Quit

Select access or quit [admin] : s

Connecting now, 'exit' to disconnect from shell ...

#
```

Local User Management

Skill level: *Beginner*

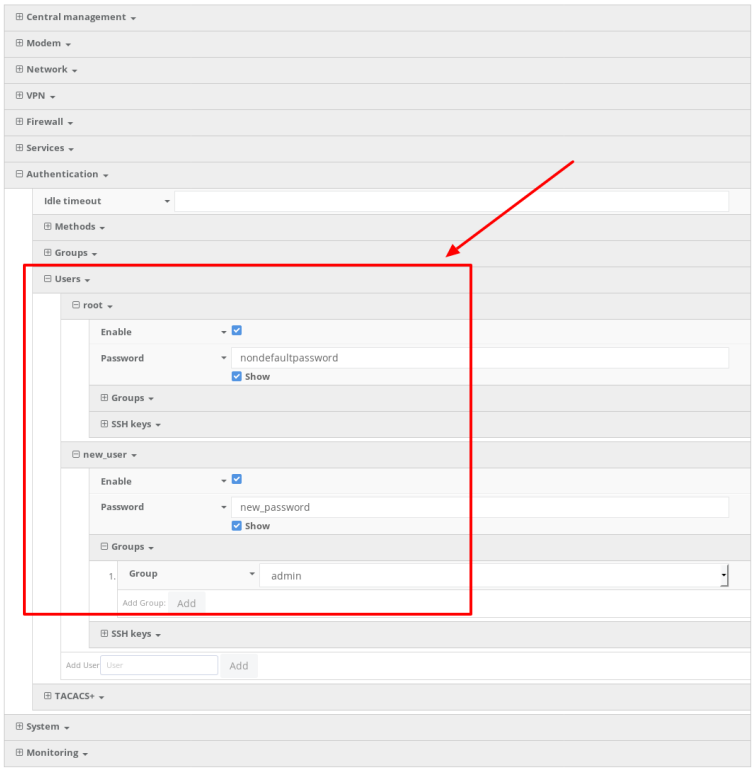
Goal

To create a new user and/or change the password of the default root user.

Details

Open the configuration profile for the 63xx-series router and make the following changes:

1. To update the root user password, enter in the new password in the in the *Authentication -> Users -> root -> Password* option.
2. To create a new local admin user:
   1. Under *Authentication -> Users -> Add User*, enter in the new username and click *Add*.
   2. Enter in the password for the new user
   3. Under *Groups* for the new user, select the default *admin* group. You can create a new group, or edit the admin group's priviledges through the *Authentication -> Groups* section of the configuration profile.



Framed Routing in Passthrough Mode

Skill level*: Beginner*

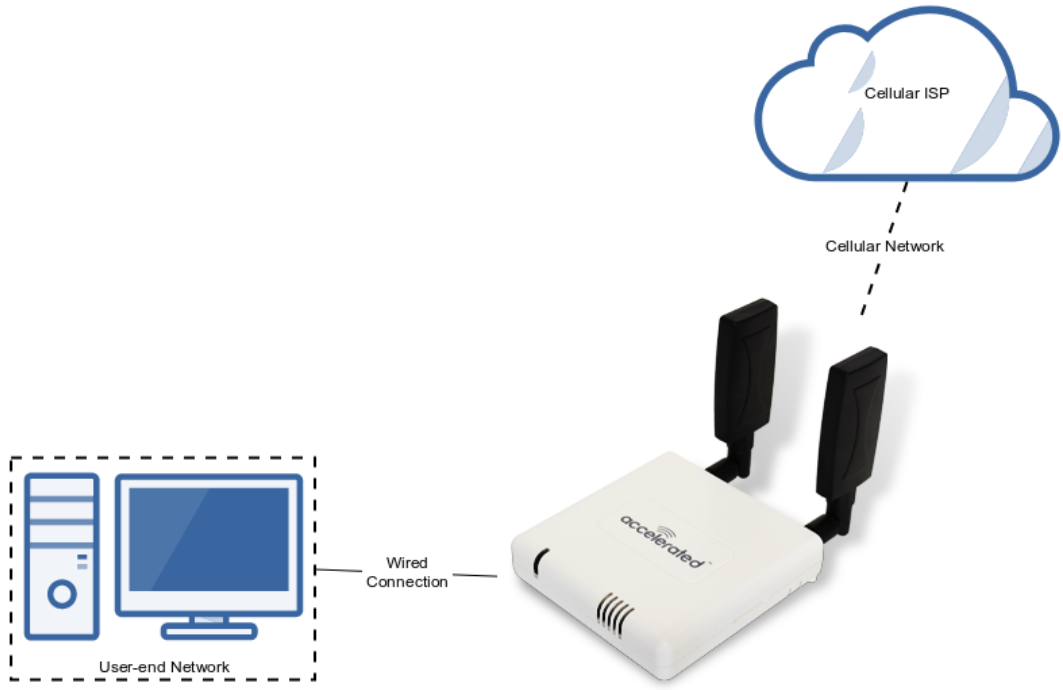
Goal

To configure the User Equipment (UE) so that it supports framed routing in passthrough mode.

Setup

This setup example assumes that you are running firmware version 18.1.29.10, although versions other than this may have similar set up procedure. The configuration is also assumed to be factory default with central management disabled.

The hardware set up requires a computer to be physically connected to the blue LAN port of the UE, and an active SIM with the appropriate plans and permissions to establish framed routing. This example uses the cellular information of a hypothetical "MyISP" network.

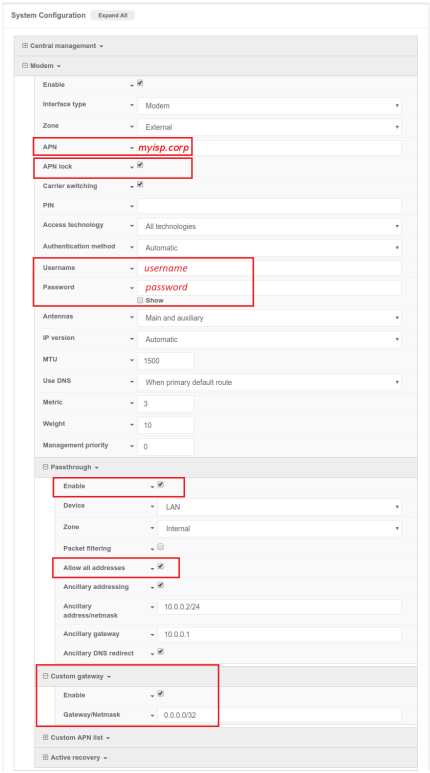


Sample Configuration

Once the UE is physically connected to a computer and central management is disabled, navigate to the WebUI via *192.168.210.1* and go to *Configuration* page > *Modem*.

1. Enter the *APN* used for the framed routing service: *myisp.corp.*

2. Check *APN Lock* to always lock onto the APN entered previously.
3. Insert your account *username* and *password* into their respective fields.
4. In the *Passthrough* section, ensure it is *Enabled.*
5. Check *Allow all addresses* to enable forwarding between the cellular network and any network/addresses via this UE.
6. In the *Custom gateway* section, check *Enable* and insert Gateway/Netmask: *0.0.0.0/32*.
7. Click *Save* at the bottom of the web page to save and enable the configurations.



Configuration for SonicWall TZ Series

Overview

The Accelerated 6300-CX LTE Router provides a reliable, high-speed cellular connection that is compatible with existing wireline infrastructure. While its 4G LTE speeds are capable of operating as a primary WAN uplink, the 6300-CX can also be configured as a backup. This network redundancy solution delivers the ultimate flexibility to minimize expenses when it comes time for upgrading equipment to the latest wireless standards.

Business continuity depends on the seamless integration of failover-connectivity solutions to prevent service interruptions. Now more than ever, contingency networks play a strategic role in sustaining business operations. Unplanned outages can cost companies significant time and money, frustrating employees and clients alike, which creates a negative perception that is difficult to overcome.

Cellular data (4G LTE) bypasses wireline Internet service providers (ISPs) to facilitate the best redundancy possible. Additionally, in some situations it may be a challenge to acquire access to wired circuits or an event may call for temporary online access. For these reasons SonicWall and Accelerated Concepts have teamed up to offer comprehensive security and flexibility for small businesses, retail, government, remote sites, and branch offices.

SonicWall's TZ Series of firewalls consolidates enterprise security measures into a single Unified Threat Management (UTM) device. It optimizes and fortifies networked environments thanks to a robust suite of administrative utilities ranging from content filtering to malware and intrusion prevention though this functionality hinges upon an active WAN connection. A TZ-Series UTM Firewall paired with the Accelerated 6300-CX LTE Router will ensure your enterprise network

remains secure and operational should its primary ISP go offline. Running a cellular backup via an Ethernet cable preserves the full security functionality of the TZ-Series device (DPI-SSL inspection), which isn't the case for USB-connected Aircards.

For additional information, please refer to SonicWall's TZ-Series datasheet and the SonicOS Administration guide.

Interoperability Matrix

This section covers interoperability information of the hardware tested for this solution. It includes the firmware versions of both devices as well as the date of testing.

Date	SonicOS Release	6300-CX Firmware
10/2016	5.9.X & 6.2.X	16.10.13

Caveats

The delivery of wireless services varies depending on the carrier and may lead to differences in the area of coverage, type of service (3G, 4G, LTE, etc.), available bandwidth, and IP address designation (Private or Public) among other factors. The interoperability test designed for this solution guide included LTE service, maximum coverage availability, and a public IP address assigned to each device.

Using the 6300-CX as a secondary connection assumes that a primary WAN Ethernet cable is plugged into the X1 port on the SonicWall device. Connect the 6300-CX's backup Ethernet cable to port X2 and proceed to the configuration described herein. (Compatible with all Gen 6 Firewalls, including TZ, NSA, and SuperMassive series.)

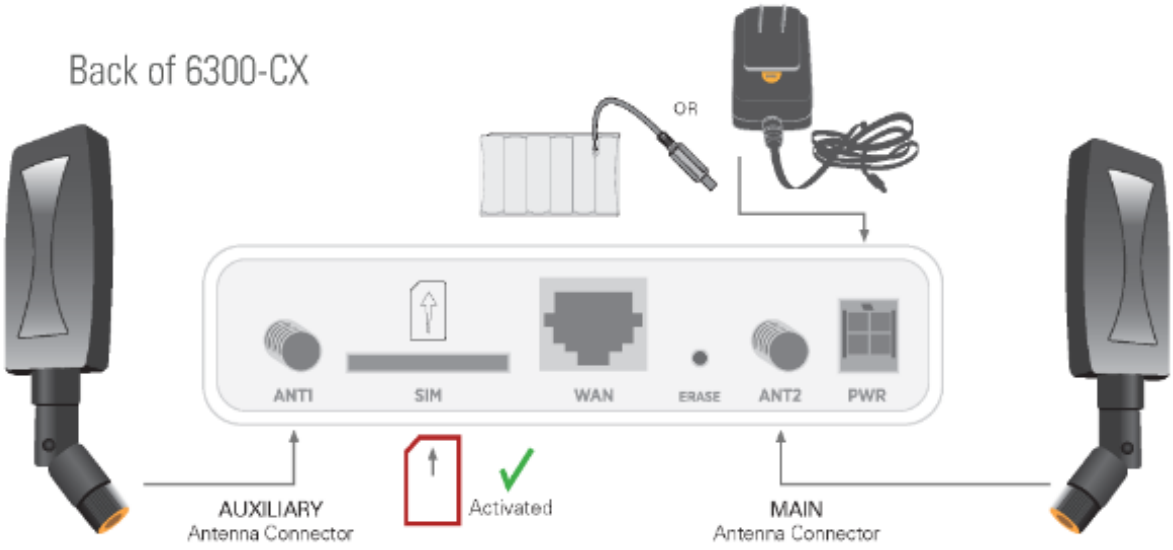
Accelerated 6300-CX LTE Router Setup

Initial Setup

Affix both antennas to the router and insert an activated SIM card before deploying the device. Be sure to select a location with optimal signal strength. For detailed instruction, refer to the tables that follow. Subsequent sections will outline site selection, powering options, and other device functionality.

Step-by-Step Guidance: Initial Setup

1. Insert the activated 2FF SIM card provided by your cellular network operator (putting the cut corner in first with metal contacts facing down). The card clicks into place when completely inserted.
2. Attach the two included antennas; both should be installed for optimal operation. Do this by gripping the metal connector section with your thumb and forefinger, tightening until secure. Do not tighten the antenna by holding any part of the plastic antenna housing.
3. To determine the optimal location for the 6300-CX, please see the “Site Survey” section.
4. Refer to the section(s) for Remote or Direct Power Installations when ready to connect the 6300-CX to the permanent power supply unit.
5. The 6300-CX uses DHCP with IP passthrough by default, which satisfies the setup requirements for most environments. If required, please use Accelerated View™ or the 6300-CX local GUI to configure the 6300-CX for router mode.



Site Survey

If you are unsure of the available cellular signal strength, or are choosing between several locations, please follow the instructions to identify the ideal installation site.

Step-by-Step Guidance: Site Survey

1. After following steps 1 and 2 in the “Initial Setup” section, connect the battery pack to temporarily power the Accelerated 6300-CX. The charge lasts two to four hours – it is not rechargeable and should be properly disposed of after use.

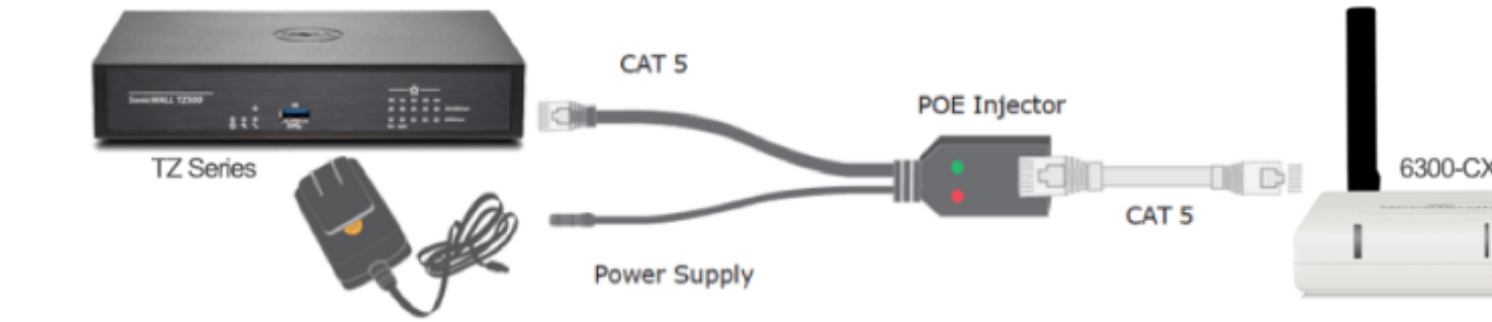
2. Move the 6300-CX to different locations within your site to determine the best compromise between signal strength and installation constraints. Since cellular signal strength may fluctuate, it is important to **wait at each location for 1 minute while observing the signal strength indicator on the front of the device.** Minimum cellular signal strength for operation is 2 bars (3+ is preferred).
3. After determining the optimal location, remove the battery pack and connect the main power supply unit or Ethernet cable connected to the PoE injector (per the power option outlined below).

Remote Power Installation – Power Option #1

The included Power-over-Ethernet (PoE) injector allows the device to be positioned away from power outlets to simplify its installation needs. The adaptor consolidates the DC power and Ethernet connections so that both can be run to the 6300-CX via a single Ethernet cable. Distances of 300 ft have been tested on CAT6 and 250 ft on CAT5e. Note that cable conditions and the number of splices will impact actual distance.

Step-by-Step Guidance: Remote Power Installation

1. Plug the 6300-CX's power supply unit (PSU) into an AC power outlet.
2. Connect the end of the PSU into the DC input (4 pin connector) of the PoE injector.
3. Insert the male RJ45 connector of the PoE injector cable into the SonicWall.
4. Connect an Ethernet cable from the RJ45 socket on the PoE injector cable to the Ethernet port of t 6300-CX. (See diagram.)

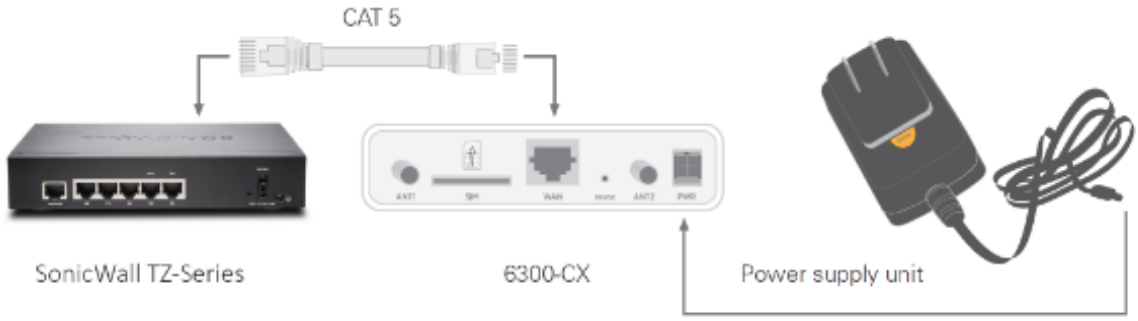


Direct Power Installation – Power Option #2

If you plan to collocate the 6300-CX with the MX device, you can directly power the 6300-CX without the PoE cable.

Step-by-Step Guidance: Direct Power Installation

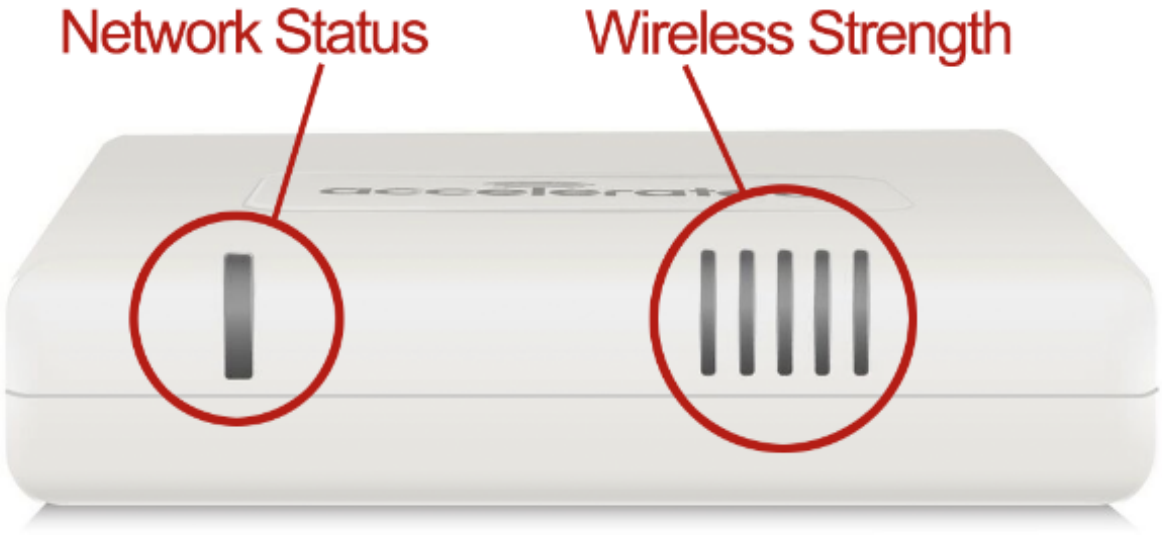
1. Use an Ethernet cable to connect the 6300-CX to the security appliance using port Internet 1 (to use the cellular network as the primary connection) or port Internet 2 (to configure a failover).
2. Plug the 6300-CX power supply unit (PSU) into an AC power outlet.
3. Connect the PSU into the 4-pin power connector of the 6300-CX. (See diagram.)



Understanding the 6300-CX LEDs

Once power has been established, your device will initialize and attempt to connect to the network. Device initialization may take 30-60 seconds. Indicator lights on the **Wireless Strength Indicator** show you the cellular network signal strength. The **Network Status Light** on the front left of the device displays connectivity information.

Please visit accelerated.com for additional information and troubleshooting tips.



Network Status LED

Solid Yellow
Initializing or starting up.

Flashing Yellow
In the process of connecting to the cellular network and to a device on its Ethernet port.

Flashing White
Has an Ethernet connection and is in the process of connecting to the cellular network.

Flashing Green
Connected to 2G or 3G and is in the process of connecting to a device on its Ethernet port (or nothing is connected to the port).

Solid Green
Connected to 2G or 3G and also has an Ethernet connection.

Flashing Blue
Connected to 4G LTE and in the process of connecting to a device on its Ethernet port.

Solid Blue
Connected to 4G LTE and also has an Ethernet connection.

Alternating Red/ Yellow
Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Wireless Strength LEDs

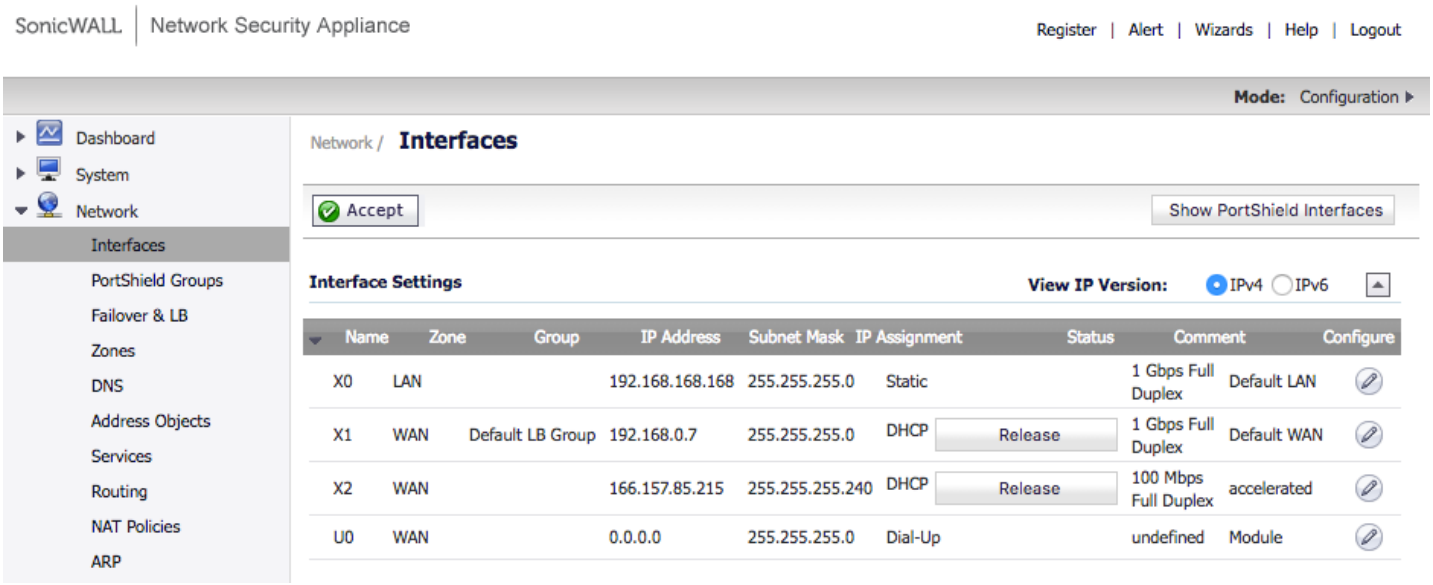
Signal Bars	Weighted dBm	Signal Strength %	Quality
	-113 to -99	0 - 23%	Bad
	-98 to -87	24 - 42%	Marginal
	-86 to -76	43 - 61%	OK
	-75 to -64	62 - 80%	Good
	-63 to -51	81 - 100%	Excellent

SonicWall Configuration with the Accelerated 6300-CX

Multiple WAN (MWAN) Configuration

More than one network must be assigned to the SonicWall's WAN Zone to create a contingency solution. Once assigned to a zone, configure the connection's IP assignment, group membership, and any other relevant specifications. MWAN functionality automatically assigns the primary WAN interface from the X1 port. All other ports can be manually allocated for WAN network routing aside from X0, which must remain dedicated to local administration (LAN).

Access the SonicWall admin portal at 192.168.168.168



Please refer to the SonicWall knowledge article for an in-depth walkthrough of the Interfaces Screen.

Step-by-Step Guidance: MWAN Configuration

NOTE: X0 is reserved for the default LAN and X1 is predefined as the default WAN, making X2 the first available interface for a failover WAN.

1. From the Interfaces tab of the admin portal, click on the edit icon under configure.
2. Choose WAN from the Zone pull-down menu.
3. Unless otherwise specified, select DHCP from the IP Assignment pull-down menu.
4. Assign reference labels to entries using the comments field.
5. Click the OK button to finalize any changes.
6. The new interface is now configured for WAN, X2 in the image above.

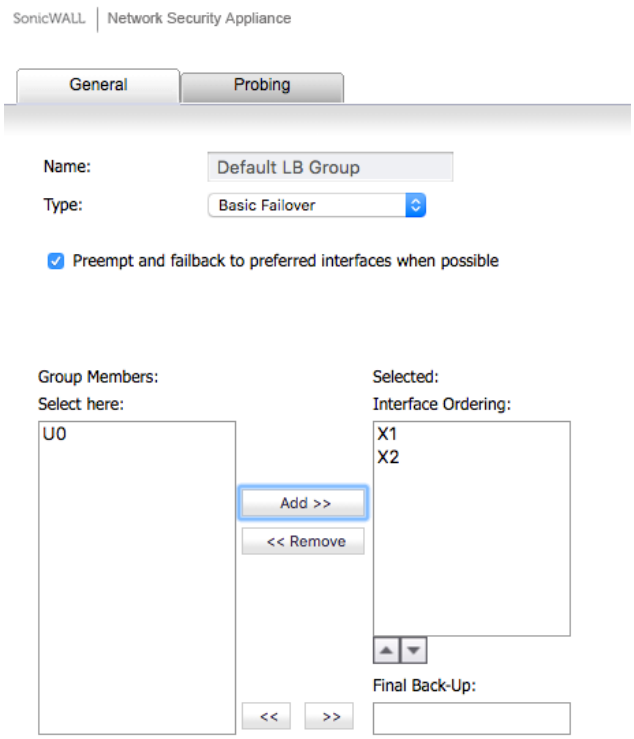
Failover & LB Management

TZ-Series Firewalls feature customizable, load-balancing (LB) automation that reroutes traffic to contingency networks when triggered by outages or user-defined limits. SonicWall recommends that load balancing remains enabled at all times, even when a single-WAN solution is in use. (It is activated by default.)

Groups respond to specific network conditions depending on their assigned type: Basic Failover, Round Robin, Spill-over, and Ratio. To set a backup connection so it takes over for the primary line in the event of a service outage, add both interfaces to the “Default LB Group” (the firewall’s basic failover grouping) and confirm that the main interface (X1) is listed above the auxiliary WAN (X2).

The “preempt and failback to preferred interfaces when possible” checkbox appears only for the “Basic Failover” type. Selected by default, it enforces the preferences established by the sort order of the interface list. These options change contextually depending on the group type, including options to set ratio or spill-over thresholds. Use the Probing tab to modify parameters for failback detection via Logical probes, which verify whether or not connectivity has been restored to an inactive interface before reestablishing it as the primary WAN.

Please refer to the SonicWall knowledge article for an in-depth walkthrough of the Failover & LB Screen.



Step-by-Step Guidance: Failover & LB Management

1. After setting up the WAN from the Accelerated 6300-CX LTE, navigate to the Failover & LB page of the SonicWall admin portal.
2. Next to “Default LB Group,” click the configure button to add a new member.
3. The Group Members column on the left lists all available interfaces.
4. Select X2.
5. Use the Add button to move the chosen interface(s) to the Selected column.
6. The Probing tab specifies how test packets are sent and received to verify WAN path availability.
7. Click OK to finish editing the group’s settings.
8. The X2 interface is now set as a failover for the primary network.

***NOTE:** Interface priority within a group is established by list position, which can be adjusted using the Up/Down buttons or the Final Back-Up field. The member listed first takes*

precedence over subsequent members; the final back-up is always considered last.

Site-to-Site VPN with SonicWall Firewalls

Skill level: ***Expert*** (requires knowledge of IPSec tunnel setup)

Goal

To build an IPSec tunnel through the 63xx router's WAN internet connection, and use that IPSec tunnel to access endpoints inside a VPN.

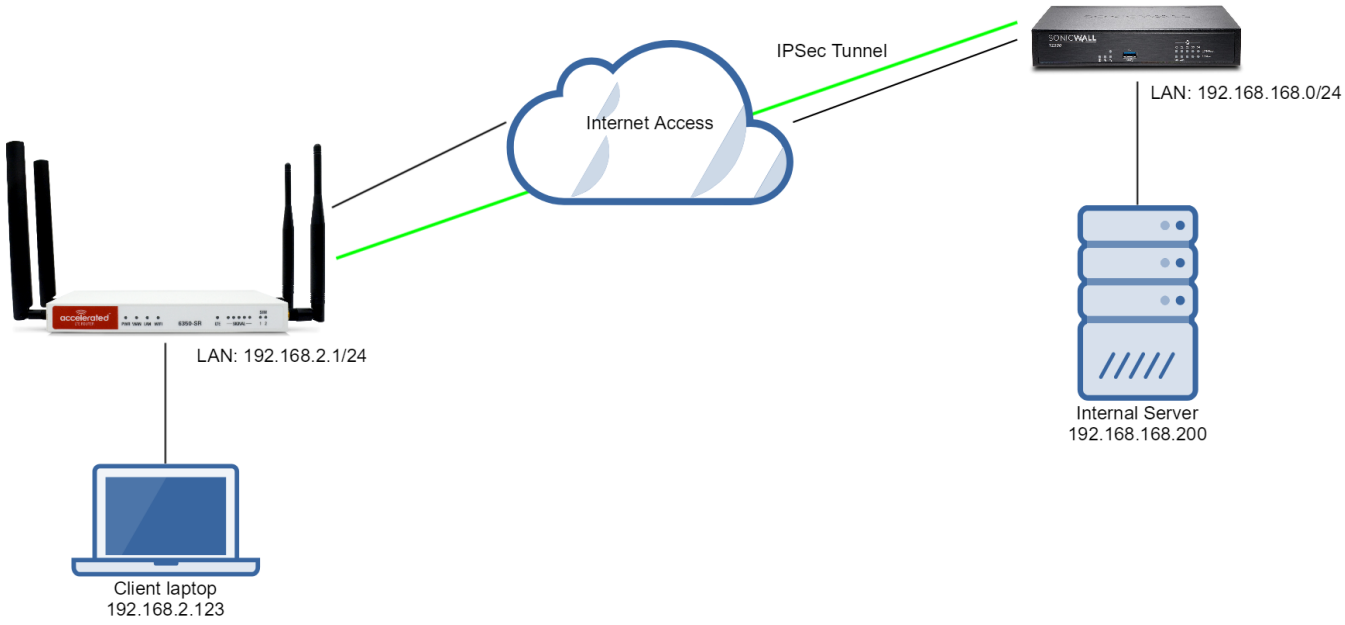
Setup

For this setup the Accelerated router will need an active WAN Internet connection (cellular for the CX series, cellular or wireline broadband for the SR and MX series). This connection must have a publicly reachable IP address.

Similarly, the SonicWall firewall must have an active Internet connection with a publicly reachable IP address.

Sample

The sample configuration below shows a 6350-SR building a tunnel to a SonicWall TZ300 through its cellular modem. A client laptop connected to the LAN Ethernet port of the 6350-SR will be able to access the SonicWall's LAN (and vice versa).



Sample Configuration: 6350-SR

Open the configuration profile for the 6350-SR. Under IPSec, create a new entry with the following settings:

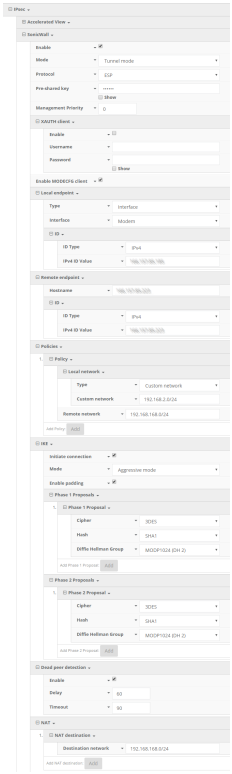
1. Enter in a PSK into the *Pre-shared key*. This must match what is ultimately entered as the SonicWall's "Shared Secret."
2. Check the *Enable MODECFG client* box.
3. Change *Local endpoint* to *Interface* and select the intended route for the IPSec tunnel: "Modem" to leverage a cellular connection or "WAN" for a wireline ISP.
4. Set *Local Endpoint -> ID -> ID type* to "IPv4"
5. Set the local ID in *Local endpoint -> ID -> IPv4 ID Value* to the publicly reachable IP address associated with the selected Interface in step 3.

> NOTE: Leaving *Local endpoint -> type* to *Interface* as *Default route* will allow the tunnel to be built through any available WAN interface.

6. The *Remote endpoint Hostname* is the publicly reachable IP address of the SonicWall.
7. Change *Remote endpoint -> ID -> ID type* to *IPv4*
8. Set the IP address of the SonicWall device in *Remote endpoint -> ID -> IPv4 ID Value* (same value as step 6).
9. Set *IKE -> Mode* to *Aggressive mode*.
10. Set *IKE -> Phase 1 Proposals* and *IKE -> Phase 2 Proposals* to match the IKE settings required by the SonicWall. In this example, both proposals are set to 3DES, SHA1, MODP1024 (DH 2).
11. Under *NAT* click the *Add* button and specify the *Destination network*. This will be the same value entered in the remote policy specified below.

Under IPSec -> Policies, click "Add" to create a new policy, and enter the following settings:

1. Set *Policy -> Local network -> Type* to *Custom network.*
2. Enter the local subnet of the Accelerated router in the *Custom network* field (192.168.2.0/24 by default).
3. Set *Policy -> Remote network* to the IPv4 network you wish to access through the tunnel. (The local subnet of the SonicWall.)



Under Firewall -> Packet filtering, create a new entry by clicking Add and enter the following settings:

Action: Accept

IP Version: IPv4

Protocol: UDP

Secure zone: IPsec

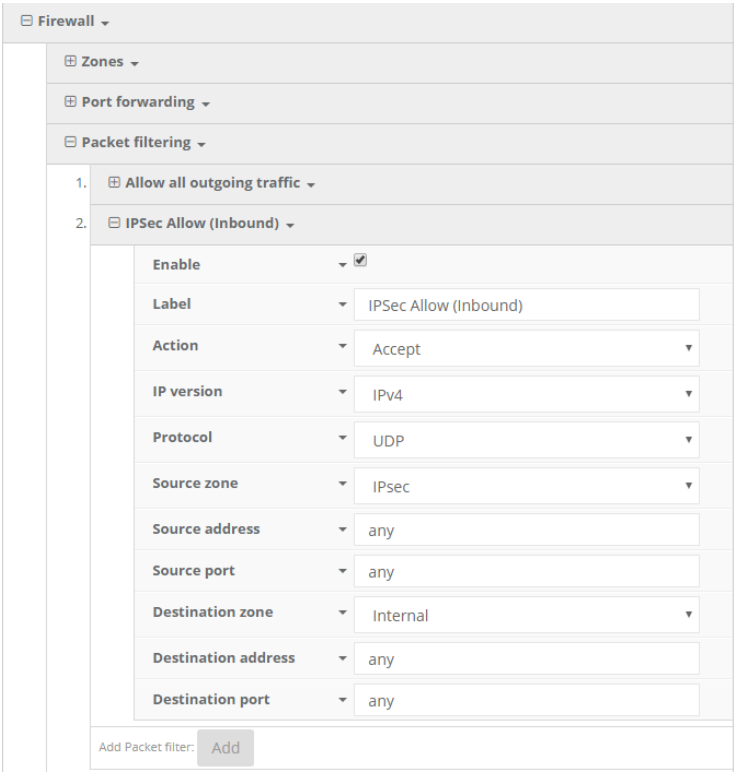
Source address: any

Source port: any

Destination zone: Internal

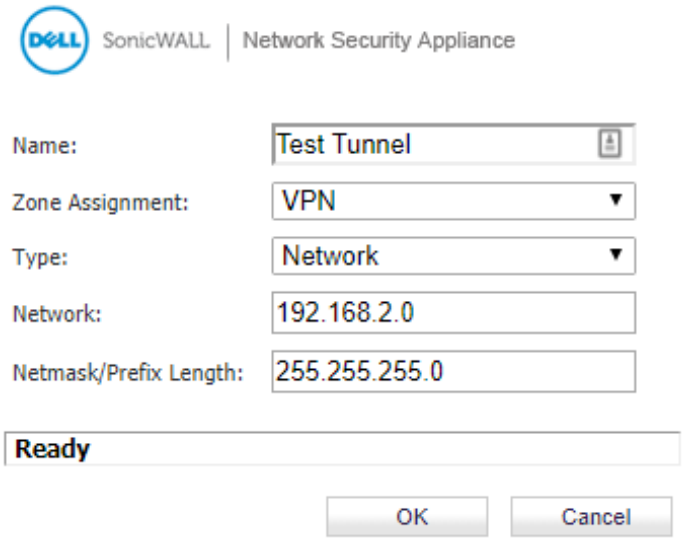
Destination address: any

Destination port: any



Sample Configuration: SonicWall TZ300

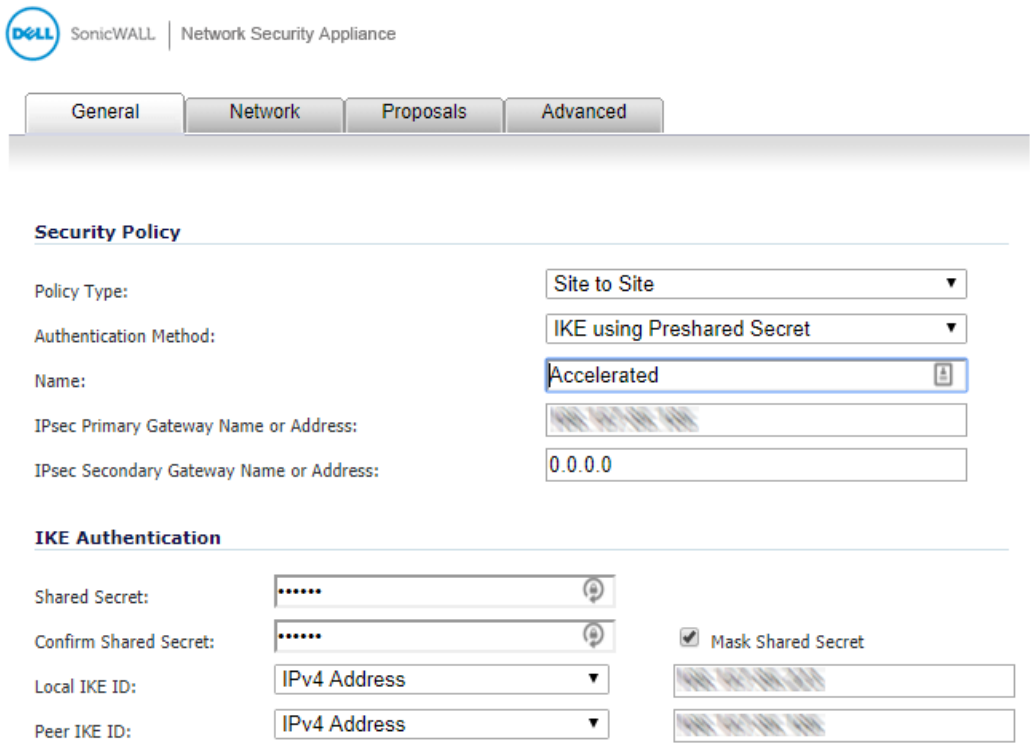
Step 1: Create a new Address Object for VPN Subnets



1. Log in to the SonicWall Management Interface
2. Navigate to *Network > Address Objects*, click on *ADD* button.
3. Configure the Address Object as depicted above, click *Add* and click *Close* when finished.

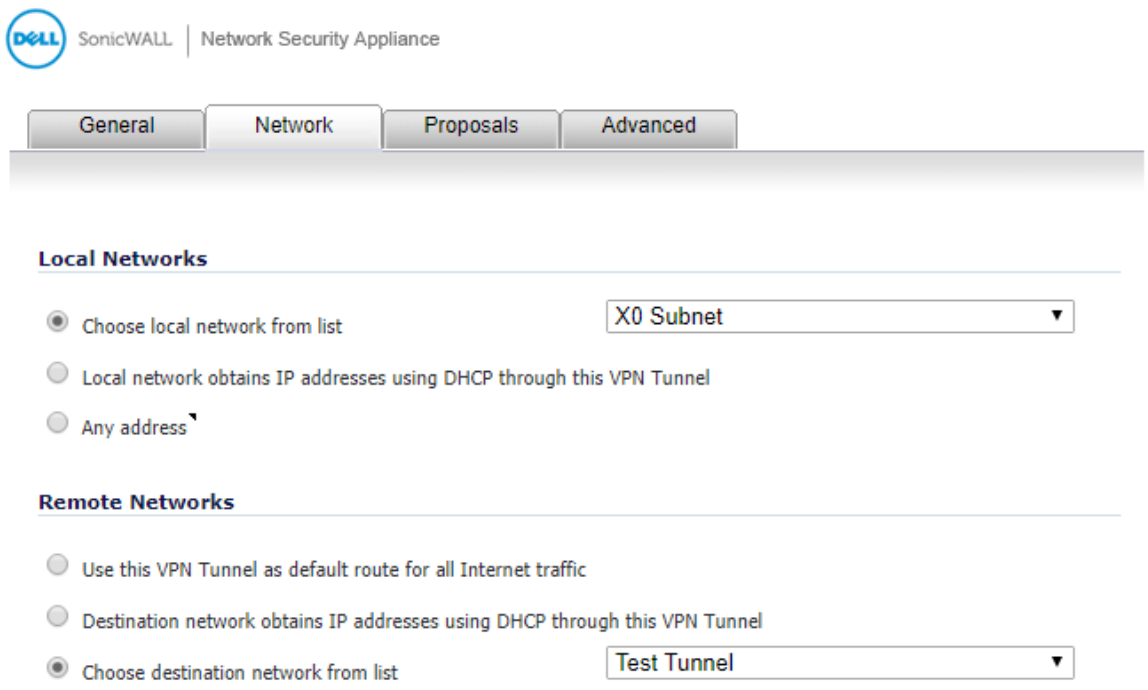
NOTE: The *Network* and *Netmask* must match the local subnet on the Accelerated router. Settings depicted in the screenshot above assume the router is still configured per its defaults.

Step 2: Configure a VPN policy on the SonicWall

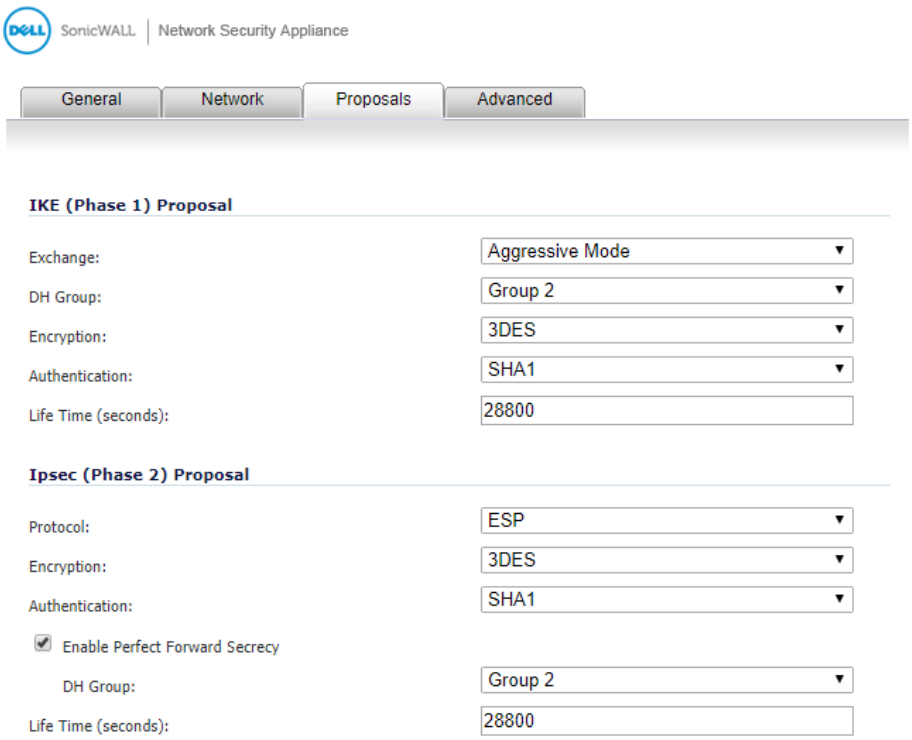


1. Navigate to *VPN > Settings* page. Click *Add* button. The VPN Policy window is displayed.
2. Click the *General* tab.
3. Select *IKE using Preshared Secret* from the *Authentication Method* menu.
4. Enter a name for the policy in the *Name* field.
5. Enter the WAN IP address of the Accelerated connection in the *IPsec Primary Gateway Name or Address* field.
6. Enter a *Shared Secret* password to be used to setup the Security Association the Shared Secret and Confirm Shared Secret fields. The Shared Secret must be at least 4 characters long, and should comprise both numbers and letters.

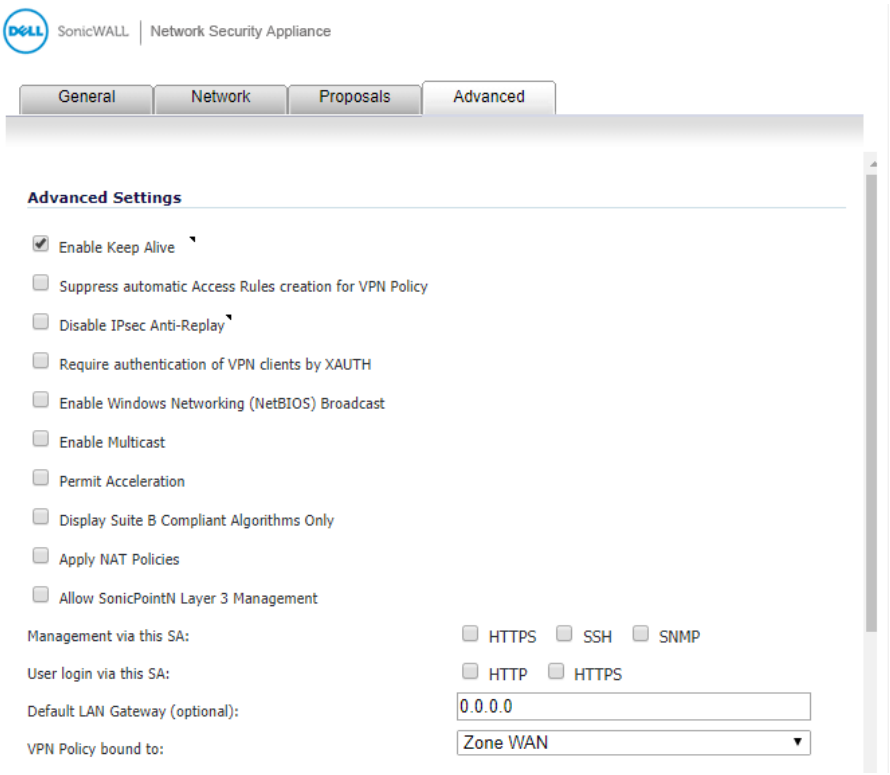
NOTE: The shared secret must match the Pre-shared key entered into the Accelerated configuration.



7. Click the *Network* tab.
8. Under *Local Networks*, select *Choose local network from list* and specify the "X0 Subnet."
9. Under *Remote Networks*, select *Choose destination network from list* and specify the Address Object created in Step 1 above.



10. Click the *Proposals* tab.
11. Under *IKE (Phase 1) Proposal*, change the *Exchange* field to "Aggressive Mode."
12. Leave the default settings for *Encryption* and *Authentication* ("3DES" and "SHA1," respectively) for both *Phase 1* and *Phase 2 Proposals*.
13. *Life Time* may be left at its default value as well.
14. Under *Ipsec (Phase 2) Proposal*, leave "ESP" as the selected *Protocol*
15. Check *Enable Perfect Forward Secrecy*, leaving Group 2 selected in the corresponding field.



16. Click the *Advanced* tab.
17. Select *Enable Keep Alive*.
18. Finalize these settings by clicking the *OK* button.

Configuration for Meraki MX Series

Overview

The Accelerated 6300-CX LTE Router provides a reliable, high-speed cellular connection that is compatible with existing wireline infrastructure. While its 4G LTE speeds are capable of operating as a primary WAN uplink, the 6300-CX can also be configured as a backup. This network redundancy solution delivers the ultimate flexibility to minimize expenses when it comes time for upgrading equipment to the latest wireless standards.

Business continuity depends on the seamless integration of failover-connectivity solutions to prevent service interruptions. Now more than ever, contingency networks play a strategic role in sustaining business operations. Unplanned outages can cost companies significant time and money, frustrating employees and clients alike, which creates a negative perception that is difficult to overcome.

Cellular data (4G LTE) bypasses wireline Internet service providers (ISPs) to facilitate the best redundancy possible. Additionally, in some situations it may be a challenge to acquire access to wired circuits or an event may call for temporary online access. Accelerated Concepts extensively tests the 6300-CX LTE router to ensure its interoperability with a wide variety of security appliances, including equipment produced by Meraki, to best accommodate enterprise networks. Pairing the Accelerated 6300-CX with one of Meraki's MX-series devices offers comprehensive security and flexibility for small business, retail, government, remote sites, and branch offices.

Meraki's MX of Security Appliances are configured using a cloud-based dashboard designed to offer a dynamic management platform reachable via any web browser. From the dashboard, administrators have access to zero-touch provisioning, remote troubleshooting, and real-time reporting on all Meraki equipment within their network. Devices must maintain an active Internet connection to take advantage of cloud functionality, of course, which is why the MX line supports dual WAN interfaces with automated failover and load balancing. The Accelerated 6300-CX's embedded, carrier-certified cellular modem integrates effortlessly with all MX appliances as either the primary or backup uplink.

For additional information, please refer to Meraki's MX-series user guides.

Interoperability Matrix

This section covers interoperability information of the hardware tested for this solution. It includes the firmware versions of both devices as well as the date of testing.

Date	Meraki Firmware	6300-CX Firmware
12/2016	N/A*	16.10.13

*At this time, Meraki does not publish firmware version numbers or specific change logs.

Caveats

The delivery of wireless services varies depending on the carrier and may lead to differences in the area of coverage, type of service (3G, 4G, LTE, etc.), available bandwidth, and IP address designation (Private or Public) among other factors. The interoperability test designed for this solution guide included LTE service, maximum coverage availability, and a public IP address assigned to each device.

Using the 6300-CX as a secondary connection assumes that a primary WAN Ethernet cable is plugged into the Internet-1 port on the Meraki device. Connect the 6300-CX's backup Ethernet cable to port labeled Internet 2 and proceed to the configuration described herein. (Compatible with all MX Security Appliances.)

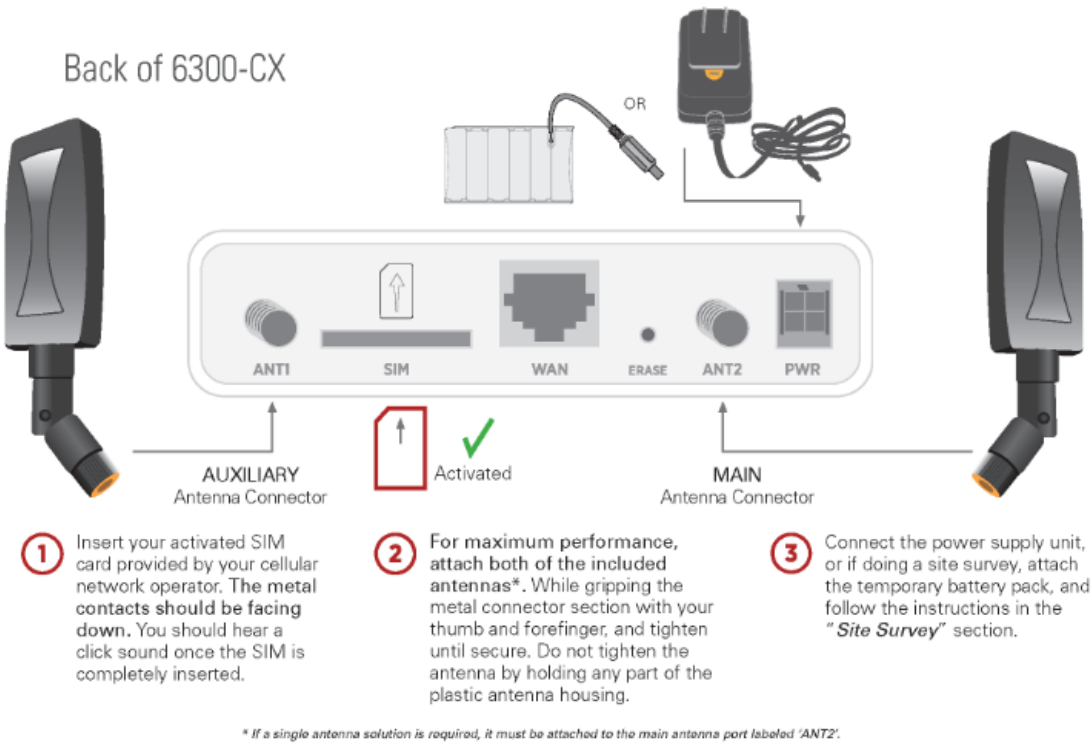
Accelerated 6300-CX LTE Router Setup

Initial Setup

Affix both antennas to the router and insert an activated SIM card before deploying the device. Be sure to select a location with optimal signal strength. For detailed instruction, refer to the tables that follow. Subsequent sections will outline site selection, powering options, and other device functionality.

Step-by-Step Guidance: Initial Setup

1. Insert the activated 2FF SIM card provided by your cellular network operator (putting the cut corner in first with metal contacts facing down). The card clicks into place when completely inserted.
2. Attach the two included antennas; both should be installed for optimal operation. Do this by gripping the metal connector section with your thumb and forefinger, tightening until secure. Do not tighten the antenna by holding any part of the plastic antenna housing.
3. To determine the optimal location for the 6300-CX, please see the “Site Survey” section.
4. Refer to the section(s) for Remote or Direct Power Installations when ready to connect the 6300-CX to the permanent power supply unit.
5. The 6300-CX uses DHCP with IP passthrough by default, which satisfies the setup requirements for most environments. If required, please use Accelerated View™ or the 6300-CX local GUI to configure the 6300-CX for router mode.



Site Survey

If you are unsure of the available cellular signal strength, or are choosing between several locations, please follow the instructions to identify the ideal installation site.

Step-by-Step Guidance: Site Survey

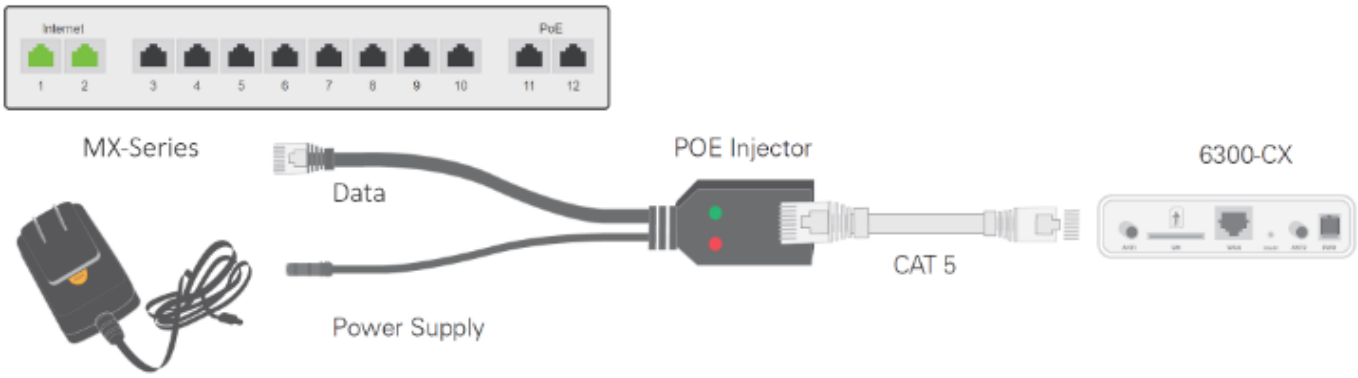
1. After following steps 1 and 2 in the “Initial Setup” section, connect the battery pack to temporarily power the Accelerated 6300-CX. The charge lasts two to four hours – it is not rechargeable and should be properly disposed of after use.
2. Move the 6300-CX to different locations within your site to determine the best compromise between signal strength and installation constraints. Since cellular signal strength may fluctuate, it is important to **wait at each location for 1 minute while observing the signal strength indicator on the front of the device.** Minimum cellular signal strength for operation is 2 bars (3+ is preferred).
3. After determining the optimal location, remove the battery pack and connect the main power supply unit or Ethernet cable connected to the PoE injector (per the power option outlined below).

Remote Power Installation – Power Option #1

The included Power-over-Ethernet (PoE) injector allows the device to be positioned away from power outlets to simplify its installation needs. The adaptor consolidates the DC power and Ethernet connections so that both can be run to the 6300-CX via a single Ethernet cable. Distances of 300 ft have been tested on CAT6 and 250 ft on CAT5e. Note that cable conditions and the number of splices will impact actual distance.

Step-by-Step Guidance: Remote Power Installation

1. Plug the 6300-CX’s power supply unit (PSU) into an AC power outlet.
2. Connect the end of the PSU into the DC input (4 pin connector) of the PoE injector.
3. Insert the male RJ45 connector of the PoE injector cable into the Meraki.
4. Connect an Ethernet cable from the RJ45 socket on the PoE injector cable to the Ethernet port of the 6300-CX. (See diagram.)

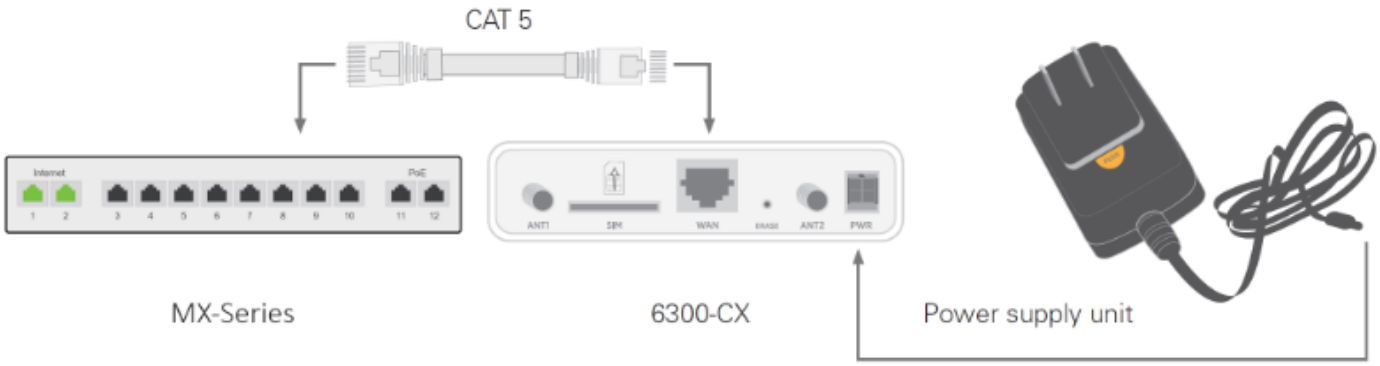


Direct Power Installation – Power Option #2

If you plan to collocate the 6300-CX with the MX device, you can directly power the 6300-CX without the PoE cable.

Step-by-Step Guidance: Direct Power Installation

1. Use an Ethernet cable to connect the 6300-CX to the security appliance using port Internet 1 (to use the cellular network as the primary connection) or port Internet 2 (to configure a failover).
2. Plug the 6300-CX power supply unit (PSU) into an AC power outlet.
3. Connect the PSU into the 4-pin power connector of the 6300-CX. (See diagram.)

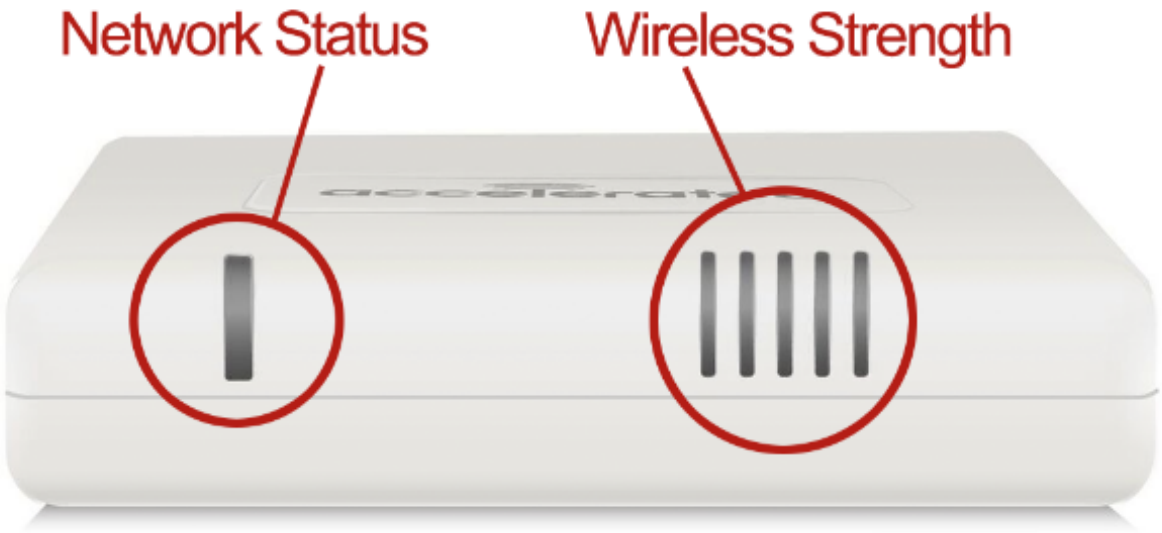


Understanding the 6300-CX LEDs

Once power has been established, your device will initialize and attempt to connect to the network. Device initialization may take 30-60 seconds. Indicator lights on the **Wireless Strength**

Indicator show you the cellular network signal strength. The Network Status Light on the front left of the device displays connectivity information.

Please visit accelerated.com for additional information and troubleshooting tips.



Network Status LED

Solid Yellow
Initializing or starting up.

Flashing Yellow
In the process of connecting to the cellular network and to a device on its Ethernet port.

Flashing White
Has an Ethernet connection and is in the process of connecting to the cellular network.

Flashing Green
Connected to 2G or 3G and is in the process of connecting to a device on its Ethernet port (or nothing is connected to the port).

Solid Green
Connected to 2G or 3G and also has an Ethernet connection.

Flashing Blue
Connected to 4G LTE and in the process of connecting to a device on its Ethernet port.

Solid Blue
Connected to 4G LTE and also has an Ethernet connection.

Alternating Red/ Yellow
Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Wireless Strength LEDs

Signal Bars	Weighted dBm	Signal Strength %	Quality
	-113 to -99	0 - 23%	Bad
	-98 to -87	24 - 42%	Marginal
	-86 to -76	43 - 61%	OK
	-75 to -64	62 - 80%	Good
	-63 to -51	81 - 100%	Excellent

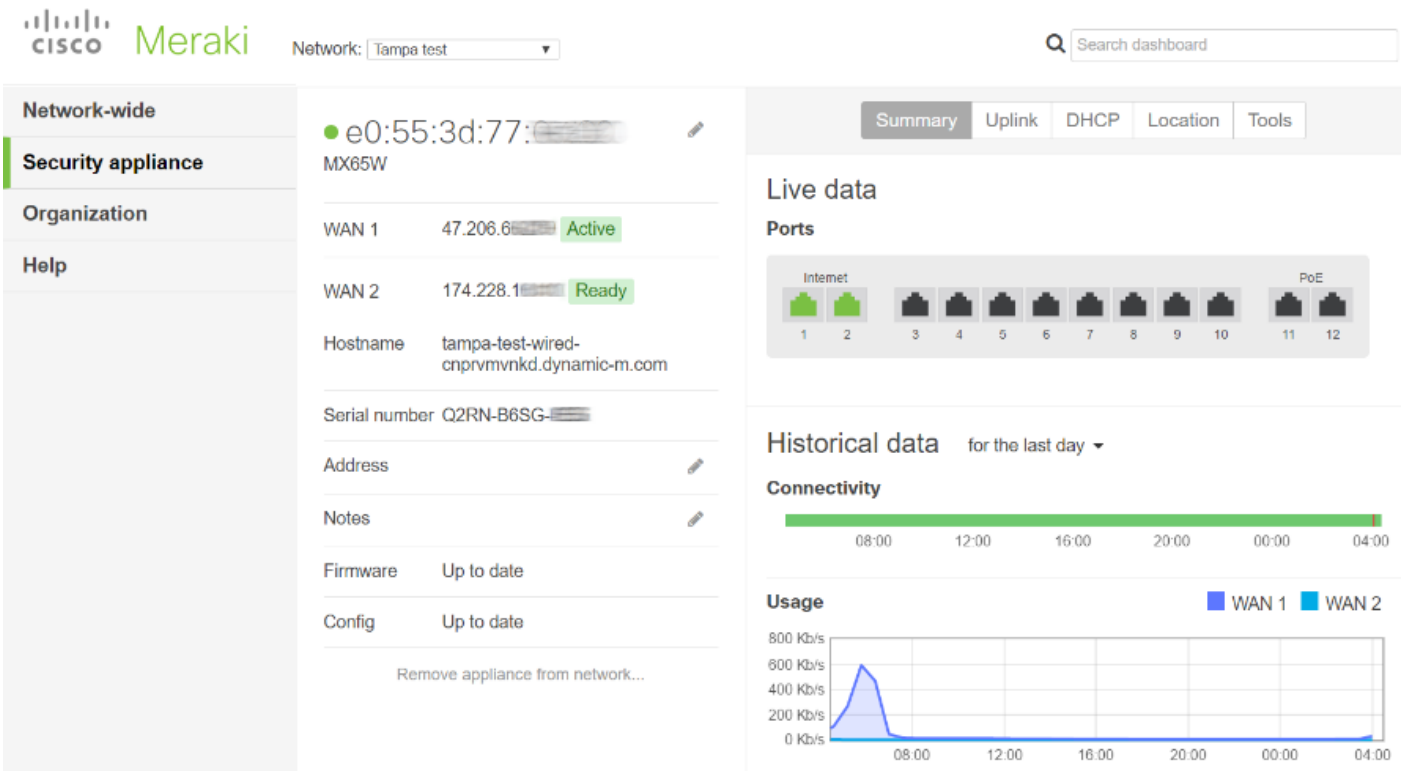
MX-Series Configuration with the Accelerated 6300-CX

Dual WAN Configuration

All Meraki MX Security Appliances support dual WAN connectivity right out of the box. To establish primary and secondary uplinks, connect an Ethernet cable from your modem to one of the interfaces labeled Internet 1 or Internet 2 on the back of the MX appliance. The secondary connection, WAN 2 unless otherwise specified, activates automatically to keep the device online should its primary WAN lose connectivity. While load balancing between the two uplinks is disabled by default, it and other traffic-related preferences can be configured to a

variety of specifications via the **Traffic shaping** menu option found in the dashboard's **Security appliance** tab.

Access the Meraki dashboard at [dashboard.meraki.com.](dashboard.meraki.com)



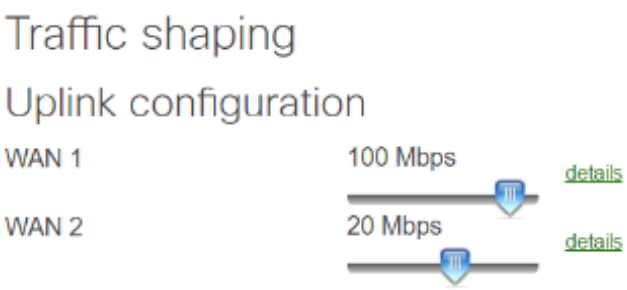
Please refer to the MX Quick Start guide for an in-depth walkthrough of how to manage your Meraki MX device.

Step-by-Step Guidance: Dual WAN Configuration

***NOTE:** Verify the device's MAC address, found on the bottom label of the MX series, to ensure the correct device is selected in the dashboard. (MACs, IPs, and Serial #s have been partially obscured in the screenshot above.)*

1. From the **Security appliance** tab of the admin portal, select **Appliance status** (found under **Monitor**).
2. The **Live data** view shows which interfaces are currently in use by highlighting active ports green. When configured for primary and secondary internet connections, the device should indicate activity on its first two ports – Internet 1 and Internet 2.
3. Each connection's IP address is displayed next to its WAN designation along with its connection status.

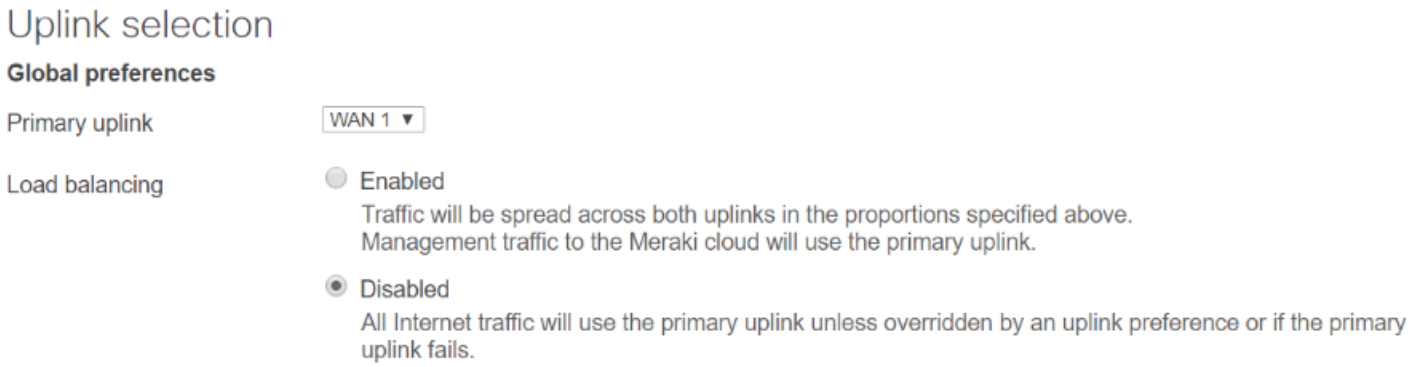
Load Balancing and Automatic Failover



From the Meraki dashboard, MX Security Appliances can be configured for customized WAN utilization, or "traffic shaping," which allows network administrators to model the flow of data according to the needs and specifications of their enterprise environment.

The **uplink configuration** sliders define the throughput for WAN 1 and WAN 2 to implement load distribution (or load balancing) across the two connections. When set to differing values, a ratio is established that defines flow control. For example, setting WAN 1 to 100 Mbps and WAN 2 to 20 Mbps creates a 5:1 ratio between the two for every five "flows" sent over WAN 1, a single flow will be sent over WAN 2.

Before the uplink configuration takes effect, load balancing must be initialized from the corresponding menu option found under **Global preferences**. Traffic will route according to the slider-defined proportion so long as the feature is enabled. When disabled, data transmission defaults to the primary uplink. Exceptions can be defined on a case-by-case basis with or without active load balancing via flow preferences and traffic-shaping rules.



Please refer to the Meraki knowledge article for an in-depth walkthrough of load balancing and flow preferences.

Step-by-Step Guidance: Load Balancing and Automatic Failover

NOTE: Clicking the details link allows for upload- and download-specific settings.

1. From the **Security appliance** tab of the admin portal, select **Traffic shaping** (found under **Configure**).
2. Use the **Uplink configuration** sliders to establish a proportional rate between WAN 1 and WAN 2.
3. These settings are not active until selecting **Enable** next to **Load balancing** under the **Global preferences** heading of the **Uplink selection** menu.
4. The **Primary uplink** pull-down establishes which WAN serves as the primary connection. The secondary WAN handles traffic only when load balancing is enabled (or if the primary WAN goes offline).
5. Define any exceptions by setting **Flow preferences** or **Traffic-shaping rules**, which allows for utilization of the secondary WAN on a case-by-case basis.

Configuration for Fortinet FortiGate Series

Overview

The Accelerated 6300-CX LTE Router provides a reliable, high-speed cellular connection that is compatible with existing wireline infrastructure. While its 4G LTE speeds are capable of operating as a primary WAN uplink, the 6300-CX can also be configured as a backup. This network redundancy solution delivers the ultimate flexibility to minimize expenses when it comes time for upgrading equipment to the latest wireless standards.

Business continuity depends on the seamless integration of failover-connectivity solutions to prevent service interruptions. Now more than ever, contingency networks play a strategic role in sustaining business operations. Unplanned outages can cost companies significant time and money, frustrating employees and clients alike, which creates a negative perception that is difficult to overcome.

Cellular data (4G LTE) bypasses wireline Internet service providers (ISPs) to facilitate the best redundancy possible. Additionally, in some situations it may be a challenge to acquire access to wired circuits or an event may call for temporary online access. Accelerated Concepts extensively tests the 6300-CX LTE router to ensure its interoperability with a wide variety of security appliances, including equipment produced by Fortinet, to best accommodate enterprise networks. Pairing the Accelerated 6300-CX with a dedicated firewall offers comprehensive security and flexibility for small business, retail, government, remote sites, and branch offices.

Fortinet's FortiGate series of next-generation firewalls (NGFWs) offers award-winning network security capable of accommodating all scales of distributed enterprise data usage. FortiGate NGFWs are powered by the proprietary FortiASIC SoC3 technology, which consolidates its security and networking functionality into a single, optimized SoC (system on a chip). This innovative architecture surpasses industry standards for data throughput, latency, and the hosting of concurrent sessions, all while reducing each model’s power consumption and heat signature. Network performance settings, such as WAN Optimization and Load Balancing, can be configured locally via command-line interface (CLI) or centrally by way of FortiOS to communicate with all FortiGates connected to the same environment.

For additional information, please refer to Fortinet's FortiOS Handbook.

Interoperability Matrix

This section covers interoperability information of the hardware tested for this solution. It includes the firmware versions of both devices as well as the date of testing.

Date	Fortigate Firmware	6300-CX Firmware
12/2016	5.4.3	16.11.142

Caveats

The delivery of wireless services varies depending on the carrier and may lead to differences in the area of coverage, type of service (3G, 4G, LTE, etc.), available bandwidth, and IP address designation (Private or Public) among other factors. The interoperability test designed for this solution guide included LTE service, maximum coverage availability, and a public IP address assigned to each device.

Using the 6300-CX as a secondary connection assumes that a primary WAN Ethernet cable is plugged into port WAN 1 on the Fortinet device. Connect the 6300-CX's backup Ethernet cable to port labeled WAN 2 and proceed to the configuration described herein. (Compatible with all FortiGate Series Firewalls.)

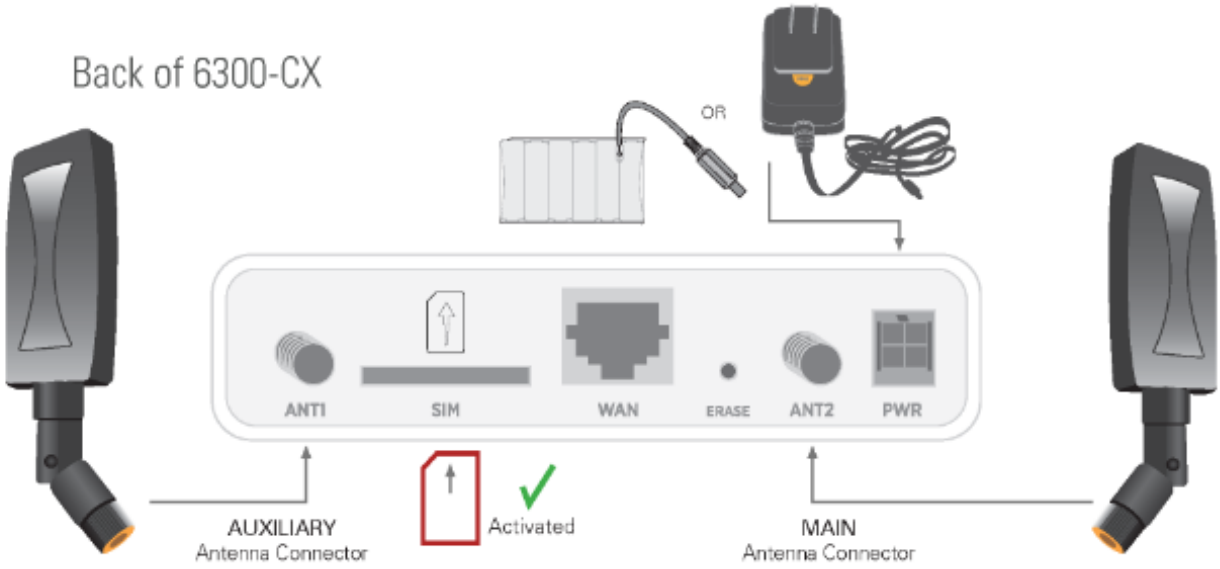
Initial Setup

Affix both antennas to the router and insert an activated SIM card before deploying the device. Be sure to select a location with optimal signal strength. For detailed instruction, refer to the tables that follow. Subsequent sections will outline site selection, powering options, and other device functionality.

Step-by-Step Guidance: Initial Setup

1. Insert the activated 2FF SIM card provided by your cellular network operator (putting the cut corner in first with metal contacts facing down). The card clicks into place when completely inserted.
2. Attach the two included antennas; both should be installed for optimal operation. Do this by gripping the metal connector section with your thumb and forefinger, tightening until secure. Do not tighten the antenna by holding any part of the plastic antenna housing.
3. To determine the optimal location for the 6300-CX, please see the "Site Survey" section.
4. Refer to the section(s) for Remote or Direct Power Installations when ready to connect the 6300-CX to the permanent power supply unit.

5. The 6300-CX uses DHCP with IP Passthrough by default, which satisfies the setup requirements for most environments. If required, please use Accelerated View™ or the 6300-CX local GUI to configure the 6300-CX for router mode.



Site Survey

If you are unsure of the available cellular signal strength, or are choosing between several locations, please follow the instructions to identify the ideal installation site.

Step-by-Step Guidance: Site Survey

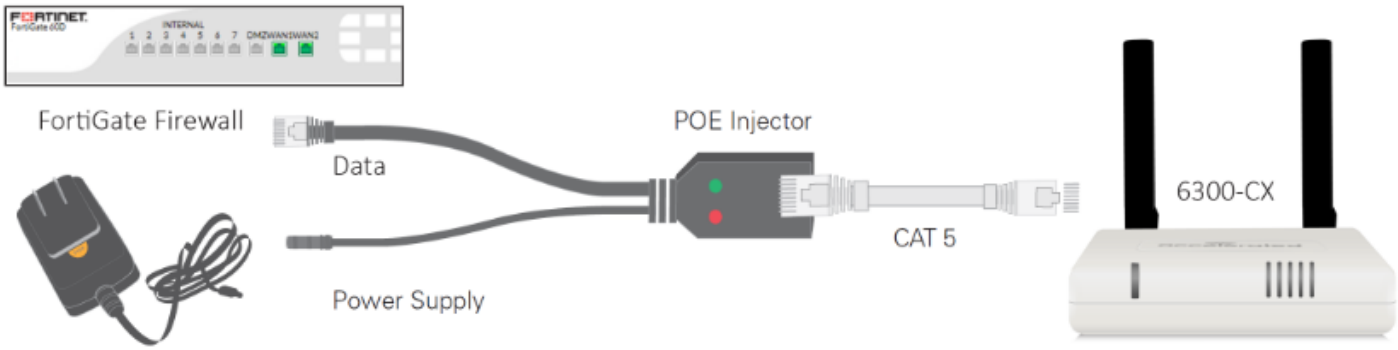
1. After following steps 1 and 2 in the “Initial Setup” section, connect the battery pack to temporarily power the Accelerated 6300-CX. The charge lasts two to four hours – it is not rechargeable and should be properly disposed of after use.
2. Move the 6300-CX to different locations within your site to determine the best compromise between signal strength and installation constraints. Since cellular signal strength may fluctuate, it is important to **wait at each location for 1 minute while observing the signal strength indicator** on the front of the device. Minimum cellular signal strength for operation is 2 bars (3+ is preferred).
3. After determining the optimal location, remove the battery pack and connect the main power supply unit or Ethernet cable connected to the PoE injector (per the power option outlined below).

Remote Power Installation – Powering Option #1

The included Power-over-Ethernet (PoE) injector allows the device to be positioned away from power outlets to simplify its installation needs. The adaptor consolidates the DC power and Ethernet connections so that both can be run to the 6300-CX via a single Ethernet cable. Distances of 300 ft have been tested on CAT6 and 250 ft on CAT5e. Note that cable conditions and the number of splices will impact actual distance.

Step-by-Step Guidance: Remote Power Installation

1. Plug the 6300-CX's power supply unit (PSU) into an AC power outlet.
2. Connect the end of the PSU into the DC input (4 pin connector) of the PoE injector.
3. Insert the male RJ45 connector of the PoE injector cable into the firewall.
4. Connect an Ethernet cable from the RJ45 socket on the PoE injector cable to the Ethernet port of the 6300-CX. (See diagram.)

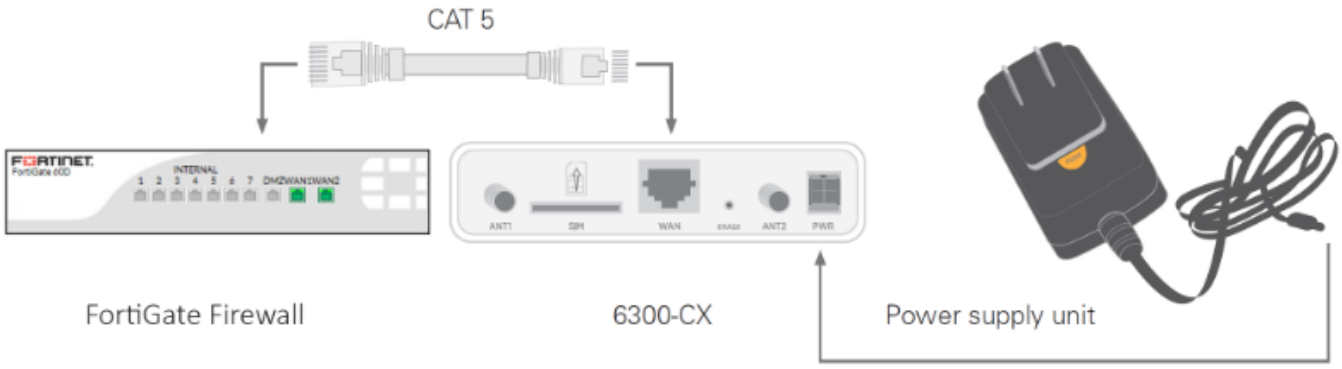


Direct Power Installation – Powering Option #2

If you plan to collocate the 6300-CX with the firewall device, you can directly power the 6300-CX without the PoE cable.

Step-by-Step Guidance: Direct Power Installation

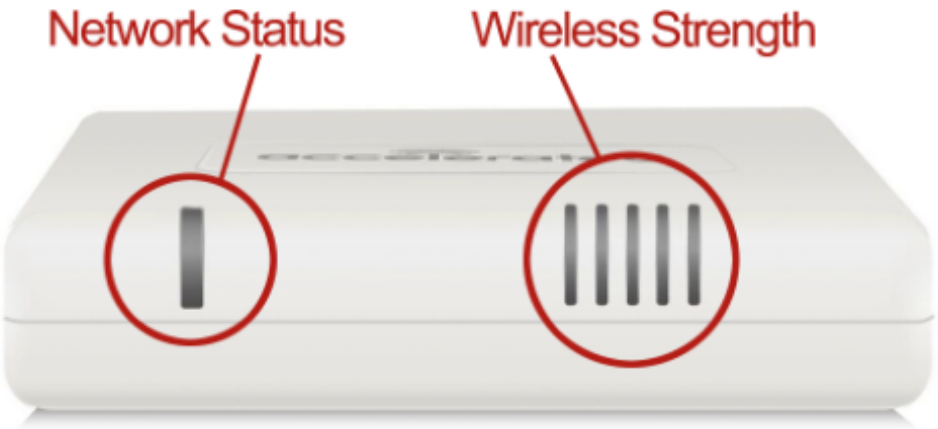
1. Use an Ethernet cable to connect the 6300-CX to the security appliance using port wan1 (to use the cellular network as the primary connection) or port wan2 (to configure a failover).
2. Plug the 6300-CX power supply unit (PSU) into an AC power outlet.
3. Connect the PSU into the 4-pin power connector of the 6300-CX. (See diagram.)



Understanding the 6300-CX LEDs

Once power has been established, your device will initialize and attempt to connect to the network. Device initialization may take 30-60 seconds. Indicator lights on the **Wireless Strength Indicator** show you the Cellular Network Signal Strength. The **Network Status Light** on the front left of the device displays connectivity information.

Please visit www.accelerated.com for additional information and trouble-shooting tips.



Network Status LED

Solid Yellow
Initializing or starting up.

Flashing Yellow
In the process of connecting to the cellular network and to a device on its Ethernet port.

Flashing White
Has an Ethernet connection and is in the process of connecting to the cellular network.

Flashing Green
Connected to 2G or 3G and is in the process of connecting to a device on its Ethernet port (or nothing is connected to the port).

Solid Green
Connected to 2G or 3G and also has an Ethernet connection.

Flashing Blue
Connected to 4G LTE and in the process of connecting to a device on its Ethernet port.

Solid Blue
Connected to 4G LTE and also has an Ethernet connection.

Alternating Red/ Yellow
Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Wireless Strength LEDs

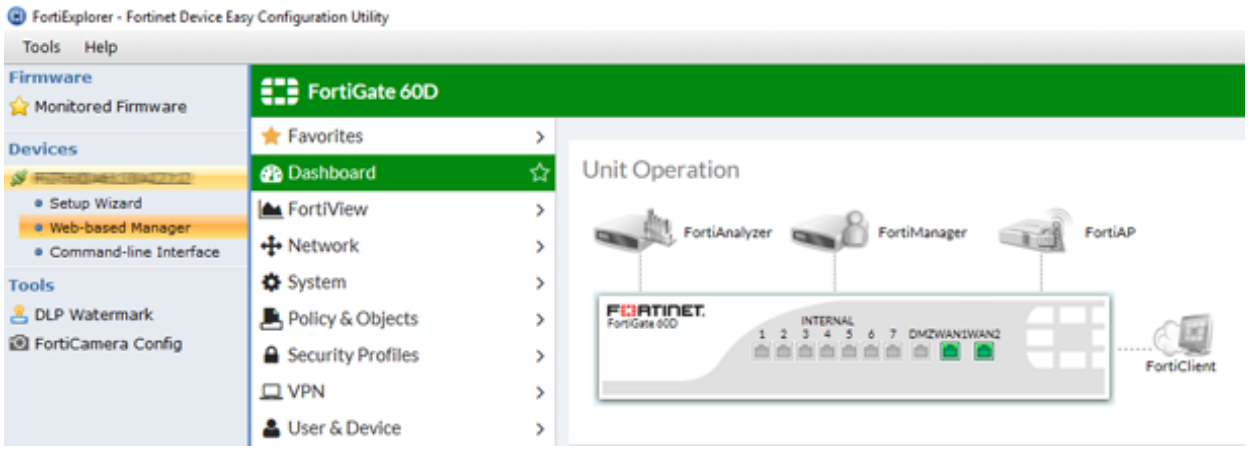
Signal Bars	Weighted dBm	Signal Strength %	Quality
	-113 to -99	0 - 23%	Bad
	-98 to -87	24 - 42%	Marginal
	-86 to -76	43 - 61%	OK
	-75 to -64	62 - 80%	Good
	-63 to -51	81 - 100%	Excellent

FortiGate Configuration with the Accelerated 6300-CX

Verify Interface Settings

IP Policies and Static Routes serve as the foundation for how firewalls control and shape the flow of data through the networks they safeguard. FortiGate devices come preconfigured with security settings in place, though these routes and policies assume a traditional, single-WAN setup. It is critical to remove any default values before implementing failover to ensure proper traffic prioritization.

NOTE: Device administration is best handled using the FortiExplorer desktop application, which connects a computer to the firewall via its USB MGMT console port. (Both the CLI and web-facing GUI, FortiOS, are available using this tool.) If necessary, FortiOS can also be accessed via its default gateway IP: 192.168.1.99.



For an in-depth walkthrough of how to manage your FortiGate device, please refer to Fortinet's [FortiOS Handbook](#).

Step-by-Step Guidance: Verify Interfaces, Routes, and Policies

*NOTE: Both wan1 and wan2 should be set for DHCP **Addressing** mode.*

1. From the **Web-based Manager**, expand the **Network** menu and navigate to **Interfaces**.
2. Confirm that both wan1 and wan2 are online, indicated by the green arrow pointing up.
3. View interface details by double clicking on its entry in the **Physical** table.
4. Set wan1's **Distance** value so it's LOWER than the value used for wan2 (e.g. set wan1 to 1 and wan2 to 5).
5. Deactivate **Override internal DNS** if it is enabled.
6. Click **OK** to finalize any configuration changes.
7. Select **Routing** from the **Network** menu – delete any pre-defined **Static Routes**.
8. Expand the **Policy & Objects** menu and navigate to **IPv4 Policy** – delete all existing policies for wan1 & 2.

NOTE: Please refer to Fortinet's guidance on how to perform a configuration backup if there is concern over being able to recreate any policies or routes.

Dual-WAN Routes and Policies

The FortiGate device is ready for dual-WAN configuration once its preexisting settings have been cleared out and its two WAN connections are properly set (per the guidance from page 6 of this document). Any active interface must have an IPv4 Policy defined in order to bypass the "Implicit Deny" default policy that is used as a failsafe for unauthorized traffic. Networks can then leverage advanced prioritization options to further reinforce the failover redundancy provided by the 6300-CX's backup LTE connection by establishing a static route for each WAN interface.

For an in-depth walkthrough of how to manage your FortiGate device, please refer to Fortinet's FortiOS Handbook.

Step-by-Step Guidance: Dual-WAN Routes and Policies

NOTE: *Just like the **Distance** value set during Interface setup (step 4 on the previous page), FortiGate firewalls give precedence to whichever static route has the lowest **Priority** value.*

1. From the **Web-based Manager**, expand the **Network** menu and navigate to **Routing**.
2. Click the **Create New** button under the **Static Routes** section.
3. Select a **Device:** either wan1 or wan2.

4. Enter the **Gateway** IP address, which can be found by viewing the uplink's corresponding entry in the **Interfaces** menu.
5. Also enter this Gateway IP into the **Destination** field.
6. Expand **Advanced Options** and set the **Priority** for wan1 so that its value is LOWER than wan2 to establish failover prioritization.
7. Click **OK** to finalize any configuration changes.
8. Repeat steps 1–7 for the second WAN interface, ensuring that the intended primary connection has the lowest priority value.
9. Expand the **Policy & Objects** menu and navigate to **IPv4 Policy**.
10. Click the **Create New** button found at the top of the screen.
11. Set the **Incoming Interface** to "internal" and the **Outgoing Interface** to the intended WAN uplink (1 or 2).
12. Enter a **Name** that corresponds to the **Outgoing Interface** (e.g. "Primary" for wan1).
13. Select "All" for the **Source**, **DestinationAddress**, and **Service**.
14. Unless otherwise required per existing security standards, all other values can be left as defaults.
15. Ensure **Enable this policy** is active and click **OK** to finalize its configuration.
16. Repeat steps 9–15 for the second WAN interface.

WAN Status Check

Failover is established by the proper configuration of two WAN interfaces as well as their related policies and routes, which ensures the FortiGate knows how to reroute traffic if its active uplink goes offline. The backup/ secondary connection, however, will stay active indefinitely unless WAN Status Check is activated and configured.

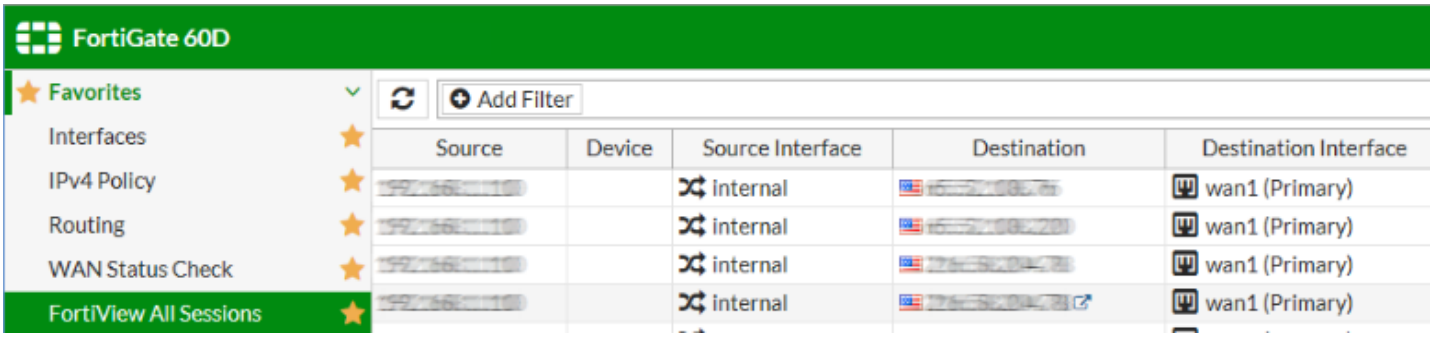
For an in-depth walkthrough of how to manage your FortiGate device, please refer to Fortinet's FortiOS Handbook.

Step-by-Step Guidance: FortiView Verification

1. From the **Web-based Manager**, expand the **Network** menu and navigate to **WAN Status Check**.
2. Click the **Create New** button found at the top of the screen.
3. Enter a **Name** for tracking purposes (e.g. Active Recovery).
4. Set the **Protocol** as "Ping".
5. Unless an alternative is preferred, point the **Server** to "8.8.8.8".
6. The **Link Status** fields can be adjusted as necessary; the default values suffice.

FortiView Verification

FortiView provides real-time monitoring of traffic flowing through FortiGate devices. After completing the Accelerated 6300-CX configuration to establish backup connectivity, FortiView can confirm that both the failover and failback mechanisms are functioning as intended.



For an in-depth walkthrough of how to manage your FortiGate device, please refer to Fortinet's [FortiOS Handbook](#).

Step-by-Step Guidance: FortiView Verification

1. From the **Web-based Manager**, expand the **FortiView** menu and navigate to **All Sessions**.
2. Reference the **Destination Interface** column to see which WAN uplink is currently active (wan1 unless there is a service interruption).
3. To confirm failover, unplug the Ethernet cable from the wan1 Interface. Refresh the **All Sessions** view to see wan2 become the new **Destination Interface**, and similarly confirm wan1 reverts to being the active interface once it is reconnected.

Configuration for Juniper SRX Series

Overview

The Accelerated 6300-CX LTE Router provides a reliable, high-speed cellular connection that is compatible with existing wireline infrastructure. While its 4G LTE speeds are capable of operating as a primary WAN uplink, the 6300-CX can also be configured as a backup. This network redundancy solution delivers the ultimate flexibility to minimize expenses when it comes time for upgrading equipment to the latest wireless standards.

Business continuity depends on the seamless integration of failover-connectivity solutions to prevent service interruptions. Now more than ever, contingency networks play a strategic role in sustaining business operations. Unplanned outages can cost companies significant time and money, frustrating employees and clients alike, which creates a negative perception that is difficult to overcome.

Cellular data (4G LTE) bypasses wireline Internet service providers (ISPs) to facilitate the best redundancy possible. Additionally, in some situations it may be a challenge to acquire access to wired circuits or an event may call for temporary online access. For these reasons Juniper and Accelerated Concepts have teamed up to offer comprehensive security and flexibility for small businesses, retail, government, remote sites, and branch offices.

Combining next-generation firewall functionality with unified threat management (UTM) services, the Juniper SRX Series Services Gateways provides high-performance, cost-effective network security. It optimizes and fortifies networked environments thanks to a robust suite of administrative utilities ranging from automated configuration to enhanced Web filtering though this functionality hinges upon an active WAN connection. An SRX Series device paired with an Accelerated 6300-CX LTE Router will ensure your enterprise network remains secure and operational should its primary ISP go offline. Running a cellular backup via an Ethernet cable preserves the full security functionality of the SRX Gateway, which isn't the case for USB-connected Aircards.

For additional information, please refer to Juniper's SRX Series datasheet and the J-Web User Guide.

Interoperability Matrix

This section covers interoperability information of the hardware tested for this solution. It includes the firmware versions of both devices as well as the date of testing.

Date	JUNOS Release	6300-CX Firmware
05/2017	15.1X49-D5	17.2.22

Caveats

The delivery of wireless services varies depending on the carrier and may lead to differences in the area of coverage, type of service (3G, 4G, LTE, etc.), availability of bandwidth, and IP address designation (Private or Public) among other factors. The interoperability test designed for this solution guide included LTE service, maximum coverage availability, and a public IP address assigned to each device.

Using the 6300-CX as a secondary connection assumes that a primary WAN Ethernet cable is plugged into the 0/0 port on the Juniper device. Connect the 6300-CX's backup Ethernet cable to port 0/2 and proceed to the configuration described herein. (Compatible with all SRX Series Services Gateways.)

Accelerated 6300-CX LTE Router Setup

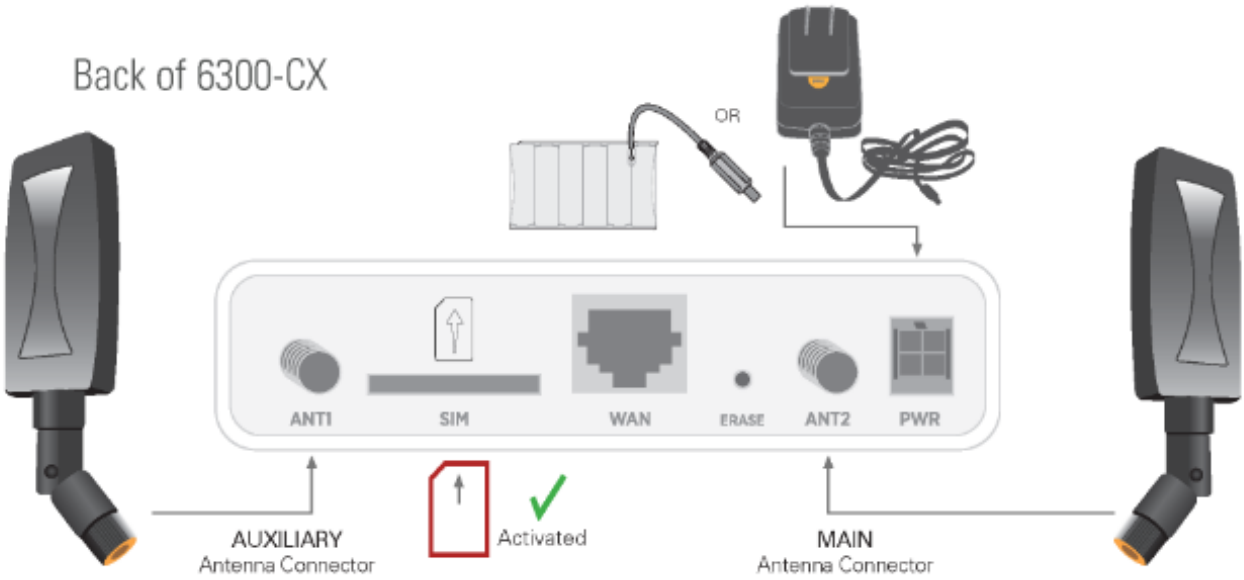
Initial Setup

Affix both antennas to the router and insert an activated SIM card before deploying the device. Be sure to select a location with optimal signal strength. For detailed instruction, refer to the tables that follow. Subsequent sections will outline site selection, powering options, and other device functionality.

Step-by-Step Guidance: Initial Setup

1. Insert the activated 2FF SIM card provided by your cellular network operator (putting the cut corner in first with metal contacts facing down). The card clicks into place when completely inserted.

2. Attach the two included antennas; both should be installed for optimal operation. Do this by gripping the metal connector section with your thumb and forefinger, tightening until secure. Do not tighten the antenna by holding any part of the plastic antenna housing.
3. To determine the optimal location for the 6300-CX, please see the “Site Survey” section.
4. Refer to the section(s) for Remote or Direct Power Installations when ready to connect the 6300-CX to the permanent power supply unit.
5. The 6300-CX uses DHCP with IP passthrough by default, which satisfies the setup requirements for most environments. If required, please use Accelerated View™ or the 6300-CX local GUI to configure the 6300-CX for router mode.



Site Survey

If you are unsure of the available cellular signal strength, or are choosing between several locations, please follow the instructions to identify the ideal installation site

Step-by-Step Guidance: Site Survey

1. After following steps 1 and 2 in the “Initial Setup” section, connect the battery pack to temporarily power the Accelerated 6300-CX. The charge lasts two to four hours – it is not rechargeable and should be properly disposed of after use.
2. Move the 6300-CX to different locations within your site to determine the best compromise between signal strength and installation constraints. Since cellular signal strength may fluctuate, it is important to **wait at each location for 1 minute while observing the signal strength indicator** on the front of the device. Minimum cellular signal strength for operation is 2 bars (3+ is preferred).

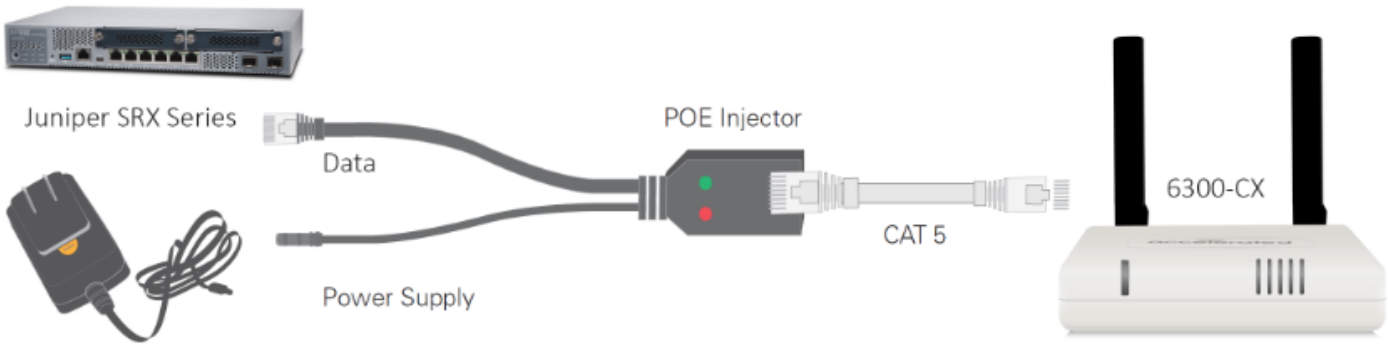
3. After determining the optimal location, remove the battery pack and connect the main power supply unit or Ethernet cable connected to the PoE injector (per the power option outlined below).

Remote Power Installation – Powering Option #1

The included Power-over-Ethernet (PoE) injector allows the device to be positioned away from power outlets to simplify its installation needs. The adaptor consolidates the DC power and Ethernet connections so that both can be run to the 6300-CX via a single Ethernet cable. Distances of 300 ft have been tested on CAT6 and 250 ft on CAT5e. Note that cable conditions and the number of splices will impact actual distance.

Step-by-Step Guidance: Remote Power Installation

1. Plug the 6300-CX's power supply unit (PSU) into an AC power outlet.
2. Connect the end of the PSU into the DC input (4 pin connector) of the PoE injector.
3. Insert the male RJ45 connector of the PoE injector cable into the SRX device.
4. Connect an Ethernet cable from the RJ45 socket on the PoE injector cable to the Ethernet port of the 6300-CX. (See diagram.)

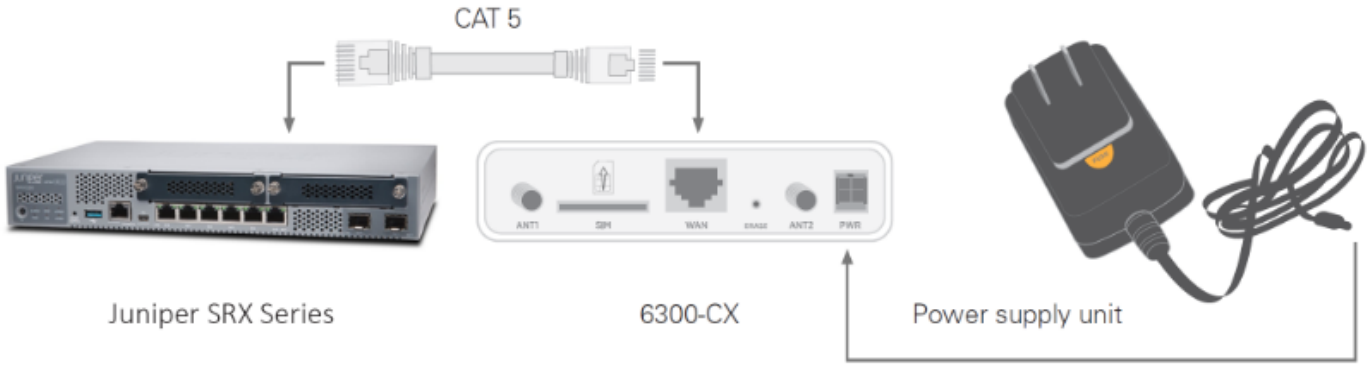


Direct Power Installation – Powering Option #2

If you plan to collocate the 6300-CX with the MX device, you can directly power the 6300-CX without the PoE cable.

Step-by-Step Guidance: Direct Power Installation

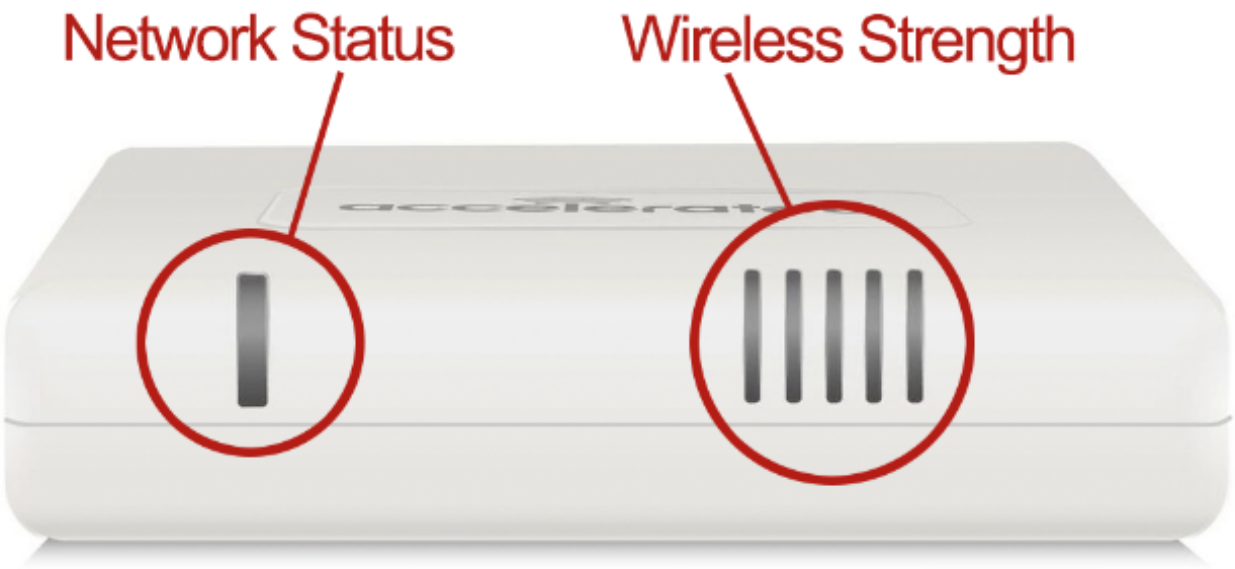
1. Use an Ethernet cable to connect the 6300-CX to the security appliance using port Internet 1 (to use the cellular network as the primary connection) or port Internet 2 (to configure a failover).
2. Plug the 6300-CX power supply unit (PSU) into an AC power outlet.
3. Connect the PSU into the 4-pin power connector of the 6300-CX. (See diagram.)



Understanding the 6300-CX LEDs

Once power has been established, your device will initialize and attempt to connect to the network. Device initialization may take 30-60 seconds. Indicator lights on the **Wireless Strength Indicator** show you the cellular network signal strength. The **Network Status Light** on the front left of the 6300-CX displays connectivity information.

Please visit *www.accelerated.com* for additional information and troubleshooting tips.



Network Status LED

Solid Yellow
Initializing or starting up.

Flashing Yellow
In the process of connecting to the cellular network and to a device on its Ethernet port.

Flashing White
Has an Ethernet connection and is in the process of connecting to the cellular network.

Flashing Green
Connected to 2G or 3G and is in the process of connecting to a device on its Ethernet port (or nothing is connected to the port).

Solid Green
Connected to 2G or 3G and also has an Ethernet connection.

Flashing Blue
Connected to 4G LTE and in the process of connecting to a device on its Ethernet port.

Solid Blue
Connected to 4G LTE and also has an Ethernet connection.

Alternating Red/ Yellow
Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Wireless Strength LEDs

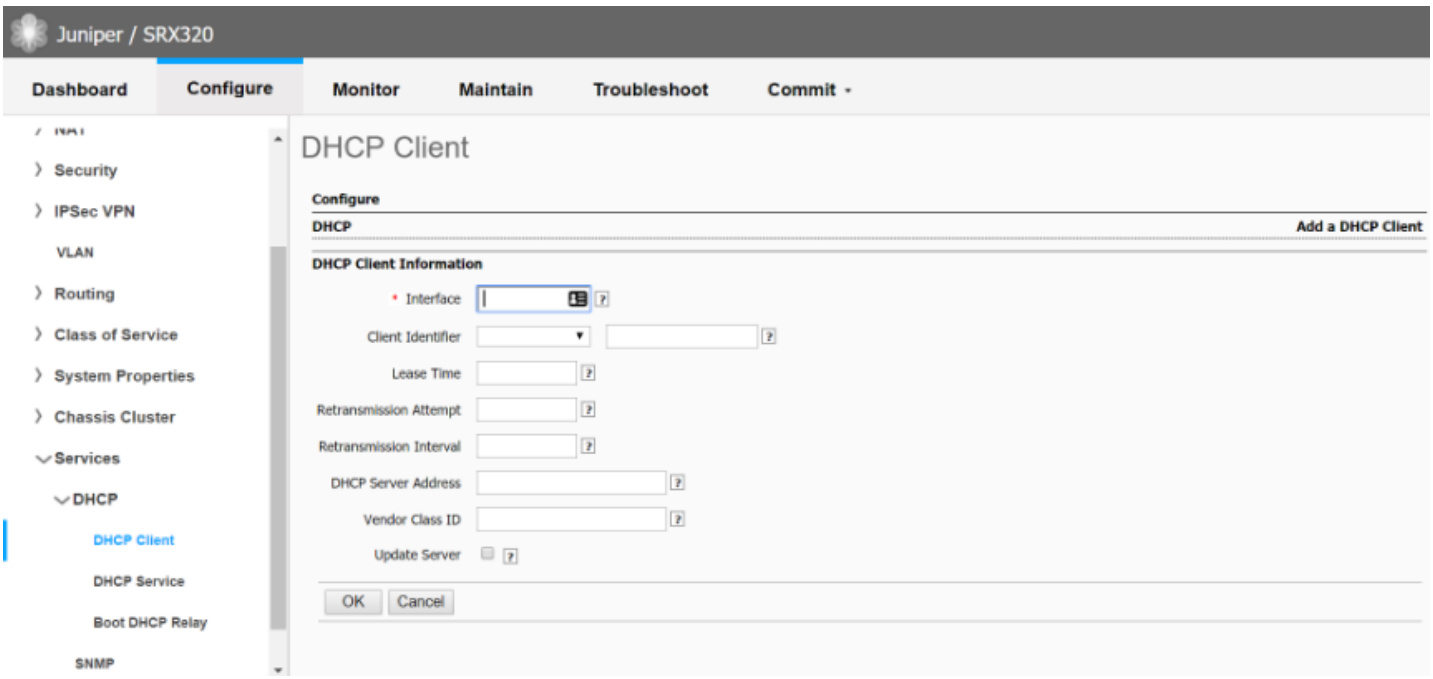
Signal Bars	Weighted dBm	Signal Strength %	Quality
	-113 to -99	0 - 23%	Bad
	-98 to -87	24 - 42%	Marginal
	-86 to -76	43 - 61%	OK
	-75 to -64	62 - 80%	Good
	-63 to -51	81 - 100%	Excellent

Juniper Configuration with the Accelerated 6300-CX

DHCP Client Configuration

The 6300-CX's cellular network access must be associated with a specific Ethernet port on the SRX Series security appliance before it can serve as a backup connection. Once assigned to an interface, additional options are available to further define the new DHCP Client's characteristics (lease time, retransmission intervals, and other supplemental information). Since Juniper SRXs come preconfigured with the first two Ethernet ports assigned to WAN and LAN functionality (in that order), the third port (labeled 0/2) will be the first available interface for assignment in new deployments.

Access the J-Web admin portal at 192.168.1.1



Please refer to the [Juniper knowledge article] for an in-depth walkthrough of the DHCP Client screen.

Step-by-Step Guidance: DHCP Client Configuration

NOTE:Port0/0 is reserved for the default WAN and 0/1 is predefined as the default LAN, making 0/2 the first available interface for a failover WAN uplink. Be sure to type the full name, ge-0/0/2.0

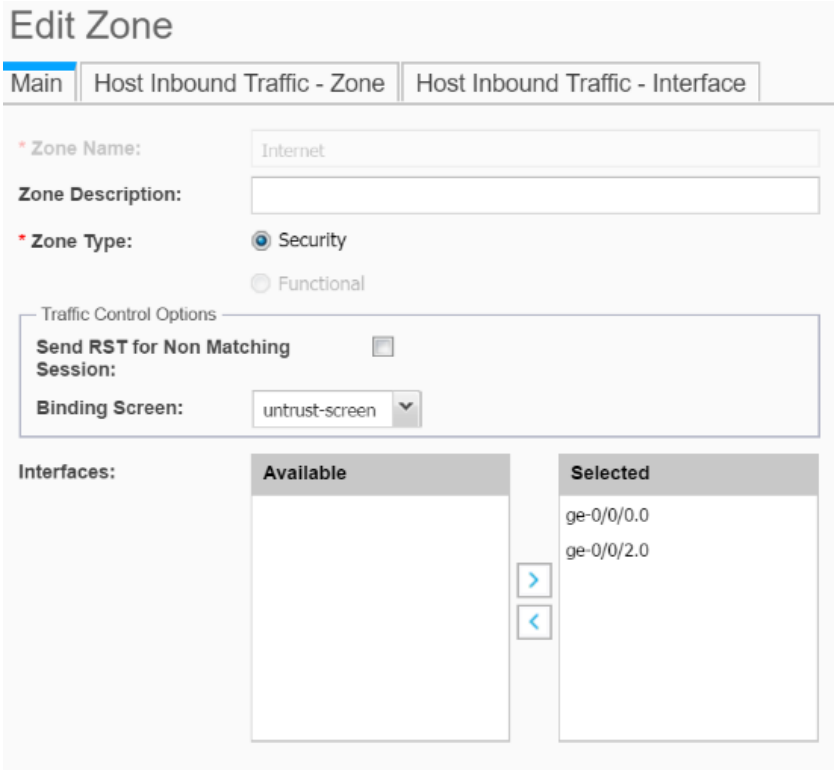
1. From the **Configure** tab of the admin portal, click on the **Services** menu option, select **DHCP**, and navigate to the **DHCP Client** page.
2. Click the **Add** button.
3. Specify which Ethernet **Interface** (port) will be assigned the cellular WAN connection.
4. Enter any other relevant information, clicking **Ok** to create the DHCP client.
5. Click the **Apply** button to finalize any changes.

Zones/Screens Settings

SRX Series Services Gateways leverage security zones to streamline the coordination of services and protocols associated with Ethernet traffic. The two default zones, “Internal” and “Internet,” are respectively used to delineate between LAN and WAN connections. Zone “junos-host” provides a dedicated means of managing self-traffic, both host-inbound and host-outbound. (Please refer to the Juniper knowledge article, *Understanding Security Policies for Self Traffic*, for more information regarding the junos-host zone.

Edit the Internet zone to establish the mechanisms required for WAN failover, allowing the SRX to retain an active Internet connection in light of a service interruption to its primary uplink. After configuring an interface for DHCP Clients, per the guidance on the previous page of this document, it becomes available for selection. Once assigned to the proper zone, the interface can be granted permission to JunOS' predefined services and protocols.

The SRX device is ready for failover once the new interface has been set to recognize the CX's cellular connection and it is subsequently assigned to the Internet zone with the required services enabled.



Please refer to the [Juniper knowledge article] for an in-depth walkthrough of the Zones/Screens menu.

Step-by-Step Guidance: Zones/Screens Settings

1. From the **Configure** tab of the admin portal, click on the **Security** menu option and navigate to **Zones/Screens**.
2. Select the **Internet** zone and click **Edit**.
3. The **Main** tab contains a column of **Available** interfaces. Use the > arrow to move the cellular interface to the **Selected** column.
4. Navigate to the **Host Inbound Traffic – Interface** tab and select the cellular interface.
5. Move **dhcp** and **ping** from the **Available Services** column to **Selected**. Enable other protocols or services as needed.
6. Click **Ok** to complete the configuration.

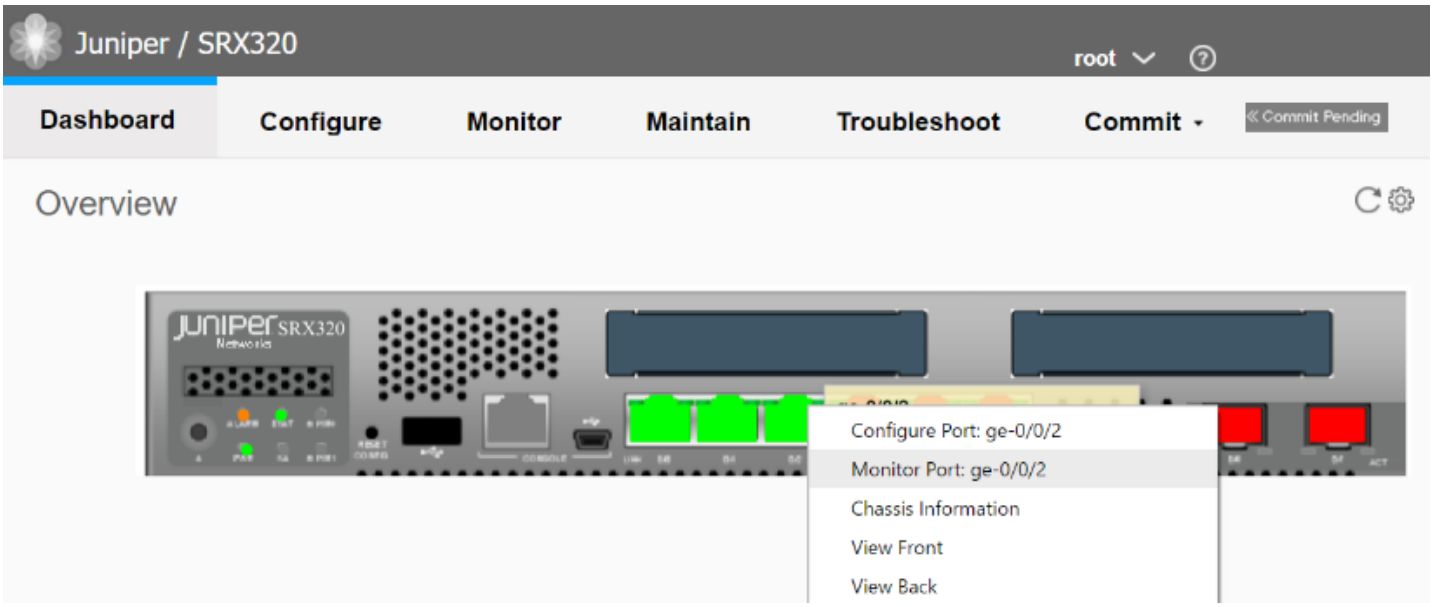
7. From the horizontal menu bar at the top of the screen, select **Commit** from the corresponding pull-down to apply any changes.

Interface Monitoring

J-Web provides real-time monitoring of traffic as it flows through SRX Series Services Gateways. After completing the Accelerated 6300-CX configuration to establish backup connectivity, JunOS can confirm that the failover and failback mechanisms are functioning as intended.

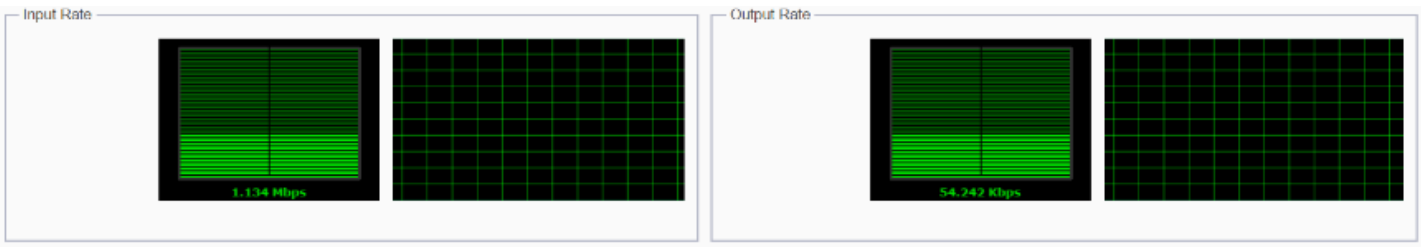
To do so, monitor the port on the SRX device that is assigned for backup connectivity. After triggering a failover condition (disabling the primary Internet connection), traffic will switch over to the secondary interface. This activity registers as input and output viewable in the Interface Statistics table.

For an in-depth walkthrough of how to monitor with J-Web, please refer to chapter 4 of [this Juniper knowledge article](#).



Step-by-Step Guidance: Interface Monitoring

1. Navigate to the Dashboard tab of the J-Web admin portal.
2. The Overview section contains a diagram of the SRX device, including green lights to indicate active Ethernet interfaces. Right click the desired interface and select Monitor Port.
3. Refer to the Interface Statistics to confirm connectivity.


Input Rate
1.134 Mbps
Output Rate
54.242 Kbps

Configuration for Cisco ASA Series

Overview

The Accelerated 6300-CX LTE Router provides a reliable, high-speed cellular connection that is compatible with existing wireline infrastructure. While its 4G LTE speeds are capable of operating as a primary WAN uplink, the 6300-CX can also be configured as a backup. This network redundancy solution delivers the ultimate flexibility to minimize expenses when it comes time for upgrading equipment to the latest wireless standards.

Business continuity depends on the seamless integration of failover-connectivity solutions to prevent service interruptions. Now more than ever, contingency networks play a strategic role in sustaining business operations. Unplanned outages can cost companies significant time and money, frustrating employees and clients alike, which creates a negative perception that is difficult to overcome.

Cellular data (4G LTE) bypasses wireline Internet service providers (ISPs) to facilitate the best redundancy possible. Additionally, in some situations it may be a challenge to acquire access to wired circuits or an event may call for temporary online access. Accelerated Concepts extensively tests the 6300-CX LTE router to ensure its interoperability with a wide variety of security appliances, including equipment produced by Fortinet, to best accommodate enterprise networks. Pairing the Accelerated 6300-CX with a dedicated firewall offers comprehensive security and flexibility for small business, retail, government, remote sites, and branch offices.

Cisco’s Adaptive Security Appliance (ASA) series is a threat-focused line of next-generation firewalls (NGFWs) designed for multilayered network protection. The latest ASA hardware is capable of integrating its proven security capabilities with Cisco’s FirePOWER service that bolsters the device’s readiness to defend against advanced and zero-day attacks. This next-generation intrusion prevention system (NGIPS) incorporates comprehensive access and

application control, threat prevention, routing policies, and contextual network awareness all under a single security appliance, a solution that was previously achieved by pairing an ASA firewall with a separate module dedicated to FirePOWER functionality.

For additional information, please refer to Cisco's ASA 5500 Series Configuration Guide.

Interoperability Matrix

This section covers interoperability information of the hardware tested for this solution. It includes the firmware versions of both devices as well as the date of testing.

Date	ASA Firmware	ASDM Version	6300-CX Firmware
12/2016	9.6(1)	7.6(1)	16.11.142

Caveats

The delivery of wireless services varies depending on the carrier and may lead to differences in the area of coverage, type of service (3G, 4G, LTE, etc.), available bandwidth, and IP address designation (Private or Public) among other factors. The interoperability test designed for this solution guide included LTE service, maximum coverage availability, and a public IP address assigned to each device.

Using the 6300-CX as a secondary connection assumes that a WAN Ethernet cable is plugged into the port configured for the primary uplink on the ASA device. Connect the 6300-CX's backup Ethernet cable to a port available for configuration as the secondary interface and proceed to the configuration described herein. (Compatible with all ASA series firewalls.)

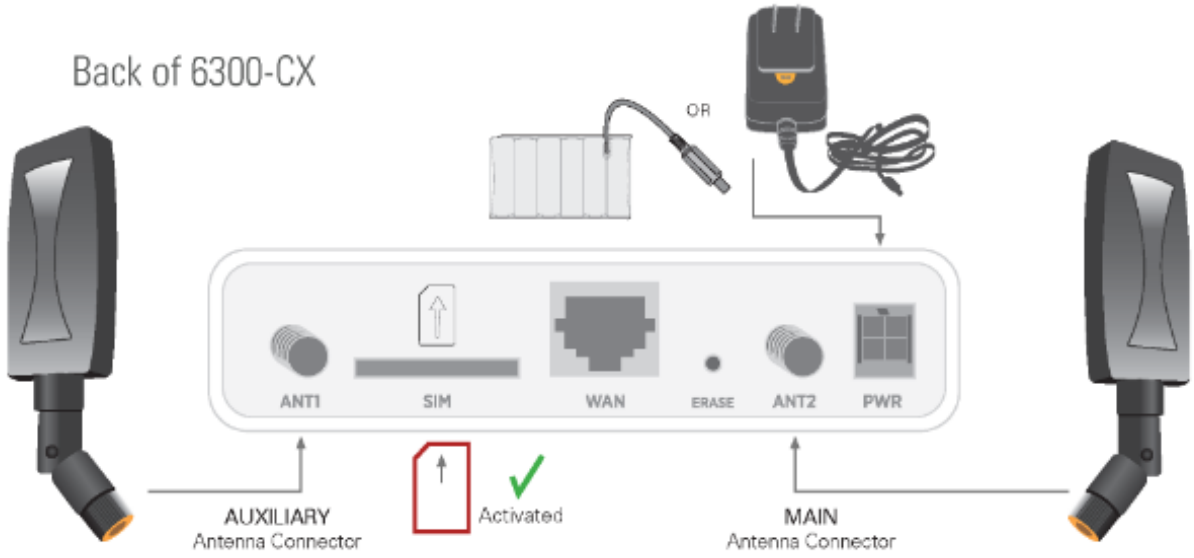
Accelerated 6300-CX LTE Router Setup

Initial Setup

Affix both antennas to the router and insert an activated SIM card before deploying the device. Be sure to select a location with optimal signal strength. For detailed instruction, refer to the tables that follow. Subsequent sections will outline site selection, powering options, and other device functionality.

Step-by-Step Guidance: Initial Setup

1. Insert the activated 2FF SIM card provided by your cellular network operator (putting the cut corner in first with metal contacts facing down). The card clicks into place when completely inserted.
2. Attach the two included antennas; both should be installed for optimal operation. Do this by gripping the metal connector section with your thumb and forefinger, tightening until secure. Do not tighten the antenna by holding any part of the plastic antenna housing.
3. To determine the optimal location for the 6300-CX, please see the “Site Survey” section.
4. Refer to the section(s) for Remote or Direct Power Installations when ready to connect the 6300-CX to the permanent power supply unit.
5. The 6300-CX uses DHCP with IP Passthrough by default, which satisfies the setup requirements for most environments. If required, please use Accelerated View™ or the 6300-CX local GUI to configure the 6300-CX for router mode.



Site Survey

If you are unsure of the available cellular signal strength, or are choosing between several locations, please follow the instructions to identify the ideal installation site.

Step-by-Step Guidance: Site Survey

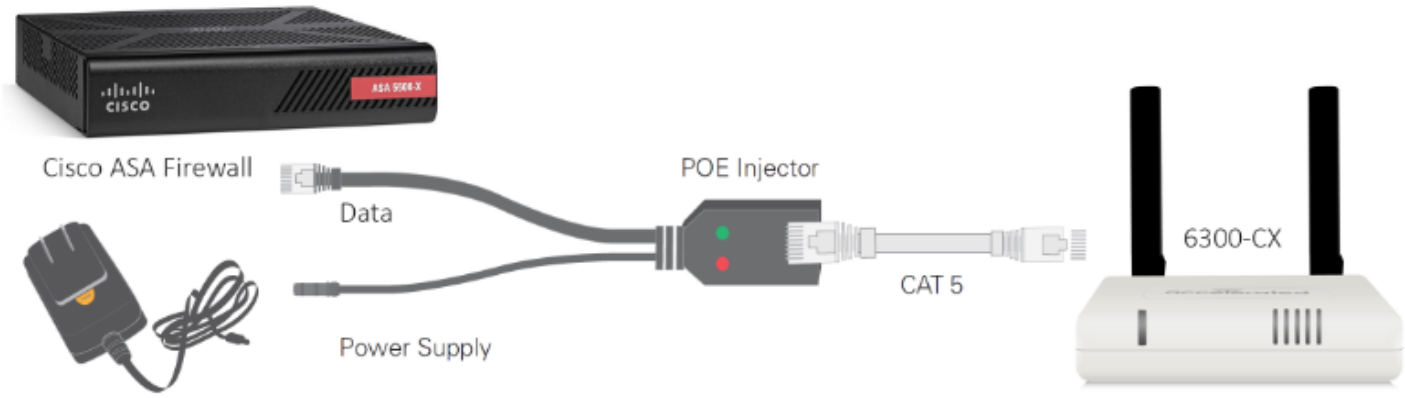
1. After following steps 1 and 2 in the “Initial Setup” section, connect the battery pack to temporarily power the Accelerated 6300-CX. The charge lasts two to four hours – it is not rechargeable and should be properly disposed of after use.
2. Move the 6300-CX to different locations within your site to determine the best compromise between signal strength and installation constraints. Since cellular signal strength may fluctuate, it is important to **wait at each location for 1 minute while observing the signal strength indicator** on the front of the device. Minimum cellular signal strength for operation is 2 bars (3+ is preferred).
3. After determining the optimal location, remove the battery pack and connect the main power supply unit or Ethernet cable connected to the PoE injector (per the power option outlined below).

Remote Power Installation – Powering Option #1

The included Power-over-Ethernet (PoE) injector allows the device to be positioned away from power outlets to simplify its installation needs. The adaptor consolidates the DC power and Ethernet connections so that both can be run to the 6300-CX via a single Ethernet cable. Distances of 300 ft have been tested on CAT6 and 250 ft on CAT5e. Note that cable conditions and the number of splices will impact actual distance.

Step-by-Step Guidance: Remote Power Installation

1. Plug the 6300-CX’s power supply unit (PSU) into an AC power outlet.
2. Connect the end of the PSU into the DC input (4 pin connector) of the PoE injector.
3. Insert the male RJ45 connector of the PoE injector cable into the firewall.
4. Connect an Ethernet cable from the RJ45 socket on the PoE injector cable to the Ethernet port of the 6300-CX. (See diagram.)

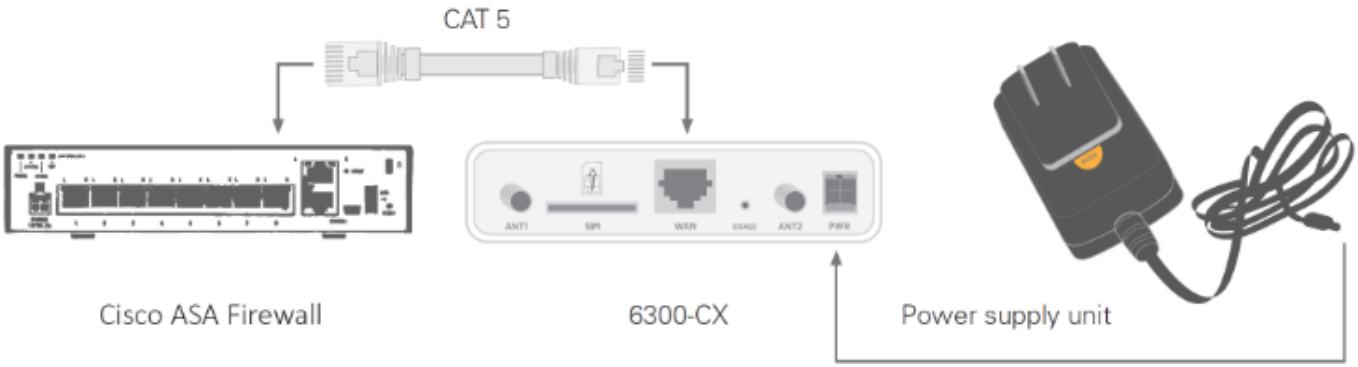


Direct Power Installation – Powering Option #2

If you plan to collocate the 6300-CX with the firewall device, you can directly power the 6300-CX without the PoE cable.

Step-by-Step Guidance: Direct Power Installation

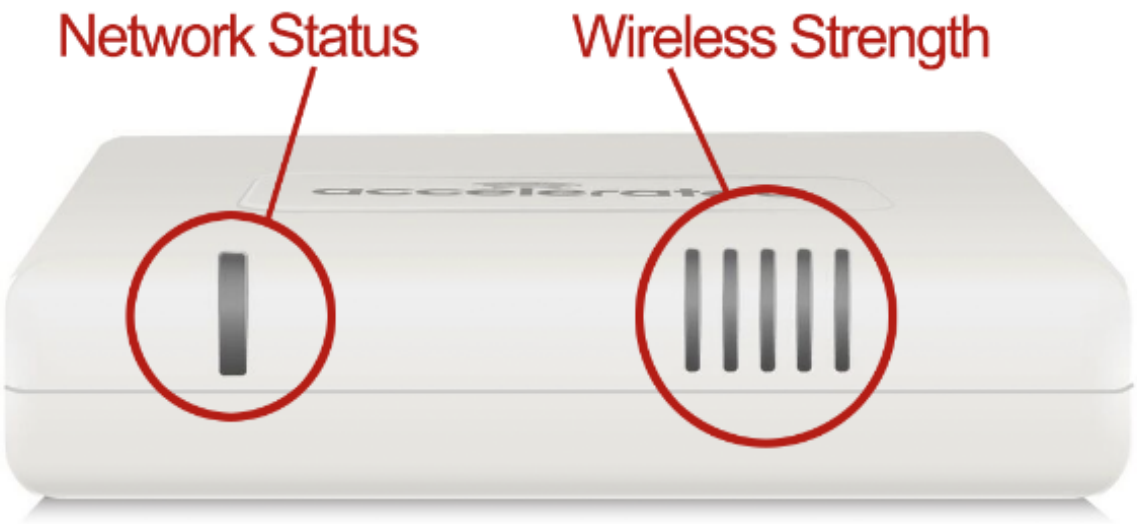
1. Use an Ethernet cable to connect the 6300-CX to the security appliance using port 1 (to use the cellular network as the primary connection) or port 3 (to configure a failover).
2. Plug the 6300-CX power supply unit (PSU) into an AC power outlet.
3. Connect the PSU into the 4-pin power connector of the 6300-CX. (See diagram.)



Understanding the 6300-CX LEDs

Once power has been established, your device will initialize and attempt to connect to the network. Device initialization may take 30-60 seconds. Indicator lights on the **Wireless Strength Indicator** show you the Cellular Network Signal Strength. The **Network Status Light** on the front left of the device displays connectivity information.

Please visit www.accelerated.com for additional information and trouble-shooting tips.



Network Status LED

Solid Yellow
Initializing or starting up.

Flashing Yellow
In the process of connecting to the cellular network and to a device on its Ethernet port.

Flashing White
Has an Ethernet connection and is in the process of connecting to the cellular network.

Flashing Green
Connected to 2G or 3G and is in the process of connecting to a device on its Ethernet port (or nothing is connected to the port).

Solid Green
Connected to 2G or 3G and also has an Ethernet connection.

Flashing Blue
Connected to 4G LTE and in the process of connecting to a device on its Ethernet port.

Solid Blue
Connected to 4G LTE and also has an Ethernet connection.

Alternating Red/ Yellow
Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Wireless Strength LEDs

Signal Bars	Weighted dBm	Signal Strength %	Quality
	-113 to -99	0 - 23%	Bad
	-98 to -87	24 - 42%	Marginal
	-86 to -76	43 - 61%	OK
	-75 to -64	62 - 80%	Good
	-63 to -51	81 - 100%	Excellent

Disable IP Passthrough on the Accelerated 6300-CX LTE Router

For failover configuration with a Cisco ASA firewall, the 6300-CX must be able to provide a static IP address to the secondary WAN interface (port). It cannot do so, however, until IP Passthrough is disabled on the Accelerated device. Reconfiguring the 6300-CX in this manner places the CX in “Router Mode.” The settings outlined below should be applied from the Configuration tab of Accelerated View™ although local administration is also possible if the need arises.

The step-by-step guidance provided below assumes that default configurations, most notably the stock IP subnets, are being leveraged on both the Accelerated 6300-CX and the Cisco ASA. These values can be altered as necessary to meet any preexisting network conditions; unless

otherwise indicated, assume the 192.168.0.X subnet belongs to the 6300-CX and that the 192.168.1.X subnet is assigned to the ASA.

Please refer to the 6300-CX User Manual for an in-depth walkthrough of both remote and local administration.

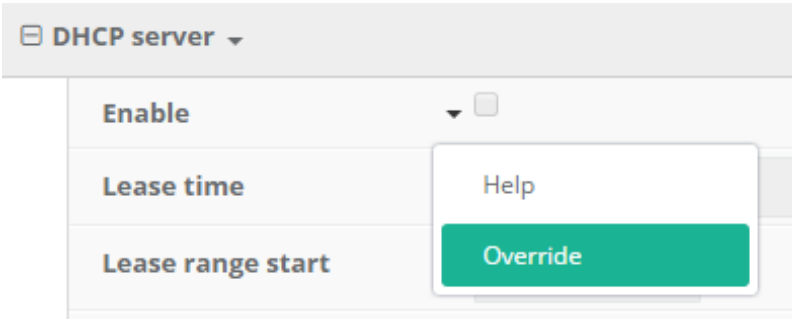
Step-by-Step Guidance: Disable IP Passthrough

NOTE: *The MAC address is a 12-character code included on the 6300-CX's bottom label.*

1. Sign in to Accelerated View and locate the 6300-CX by entering its **MAC address** in the **Search** field.
2. Click on the link in the **MAC** column to bring up the device's profile.
3. Navigate to the **Configuration** tab.
4. When configuring Accelerated devices, it is best to utilize new or existing **Group Configuration** profiles so that settings can be centrally stored and later applied to additional devices. Click the **Edit group configuration** link to proceed with the device setup.
5. **Settings** in Accelerated View are categorized and nested according to their scope of configuration:
6. Modem ? Passthrough: deselect the Enable checkbox
   Network ? Interfaces ? LAN ? IPv4: confirm the Interface type is set to Static IP address
   Network ? Interfaces ? LAN ? IPv4: confirm the Address is 192.168.0.1/24
   Network ? Interfaces ? LAN ? IPv4 ? DHCP server: select Enable
   (The "?" symbol denotes nested categories. Network ? Interfaces ? LAN, for example, points to the LAN menu nested inside the Interfaces section within the Network category.)
   points to the **LAN** menu nested inside the **Interfaces** section within the **Network** category.)
7. Click **Update** to finalize the new settings.
8. To apply the new settings immediately, reboot the CX or reference the step-by-step guidance for issuing remote commands.

NOTE:*Changes made to a group configuration are applied to ALL devices assigned to that group. To adjust settings for individual devices, select the **Override** button from the pull-down menu situated next to each field/ setting in question and make any necessary changes without editing the group config.*

NOTE:*Devices sync with Accelerated View once a day by default; pending configuration updates will apply at this time.*



ASA Configuration with the Accelerated 6300-CX

Failover Interface Settings

IP Policies and Static Routes serve as the foundation for how firewalls control and shape the flow of data through the networks they safeguard. Cisco ASA devices come preconfigured with security settings in place, though these routes and policies assume a traditional, single-WAN setup. The first Ethernet port, labeled "1," is designated for the primary WAN uplink with the remaining ports relegated to LAN access. An interface must be configured for the secondary WAN uplink to establish failover functionality. More importantly, both uplink interfaces must be configured to use a static IP address.

NOTE: Device administration is best handled using the Cisco ASDM desktop application, which connects a computer to the firewall's GUI without having to enable http server access. Initialize the ASDM-IDM Launcher and connect to the default gateway address provided by the ASA firewall: 192.168.1.1; the username and password are blank by default.

For an in-depth walkthrough of how to manage your ASA device via ASDM, please refer to Cisco's Configuration Guide.

Step-by-Step Guidance: Interface Settings

NOTE: *If the primary Internet connection routes traffic using either the 192.168.1.X or 192.168.0.X subnet, an alternative subnet will need to be used for the ASA and 6300-CX respectively.*

1. After connecting to the firewall via Cisco ASDM, navigate to the **Configuration** tab and select **Interfaces**.
2. ASA devices have two default interface configurations: GigabitEthernet1/1, allocated for the "outside" route, and GigabitEthernet1/2, allocated for the "inside" route.
3. Double click GigabitEthernet1/1 to edit the interface – rename it to "Primary" and select **Use Static IP**.

4. Specify the **IP Address** and **Subnet Mask** for the static IP assignment associated with the primary Internet connection. Contact your network administrator if these values are unknown.
5. Enter a **Description** for tracking purposes if desired. "FiOS Broadband," for example.
6. Click **OK** to finalize any changes. ASDM may display a warning about static routes being altered – click **OK**.
7. Double click GigabitEthernet1/3 to edit the secondary WAN uplink.
8. Select **Enable Interface**, assign an **Interface Name** (and optional **Description**), and toggle to **Use Static IP**.
9. Specify the static IP Address and Subnet Mask. If the 6300-CX is configured to use its default IP range, feel free to use the following values: 192.168.0.120 (IP Address) and 255.255.255.0 (Subnet Mask).
10. There should now be 3 interfaces configured: Primary, inside, and Secondary.

NOTE: Changes made to the ASA configuration via ASDM are inactive until the **Apply** button is clicked.

Static Routes and Tracking

The Cisco ASA device is ready for dual-WAN configuration once its two WAN connections are properly set (per the guidance from page 7 of this document). Any active interface must have a static route defined in order authorize traffic over the network. The firewall can then leverage advanced prioritization options to further reinforce the failover redundancy provided by the 6300-CX's backup LTE connection.

Failover itself is accomplished by the simultaneous application of interface metrics, which allows the network to establish a primary (the shorter/ smaller metric) and secondary (the longer/ larger metric) uplink, coupled with the tracking options configurable via static routes. With tracking enabled, the firewall actively verifies whether or not its primary WAN interface is online.

For an in-depth walkthrough of how to manage your ASA device via ASDM, please refer to Cisco's Configuration Guide.

Step-by-Step Guidance: Static Routes and Tracking

NOTE:*Please refer to Cisco's guidance on how to perform a configuration backup if there is concern over being able to recreate any policies or routes.*

1. After connecting to the firewall via Cisco ASDM, navigate to the **Configuration** tab and select **Static Routes from the Routing menu (found under Device Setup).**

2. Delete any existing static routes. These will need to be recreated with dual-WAN failover taken into consideration.
3. Click **Add** to create a new static route for each interface. Unless otherwise specified by the network administrator, use the following values:

Primary	Secondary
IP Address Type: IPv4 **Interface:** Primary **Network:** any4 **Gateway IP:** Use the corresponding Gateway IP established on page 7, step 4 **Metric:** 1	**IP Address Type:** IPv4 **Interface:** Secondary **Network:** any4 **Gateway IP:** Use the corresponding Gateway IP established on page 6, step 5 **Metric:** 120

1. For the **Primary** route, under **Options**, select **Tracked**. The **Track ID** and **SLA ID** are used to distinguish this configuration within ASDM. The **Track IP** Address can be set to any valid address used for connectivity testing (8.8.8.8 is a safe bet) and the **Target Interface** should remain "Primary."
2. Select Monitoring Options and set the **Frequency** to establish how often the ASA firewall should verify the connectivity of the primary WAN uplink. (10 seconds, for example.) Other settings can be adjusted as needed.

NOTE:*Set the **Number of Packets** to 3 unless otherwise specified.*

NAT Rules

The Cisco ASA comes with a default NAT rule for its primary interface to ensure the proper flow of traffic as packets travel across static routes. Once configured for two WAN interfaces, a second NAT rule should be defined for the failover connection. Note that any additional preexisting rules will need to be recreated for the secondary interface to maintain security continuity during failover.

For an in-depth walkthrough of how to manage your ASA device via ASDM, please refer to Cisco's Configuration Guide.

Step-by-Step Guidance: NAT Rules

1. After connecting to the firewall via Cisco ASDM, navigate to the Configuration tab and select the Firewall menu. Click on NAT Rules.
2. Click the Add button to generate a new rule.

3. Unless otherwise specified by your network administrator, apply the new rule as follows: **Match Criteria (Source Interface, Source Address, Destination Address, Service)** – any **Action: Translated Packet – Source NAT Type:** Dynamic PAT (Hide); **Source Address:** Secondary; **Destination Address** and **Service:** Original
4. Be sure "Enable rule" is selected under **Options**.
5. Click **OK** to finalize the new rule.

DHCP and DNS Configuration

To ensure seamless failover, it is best to specify DHCP and DNS settings so that the internal interface is used to provide consistency no matter whether the primary or failover WAN is leveraged for connectivity.

Step-by-Step Guidance: DHCP and DNS Configuration

1. From the **Configuration** tab, select the **Device Management** menu. Expand **DNS** and click on **DNS Client**.
2. Using the pull-down menus in the **DNS Lookup** table, set the WAN **Interfaces** to "False" so that their DNS is disabled. Set the "inside" interface to "True."
3. Ensure **Enable DNS Guard on all interfaces** is selected.
4. Expand the **DHCP** menu and select **DHCP Server**. Double click on "inside."
5. Select **Enable DHCP server** and utilize the predefined **DHCP Address Pool** unless otherwise notified by your network administrator.
6. Specify any DNS preferences using the **Optional Parameters**.
7. Click **OK** to finalize the configuration.

NOTE: Changes made to the ASA configuration via ASDM are inactive until the **Apply** button is clicked.

Verification/ Monitoring

Cisco ASDM provides real-time monitoring of traffic flowing through ASA devices. After completing the Accelerated 6300-CX configuration to establish backup connectivity, route monitoring can confirm that both the failover and failback mechanisms are functioning as intended.

Look for the line currently selected as the **DEFAULT**. This will change from the primary to secondary interface as soon as the failover condition is triggered (per the tracking parameters established during static route configuration), and revert back to primary once the connection is reestablished.

Protocol	Type	Destination IP	Netmask/ Prefix Length	Gateway	Interface	[AD/Metric]
STATIC	DEFAULT	0.0.0.0	0.0.0.0	172.16.3.1	Primary	[1/0]
CONNECTED		172.16.3.0	255.255.255.0		Primary	
LOCAL		172.16.3.62	255.255.255.255		Primary	
CONNECTED		192.168.0.0	255.255.255.0		Secondary	
LOCAL		192.168.0.120	255.255.255.255		Secondary	
CONNECTED		192.168.1.0	255.255.255.0		inside	
LOCAL		192.168.1.1	255.255.255.255		inside	

For an in-depth walkthrough of how to manage your ASA device via ASDM, please refer to Cisco's Configuration Guide.

Step-by-Step Guidance: Verification/ Monitoring

1. After connecting to the firewall via Cisco ASDM, navigate to the **Monitoring** tab and select the **Routing** menu. Click on **Routes**.
2. The **Type** column indicates which route is serving traffic currently by indicating the **DEFAULT** route.
3. Disconnect the primary interface by unplugging the Ethernet cable and click **Refresh**. The new default should be associated with the secondary connection.
4. Reconnect the primary interface and wait 10 to 30 seconds. Click **Refresh** and verify that the default route has reverted back to the primary WAN uplink.

NOTE: Changes made to the ASA configuration via ASDM are inactive until the **Apply** button is clicked.

Configuration for Edgewater EdgeMarc Series

Overview

The Accelerated 6300-CX LTE Router provides a reliable, high-speed cellular connection that is compatible with existing wireline infrastructure. While its 4G LTE speeds are capable of operating as a primary WAN uplink, the 6300-CX can also be configured as a backup. This network redundancy solution delivers the ultimate flexibility to minimize expenses when it comes time for upgrading equipment to the latest wireless standards.

Business continuity depends on the seamless integration of failover-connectivity solutions to prevent service interruptions. Now more than ever, contingency networks play a strategic role in sustaining business operations. Unplanned outages can cost companies significant time and money, frustrating employees and clients alike, which creates a negative perception that is difficult to overcome.

Cellular data (4G LTE) bypasses wireline Internet service providers (ISPs) to facilitate the best redundancy possible. Additionally, in some situations it may be a challenge to acquire access to wired circuits or an event may call for temporary online access. For these reasons Edgewater Networks and Accelerated Concepts have teamed up to offer comprehensive control and flexibility for small businesses, retail, government, remote sites, and branch offices.

To optimize high-quality communications for scalable voice, video, and data traffic, Edgewater Networks enterprise session border controller (ESBC) can be introduced into the infrastructure though this functionality hinges upon an active WAN connection. An EdgeMarc ESBC paired with the Accelerated 6300-CX LTE Router will ensure your enterprise network remains robust and operational should its primary ISP go offline. Running a cellular backup via an Ethernet cable preserves the full QoS optimization of the EdgeMarc ESBC, which isn't the case for USB-connected Aircards.

For additional information, please refer to Edgewater Network's Knowledge Base.

Interoperability Matrix

This section covers interoperability information of the hardware tested for this solution. It includes the firmware versions of both devices as well as the date of testing.

Date	VOS Release	6300-CX Firmware
10/2016	14.1	16.3.15

Caveats

The delivery of wireless services varies depending on the carrier and may lead to differences in the area of coverage, type of service (3G, 4G, LTE, etc.), available bandwidth, and IP address designation (Private or Public) among other factors. The interoperability test designed for this solution guide included LTE service, maximum coverage availability, and a public IP address assigned to each device.

Using the 6300-CX as a secondary connection requires dual WAN ports on the EdgeMarc. Therefore, the service described herein is compatible with the following devices: EM-4700, EM-4750, EM-4800, EM-4806, EM-4808, and EM-7301.

Notice that some Wireless Service Providers may assign a private IP to the device and voice traffic may be behind NAT. Contact your VoIP Service Provider to verify if voice traffic from a private IP is accepted and/or the Wireless Service Provider to request a static public IP for your service. While a public IP address is not an absolute requirement for the LTE Modem, the address needs to be routable and not behind NAT.

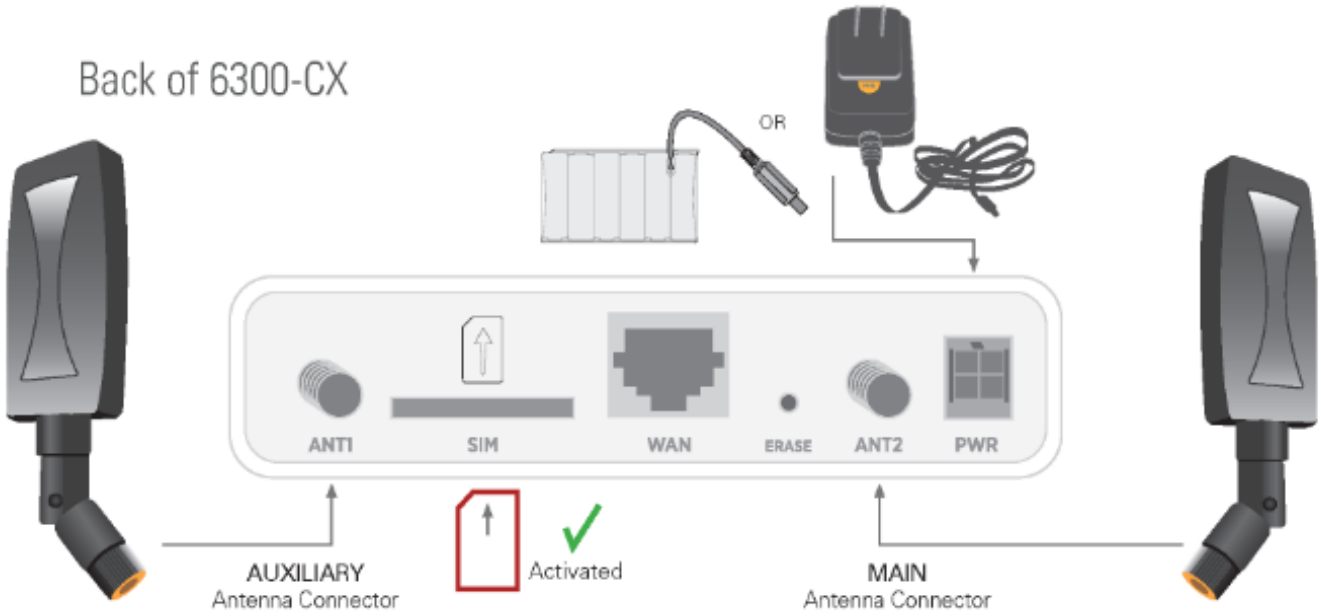
Accelerated 6300-CX LTE Router Setup

Initial Setup

Affix both antennas to the router and insert an activated SIM card before deploying the device. Be sure to select a location with optimal signal strength. For detailed instruction, refer to the tables that follow. Subsequent sections will outline site selection, powering options, and other device functionality.

Step-by-Step Guidance: Initial Setup

1. Insert the activated 2FF SIM card provided by your cellular network operator (putting the cut corner in first with metal contacts facing down). The card clicks into place when completely inserted.
2. Attach the two included antennas; both should be installed for optimal operation. Do this by gripping the metal connector section with your thumb and forefinger, tightening until secure. Do not tighten the antenna by holding any part of the plastic antenna housing.
3. To determine the optimal location for the 6300-CX, please see the “Site Survey” section.
4. Refer to the section(s) for Remote or Direct Power Installations when ready to connect the 6300-CX to the permanent power supply unit.
5. The 6300-CX uses DHCP with IP Passthrough by default, which satisfies the setup requirements for most environments. If required, please use Accelerated View™ or the 6300-CX local GUI to configure the 6300-CX for router mode.



Site Survey

If you are unsure of the available cellular signal strength, or are choosing between several locations, please follow the instructions to identify the ideal installation site.

Step-by-Step Guidance: Site Survey

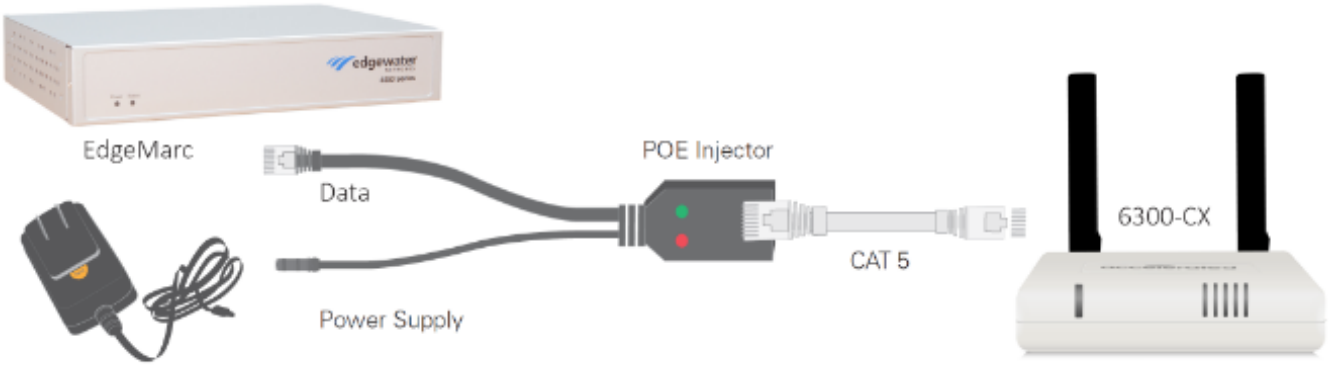
1. After following steps 1 and 2 in the “Initial Setup” section, connect the battery pack to temporarily power the Accelerated 6300-CX. The charge lasts two to four hours – it is not rechargeable and should be properly disposed of after use.
2. Move the 6300-CX to different locations within your site to determine the best compromise between signal strength and installation constraints. Since cellular signal strength may fluctuate, it is important to **wait at each location for 1 minute while observing the signal strength indicator** on the front of the device. Minimum cellular signal strength for operation is 2 bars (3+ is preferred).
3. After determining the optimal location, remove the battery pack and connect the main power supply unit or Ethernet cable connected to the PoE injector (per the power option outlined below).

Remote Power Installation – Powering Option #1

The included Power-over-Ethernet (PoE) injector allows the device to be positioned away from power outlets to simplify its installation needs. The adaptor consolidates the DC power and Ethernet connections so that both can be run to the 6300-CX via a single Ethernet cable. Distances of 300 ft have been tested on CAT6 and 250 ft on CAT5e. Note that cable conditions and the number of splices will impact actual distance.

Step-by-Step Guidance: Remote Power Installation

1. Plug the 6300-CX’s power supply unit (PSU) into an AC power outlet.
2. Connect the end of the PSU into the DC input (4 pin connector) of the PoE injector.
3. Insert the male RJ45 connector of the PoE injector cable into the EdgeMarc.
4. Connect an Ethernet cable from the RJ45 socket on the PoE injector cable to the Ethernet port of the 6300-CX. (See diagram.)

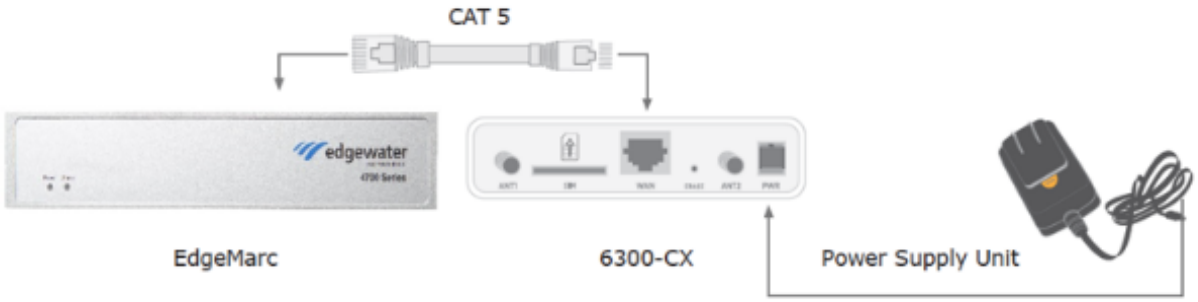


Direct Power Installation – Powering Option #2

If you plan to collocate the 6300-CX with the EdgeMarc device, you can directly power the 6300-CX without the PoE cable.

Step-by-Step Guidance: Direct Power Installation

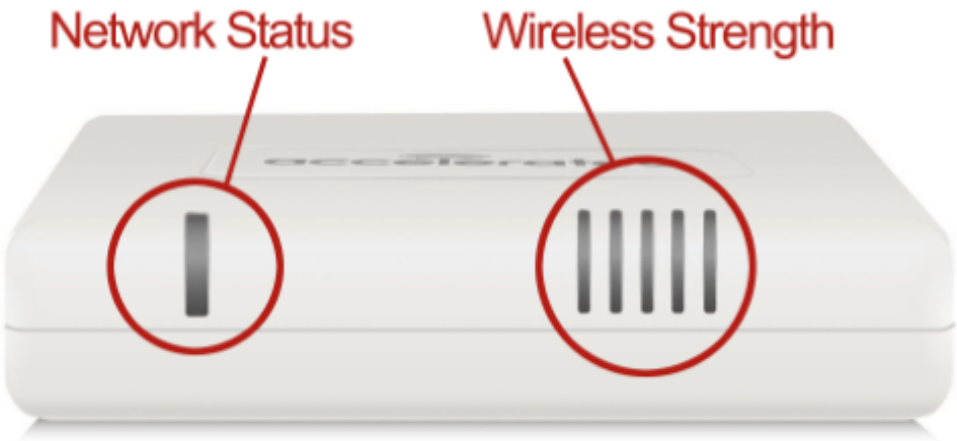
1. Use an Ethernet cable to connect the 6300-CX to the security appliance using port WAN 1 (to use the cellular network as the primary connection) or port WAN 2 (to configure a failover).
2. Plug the 6300-CX power supply unit (PSU) into an AC power outlet.
3. Connect the PSU into the 4-pin power connector of the 6300-CX. (See diagram.)



Understanding the 6300-CX LEDs

Once power has been established, your device will initialize and attempt to connect to the network. Device initialization may take 30-60 seconds. Indicator lights on the **Wireless Strength Indicator** show you the Cellular Network Signal Strength. The **Network Status Light** on the front left of the device displays connectivity information.

Please visit www.accelerated.com for additional information and trouble-shooting tips.



Network Status LED

Solid Yellow
Initializing or starting up.

Flashing Yellow
In the process of connecting to the cellular network and to a device on its Ethernet port.

Flashing White
Has an Ethernet connection and is in the process of connecting to the cellular network.

Flashing Green
Connected to 2G or 3G and is in the process of connecting to a device on its Ethernet port (or nothing is connected to the port).

Solid Green
Connected to 2G or 3G and also has an Ethernet connection.

Flashing Blue
Connected to 4G LTE and in the process of connecting to a device on its Ethernet port.

Solid Blue
Connected to 4G LTE and also has an Ethernet connection.

Alternating Red/ Yellow
Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Wireless Strength LEDs

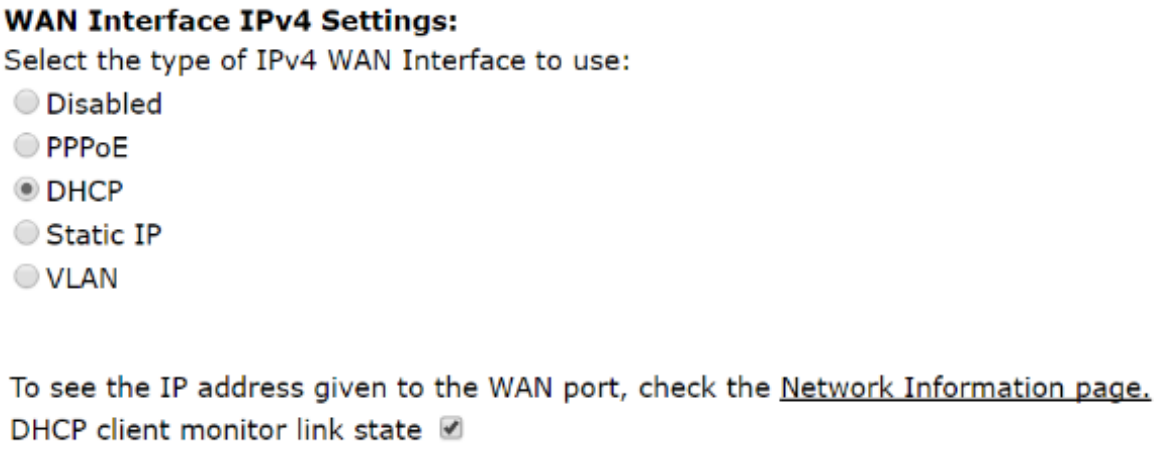
Signal Bars	Weighted dBm	Signal Strength %	Quality
	-113 to -99	0 - 23%	Bad
	-98 to -87	24 - 42%	Marginal
	-86 to -76	43 - 61%	OK
	-75 to -64	62 - 80%	Good
	-63 to -51	81 - 100%	Excellent

EdgeMarc Configuration with the Accelerated 6300-CX

WWAN as the Primary Interface

The back panel of the EdgeMarc ESBC features an array of LAN ports and two dedicated WAN interfaces. To utilize the 6300-CX's LTE Wireless WAN (WWAN) connectivity as the primary means of Internet access, connect the Accelerated LTE router to port WAN 1 on the EdgeMarc device using an Ethernet cable. A solid blue light on the 6300-CX confirms that its 4G LTE modem is online and an Ethernet connection has been established with another device. Similarly, a green light (blinking or solid) next to the ESBC's WAN port indicates that the EdgeMarc is connected to the LTE router.

Access the Edgewater admin portal at 192.168.1.1



Please refer to the EdgeMarc VOS User Guide for an in-depth walkthrough of the device's local GUI.

Step-by-Step Guidance: WWAN as the Primary Interface

NOTE: The Static IP radio button is selected by default.

1. From the **Configuration Menu**, select **Network.**
2. Locate the **WAN Interface IPv4 Settings** and select **DHCP.**
3. Enable **DHCP client monitor link state** to display detailed network configuration information.
4. Click **Submit.**
5. Click the **OK** button to finalize any changes.

NOTE: A message will indicate that service will be temporarily interrupted as the new settings are established.

WAN Link Redundancy (WLR) with WWAN Failover

The WAN Failover menu initializes WLR and further configures the interaction between primary and secondary WANs. Even with both WAN ports connected to an active Internet connection, the EdgeMarc ESBC is unable to utilize the secondary uplink until WAN Link Redundancy is enabled by selecting the corresponding check box. Additional settings may be engaged once the WLR status is updated.

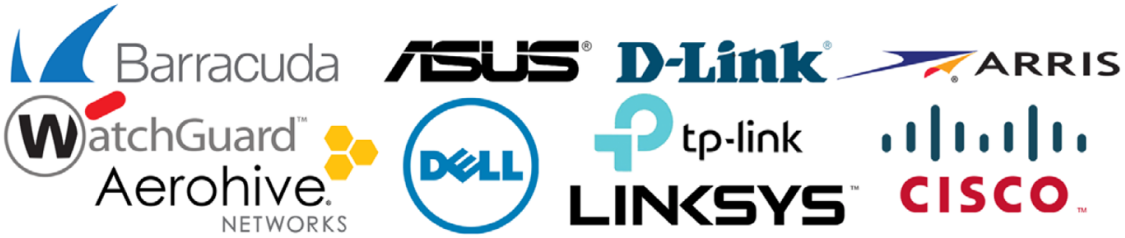
Please refer to the EdgeMarc VOS User Guide for an in-depth walkthrough of the device's local GUI.

Step-by-Step Guidance: WAN Link Redundancy with WWAN Failover

1. From the **Configuration Menu**, select **Network**.
2. Navigate to the **WAN Failover** screen.
3. Select the **Enable WAN Link Redundancy**, **Enable Revertive Mode**, and **Enable Dual WAN Ports** checkboxes.
4. Click **Submit**. See Note (a)
5. Click the **OK** button to finalize any changes.
6. Once the page reloads, verify that both the primary and secondary links are listed under **WAN Link Redundancy Status**. See Note (b)
7. Under **WAN Failover**, select **Secondary WAN**.
8. Locate the **WAN Interface IPv4 Settings** and select **DHCP**.
9. Enable **DHCP client monitor link state** to display detailed network configuration information.
10. Click **Submit** and then **OK** (per steps 4 & 6) to finalize any changes.
11. Navigate back to the **WAN Failover** screen. There should now be an address listed for the **Secondary Link IPv4 Address**.
12. Designate the desired interface for **Data** and **Voice** using the corresponding pull-down menus.
13. The **Switchover Interfaces** establishes which systems (between data and voice) will be affected by the WLR settings, allowing for selective failover functionality.
14. Failback detection is customized via the **Advanced** menu, located under **WAN Failover**. See Note (c)

NOTE (a):*A message will indicate that service will be temporarily interrupted as the new settings are established.*
NOTE (b):*The* ***Secondary Link Status*** *will read* ***UNAVAILABLE*** *until DHCP is enabled for the failover interface (explained in the following steps).*
NOTE (c):*These fields come pre-populated by default.*

Configuration for Dual-WAN Routers



Overview

The Accelerated 6300-CX LTE Router provides a reliable, high-speed cellular connection that is compatible with existing wireline infrastructure. While its 4G LTE speeds are capable of operating as a primary WAN uplink, the 6300-CX can also be configured as a backup. This network redundancy solution delivers the ultimate flexibility to minimize expenses when it comes time for upgrading equipment to the latest wireless standards.

Business continuity depends on the seamless integration of failover-connectivity solutions to prevent service interruptions. Now more than ever, contingency networks play a strategic role in sustaining business operations. Unplanned outages can cost companies significant time and money, frustrating employees and clients alike, which creates a negative perception that is difficult to overcome.

Cellular data (4G LTE) bypasses wireline Internet service providers (ISPs) to facilitate the best redundancy possible. Additionally, in some situations it may be a challenge to acquire access to wired circuits or an event may call for temporary online access. Accelerated Concepts extensively tests the 6300-CX LTE Router to ensure its interoperability with a wide variety of security appliances, including equipment produced by SonicWall, Edgewater, Meraki, Fortinet, and others to best accommodate enterprise networks. Pairing the Accelerated 6300-CX with a dedicated firewall offers comprehensive security and flexibility for small business, retail, government, remote sites, and branch offices.

Interoperability Matrix

This section covers interoperability information of the hardware tested for this solution. It includes the firmware versions of both devices as well as the date of testing.

Date	6300-CX Firmware
12/2016	16.11.142

Caveats

The delivery of wireless services varies depending on the carrier and may lead to differences in the area of coverage, type of service (3G, 4G, LTE, etc.), available bandwidth, and IP address designation (Private or Public) among other factors. The interoperability test designed for this solution guide included LTE service, maximum coverage availability, and a public IP address assigned to each device.

Using the 6300-CX as a secondary uplink requires dual WAN ports on the appliance to which it provides connectivity. Therefore, the service described herein assumes the following:

- Two available WAN ports (primary and secondary interfaces)
- Administrative access to the dual-WAN device's local GUI

Some networking appliances have interfaces that can be used as either WAN or LAN ports depending on how they're currently configured. If this is the case, please consult the documentation included with the firewall or router for step-by-step guidance before referencing the configuration notes included in this document.

NOTE: If additional LAN ports are necessary for practical use, a switch can be introduced without requiring additional configuration. Connect the switch to an available LAN port and proceed with the processes described herein.

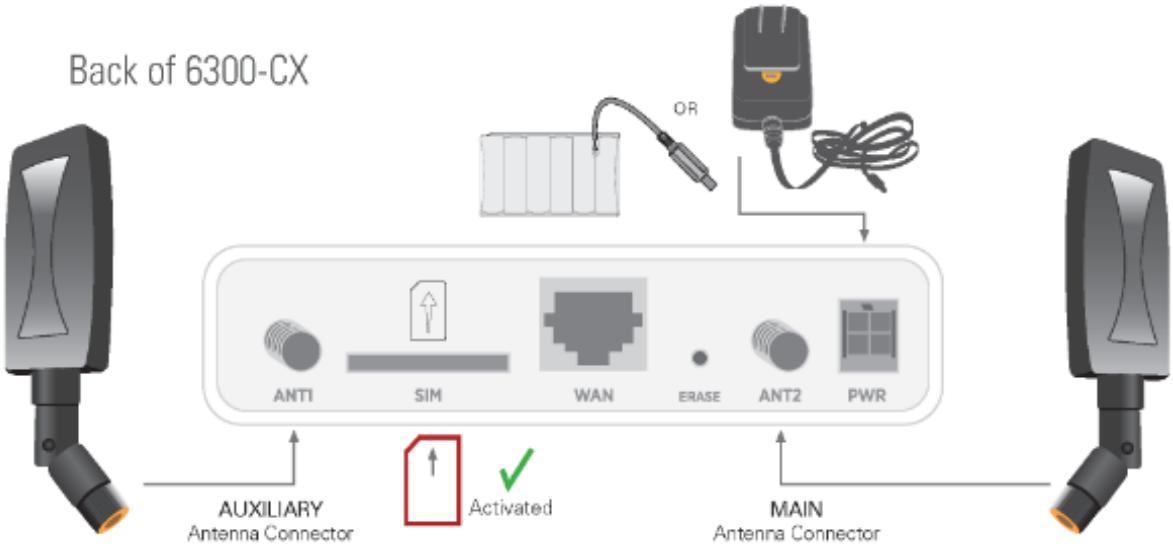
Accelerated 6300-CX LTE Router Setup

Initial Setup

Affix both antennas to the router and insert an activated SIM card before deploying the device. Be sure to select a location with optimal signal strength. For detailed instruction, refer to the tables that follow. Subsequent sections will outline site selection, powering options, and other device functionality.

Step-by-Step Guidance: Initial Setup

1. Insert the activated 2FF SIM card provided by your cellular network operator (putting the cut corner in first with metal contacts facing down). The card clicks into place when completely inserted.
2. Attach the two included antennas; both should be installed for optimal operation. Do this by gripping the metal connector section with your thumb and forefinger, tightening until secure. Do not tighten the antenna by holding any part of the plastic antenna housing.
3. To determine the optimal location for the 6300-CX, please see the “Site Survey” section.
4. Refer to the section(s) for Remote or Direct Power Installations when ready to connect the 6300-CX to the permanent power supply unit.
5. The 6300-CX uses DHCP with IP passthrough by default, which satisfies the setup requirements for most environments. If required, please use Accelerated View™ or the 6300-CX local GUI to configure the 6300-CX for router mode.



Site Survey

If you are unsure of the available cellular signal strength, or are choosing between several locations, please follow the instructions to identify the ideal installation site.

Step-by-Step Guidance: Site Survey

1. After following steps 1 and 2 in the “Initial Setup” section, connect the battery pack to temporarily power the Accelerated 6300-CX. The charge lasts two to four hours – it is not rechargeable and should be properly disposed of after use.

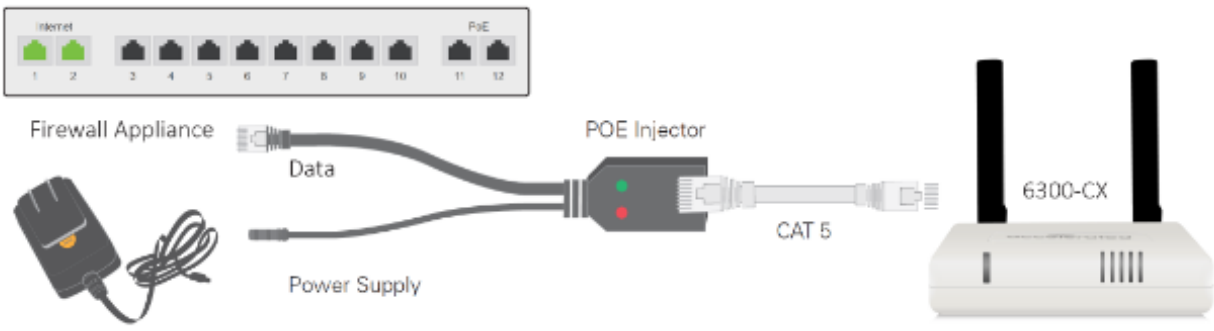
2. Move the 6300-CX to different locations within your site to determine the best compromise between signal strength and installation constraints. Since cellular signal strength may fluctuate, it is important to **wait at each location for 1 minute while observing the signal strength indicator on the front of the device.** Minimum cellular signal strength for operation is 2 bars (3+ is preferred).
3. After determining the optimal location, remove the battery pack and connect the main power supply unit or Ethernet cable connected to the PoE injector (per the power option outlined below).

Remote Power Installation – Power Option #1

The included Power-over-Ethernet (PoE) injector allows the device to be positioned away from power outlets to simplify its installation needs. The adaptor consolidates the DC power and Ethernet connections so that both can be run to the 6300-CX via a single Ethernet cable. Distances of 300 ft have been tested on CAT6 and 250 ft on CAT5e. Note that cable conditions and the number of splices will impact actual distance.

Step-by-Step Guidance: Remote Power Installation

1. Plug the 6300-CX's power supply unit (PSU) into an AC power outlet.
2. Connect the end of the PSU into the DC input (4 pin connector) of the PoE injector.
3. Insert the male RJ45 connector of the PoE injector cable into the SonicWall.
4. Connect an Ethernet cable from the RJ45 socket on the PoE injector cable to the Ethernet port of the 6300-CX. (See diagram.)

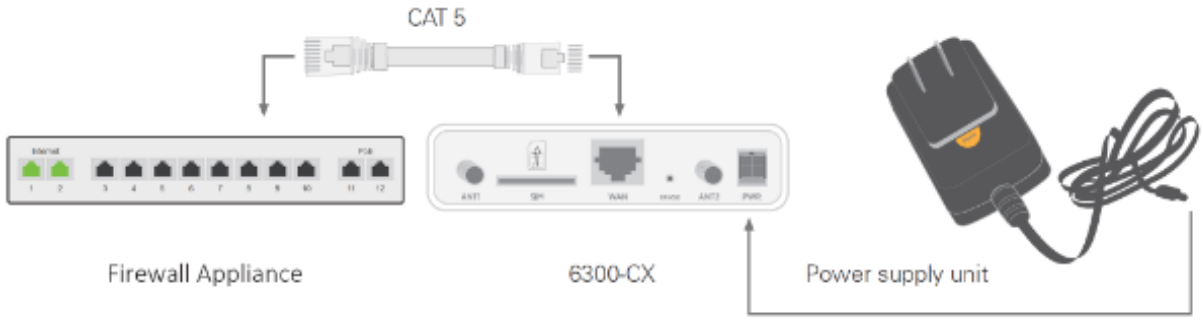


Direct Power Installation – Power Option #2

If you plan to collocate the 6300-CX with the MX device, you can directly power the 6300-CX without the PoE cable.

Step-by-Step Guidance: Direct Power Installation

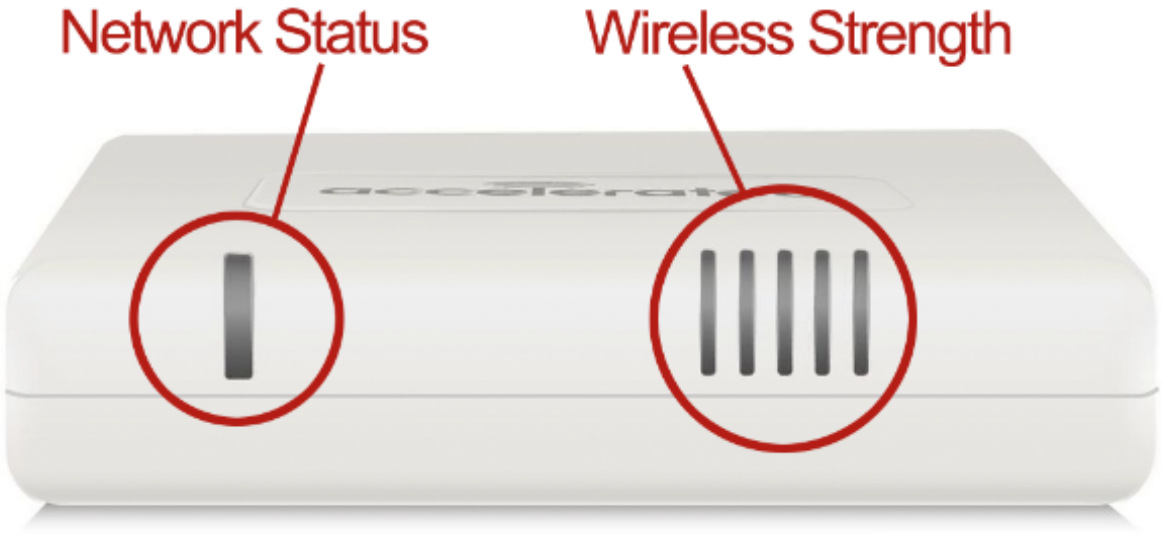
1. Use an Ethernet cable to connect the 6300-CX to the security appliance using port Internet 1 (to use the cellular network as the primary connection) or port Internet 2 (to configure a failover).
2. Plug the 6300-CX power supply unit (PSU) into an AC power outlet.
3. Connect the PSU into the 4-pin power connector of the 6300-CX. (See diagram.)



Understanding the 6300-CX LEDs

Once power has been established, your device will initialize and attempt to connect to the network. Device initialization may take 30-60 seconds. Indicator lights on the **Wireless Strength Indicator** show you the cellular network signal strength. The **Network Status Light** on the front left of the device displays connectivity information.

Please visit accelerated.com for additional information and troubleshooting tips.



Network Status LED

Solid Yellow
Initializing or starting up.

Flashing Yellow
In the process of connecting to the cellular network and to a device on its Ethernet port.

Flashing White
Has an Ethernet connection and is in the process of connecting to the cellular network.

Flashing Green
Connected to 2G or 3G and is in the process of connecting to a device on its Ethernet port (or nothing is connected to the port).

Solid Green
Connected to 2G or 3G and also has an Ethernet connection.

Flashing Blue
Connected to 4G LTE and in the process of connecting to a device on its Ethernet port.

Solid Blue
Connected to 4G LTE and also has an Ethernet connection.

Alternating Red/ Yellow
Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Wireless Strength LEDs

Signal Bars	Weighted dBm	Signal Strength %	Quality
	-113 to -99	0 - 23%	Bad
	-98 to -87	24 - 42%	Marginal
	-86 to -76	43 - 61%	OK
	-75 to -64	62 - 80%	Good
	-63 to -51	81 - 100%	Excellent

Router Configuration with the Accelerated 6300-CX

Dual-WAN Configuration

Before designating the primary and secondary Internet connections, first identify the available ports on the dual-WAN appliance's back panel. While most modern devices support multiple WAN interfaces, not all equipment contains a separate grouping specifically for WAN uplinks. Should this be the case, and there is no distinct labeling to differentiate between ports for Ethernet (LAN) and Internet (WAN), the best practice is best to start with the lowest available port (usually either 0 or 1 unless otherwise specified) for the primary uplink and to use its adjacent port for the secondary connection. Follow the same rule of thumb if the firewall features dedicated WAN interfaces, starting with the first port for the primary WAN before assigning the secondary line.

Network devices typically feature a local (or web) GUI to handle configuration settings. More often than not, this administration portal is accessed by navigating to the device's IP address using a web browser. Administration portals may vary greatly, depending on the make and model of the appliance in question, though the overall process remains the same: enable (or confirm) multiple WAN support and establish failover prioritization. Additional settings will likely be available to offer further control over how the two interfaces cooperate, such as automatic failback/ reversion, load balancing, and traffic-shaping rules or exceptions. Please refer to the proprietary documentation included with the device for an in-depth walkthrough of its local GUI/ admin portal.

In most dual-WAN scenarios, the connection supplied by the 6300-CX is best leveraged as the backup WAN interface. Its embedded cellular modem allows network administrators to run an LTE backup via an Ethernet cable as opposed to a USB solution, which preserves the full security functionality of most firewalls. (DPI-SSL inspection, for example, is not guaranteed when failover connectivity is provided by a USB-connected modem.) It is important to note that IP Passthrough must be enabled on the 6300, which is the device's default setting, to ensure that the dedicated firewall or router is able to properly control how Internet traffic is being routed. This configuration and other administrative settings can be handled remotely by logging into Accelerated View™, a centralized system for network administration that allows for web-based monitoring, management, reporting, and alerts on all Accelerated devices.

NOTE: When integrating cellular failover into existing infrastructure, it is critical to consider all factors in play. Business continuity solutions must be as reliable as they are cost-effective to mitigate the impact of network outages. Firewalls and similar appliances have many supplemental features that allow for advanced control over how data flows between the two WAN connections, but the nature of mobile data plans may not be conducive toward enabling all of these settings. Load balancing, for instance, would consume additional data so it is important to stay aware of any data caps or limitations (or at least assess the cost of exceeding them). Similarly, customizing the parameters for failback the process of switching back to the primary WAN once its connectivity is restored can optimize dual-WAN configurations by actively checking the status of both uplinks, minimizing the data usage and response time for failover while maximizing continuity. Please refer to your cellular or internet service provider for additional information about available data plans.

6300-CX Quick List

1. Place LTE router for optimal signal strength
2. Connect Ethernet cable to available WAN port
3. Confirm solid blue (4G) or green (3G) LED for network status and device connectivity
4. Verify IP Passthrough is active (it is enabled by default for the 6300-CX)
5. Reference device documentation to proceed with dual-WAN configuration via local GUI
6. Test failover scenarios for business continuity

Configuration for Single-WAN Routers

Overview

The Accelerated 6300-CX LTE Router provides a reliable, high-speed cellular connection that is compatible with existing wireline infrastructure. While its 4G LTE speeds are capable of operating as a primary WAN uplink, the 6300-CX can also be configured as a backup. This network redundancy delivers the ultimate flexibility to minimize expenses when it comes time for upgrading equipment to the latest wireless standards.

Business continuity depends on the seamless integration of failover-connectivity solutions to prevent service interruptions. Now more than ever, contingency networks play a strategic role in sustaining business operations. Unplanned outages can cost significant time and money, frustrating employees and clients alike, which creates a negative perception that is difficult to overcome.

The vast majority of residential broadband connections grant users Internet access using a router with a coaxial WAN interface, though Ethernet-based LAN ports can often be configured to route WAN traffic as well. Pairing the Accelerated 6300-CX with a traditional, single-WAN router facilitates the best redundancy possible by allowing for cellular data (4G LTE) to bypass physical infrastructure (the coaxial-based broadband connection) and provide WAN connectivity should the primary uplink fail.

Accelerated Concepts extensively tests the 6300-CX LTE Router to ensure its interoperability with a wide variety of network appliances, including equipment provided by Frontier, Spectrum, and many other ISPs. The solution outlined in this document relies primarily upon settings

controlled by the 6300-CX, minimizing any configuration requirements for the single-WAN router (to promote universal compatibility with most broadband networks).

Interoperability Matrix

This section covers interoperability information of the hardware tested for this solution. It includes the firmware versions of the device(s) as well as the date of testing.

Date	6300-CX FIrmware
12/2016	16.11.142

Caveats

The delivery of wireless services varies depending on the carrier and may lead to differences in the area of coverage, type of service (3G, 4G, LTE, etc.), available bandwidth, and IP address designation (Private or Public) among other factors. The interoperability test designed for this solution guide included LTE service, maximum coverage availability, and a public IP address assigned to each device.

The processes described herein assume the following:

- Broadband router with a single RJ45 (Ethernet) WAN interface
- Available LAN ports
- Administrative access to the broadband router's local GUI

While administration portals may vary greatly, depending on the make and model of the router being utilized, the underlying configuration remains the same.

NOTE: If additional LAN ports are necessary for practical use, a switch can be introduced without requiring additional configuration. Connect the switch to an available LAN port and proceed with the processes described herein.

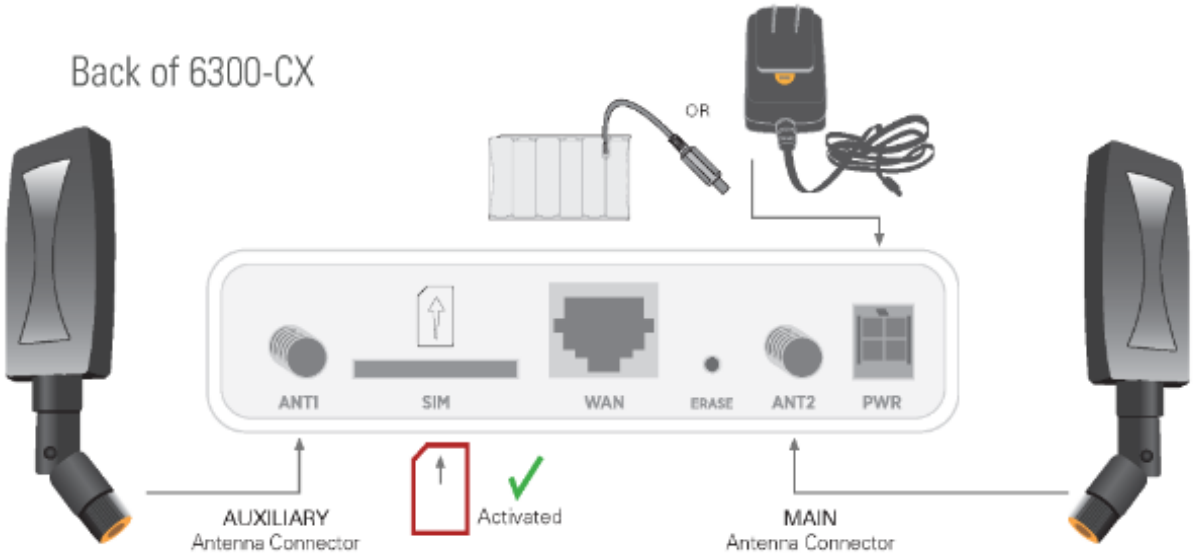
Accelerated 6300-CX LTE Router Setup

Initial Setup

Affix both antennas to the router and insert an activated SIM card before deploying the device. Be sure to select a location with optimal signal strength. For detailed instruction, refer to the tables that follow. Subsequent sections will outline site selection, powering options, and other device functionality.

Step-by-Step Guidance: Initial Setup

1. Insert the activated 2FF SIM card provided by your cellular network operator (putting the cut corner in first with metal contacts facing down). The card clicks into place when completely inserted.
2. Attach the two included antennas; both should be installed for optimal operation. Do this by gripping the metal connector section with your thumb and forefinger, tightening until secure. Do not tighten the antenna by holding any part of the plastic antenna housing.
3. To determine the optimal location for the 6300-CX, please see the “Site Survey” section.
4. Refer to the section(s) for Remote or Direct Power Installations when ready to connect the 6300-CX to the permanent power supply unit.
5. The 6300-CX uses DHCP with IP Passthrough by default, which satisfies the setup requirements for most environments. If required, please use Accelerated View™ or the 6300-CX local GUI to configure the 6300-CX for router mode.



Site Survey

If you are unsure of the available cellular signal strength, or are choosing between several locations, please follow the instructions to identify the ideal installation site.

Step-by-Step Guidance: Site Survey

1. After following steps 1 and 2 in the “Initial Setup” section, connect the battery pack to temporarily power the Accelerated 6300-CX. The charge lasts two to four hours – it is not rechargeable and should be properly disposed of after use.

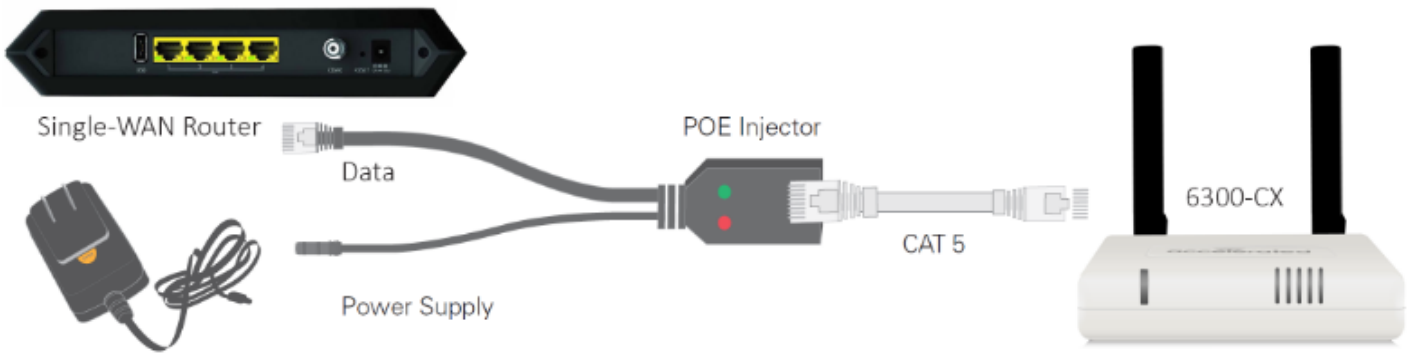
2. Move the 6300-CX to different locations within your site to determine the best compromise between signal strength and installation constraints. Since cellular signal strength may fluctuate, it is important to **wait at each location for 1 minute while observing the signal strength indicator** on the front of the device. Minimum cellular signal strength for operation is 2 bars (3+ is preferred).
3. After determining the optimal location, remove the battery pack and connect the main power supply unit or Ethernet cable connected to the PoE injector (per the power option outlined below).

Remote Power Installation – Powering Option #1

The included Power-over-Ethernet (PoE) injector allows the device to be positioned away from power outlets to simplify its installation needs. The adaptor consolidates the DC power and Ethernet connections so that both can be run to the 6300-CX via a single Ethernet cable. Distances of 300 ft have been tested on CAT6 and 250 ft on CAT5e. Note that cable conditions and the number of splices will impact actual distance.

Step-by-Step Guidance: Remote Power Installation

1. Plug the 6300-CX's power supply unit (PSU) into an AC power outlet.
2. Connect the end of the PSU into the DC input (4 pin connector) of the PoE injector.
3. Insert the male RJ45 connector of the PoE injector cable into the broadband router.
4. Connect an Ethernet cable from the RJ45 socket on the PoE injector cable to the Ethernet port of the 6300-CX. (See diagram.)



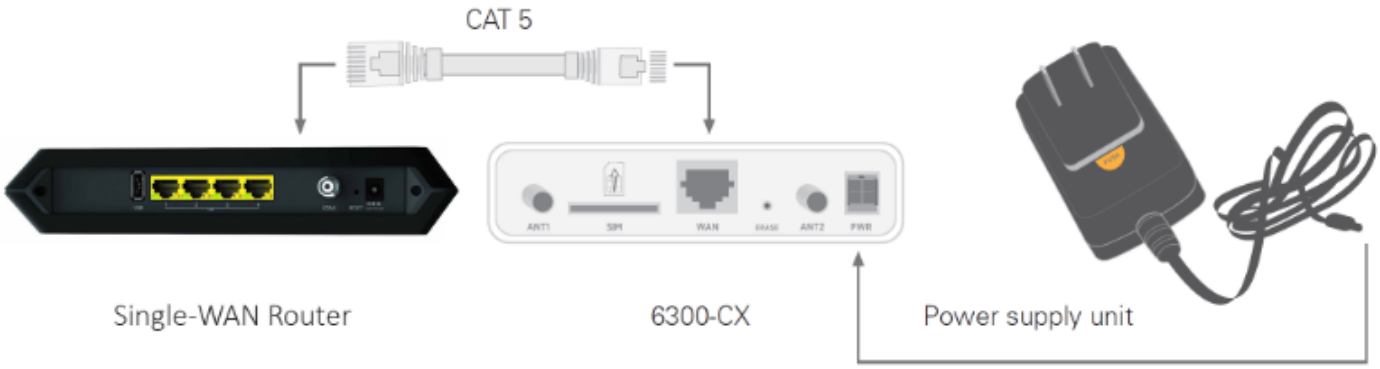
Direct Power Installation – Powering Option #2

If you plan to collocate the 6300-CX with the MX device, you can directly power the 6300-CX without the PoE cable.

Step-by-Step Guidance: Direct Power Installation

NOTE: A single-WAN router will not delineate between primary and secondary ports. This will be handled during device configuration.

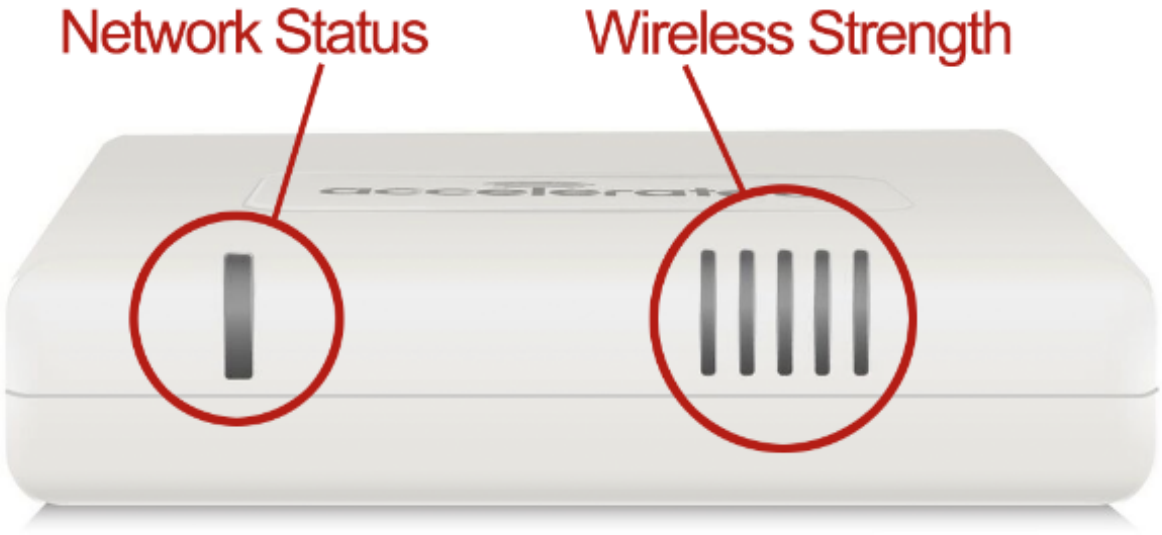
1. Use an Ethernet cable to connect the 6300-CX to the router using the primary WAN port (to use the cellular network as the primary connection) or the secondary WAN port (to configure a failover).
2. Plug the 6300-CX power supply unit (PSU) into an AC power outlet.
3. Connect the PSU into the 4-pin power connector of the 6300-CX. (See diagram.)



Understanding the 6300-CX LEDs

Once power has been established, your device will initialize and attempt to connect to the network. Device initialization may take 30-60 seconds. Indicator lights on the **Wireless Strength Indicator** show you the cellular network signal strength. The **Network Status Light** on the front left of the device displays connectivity information.

Please visit accelerated.com for additional information and troubleshooting tips.



Network Status LED

Solid Yellow
Initializing or starting up.

Flashing Yellow
In the process of connecting to the cellular network and to a device on its Ethernet port.

Flashing White
Has an Ethernet connection and is in the process of connecting to the cellular network.

Flashing Green
Connected to 2G or 3G and is in the process of connecting to a device on its Ethernet port (or nothing is connected to the port).

Solid Green
Connected to 2G or 3G and also has an Ethernet connection.

Flashing Blue
Connected to 4G LTE and in the process of connecting to a device on its Ethernet port.

Solid Blue
Connected to 4G LTE and also has an Ethernet connection.

Alternating Red/ Yellow
Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Wireless Strength LEDs

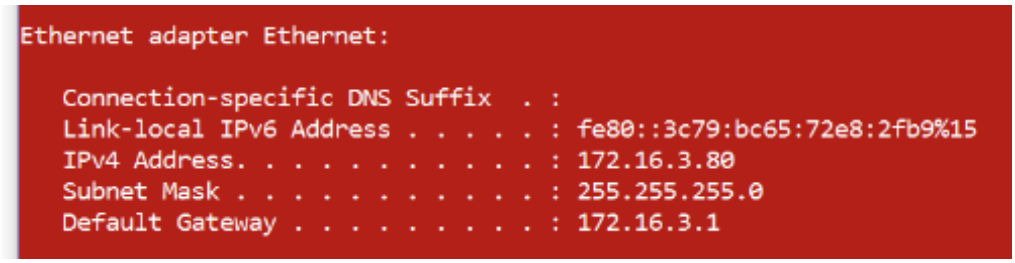
Signal Bars	Weighted dBm	Signal Strength %	Quality
	-113 to -99	0 - 23%	Bad
	-98 to -87	24 - 42%	Marginal
	-86 to -76	43 - 61%	OK
	-75 to -64	62 - 80%	Good
	-63 to -51	81 - 100%	Excellent

Single-WAN Router Configuration with the 6300-CX

Disable DHCP for the Single-WAN Router

Dynamic Host Configuration Protocol (DHCP) allows routers to assign IP addresses on a first-come, first-serve basis while also ensuring each device has a unique IP. Thanks to DHCP, routers can grant simultaneous Internet access to multiple devices using a single WAN interface. It is strongly encouraged that networks have only one active DHCP server at any given time or else overlapping IP addresses may be assigned to connected equipment. When integrating the Accelerated 6300-CX LTE Router as part of a single-WAN solution, the 6300-CX can act as the DHCP server even while using the wireline connection as its primary WAN route. Most of this configuration occurs within the CX's administration portal though the first step is always making sure the broadband router's DHCP services are disabled within the local GUI.

Most routers are configured by browsing to the IP address listed as the **Default Gateway** under ipconfig.



Proprietary GUIs will vary depending on the make and model of the single-WAN router, though the overall configuration remains the same. First, identify where the TCP/IP or LAN settings are located, and then navigate to the DHCP properties. These options are sometimes included as part of the device's "advanced" functionality and may not be directly accessible until advanced configuration is enabled. Note that devices connected to the router will lose Internet access after DHCP is disabled until the 6300-CX is configured per the steps outlined in the next section. The router's local GUI may take a minute or two to refresh as its DHCP settings are updated.

Please refer to the documentation included with the single-WAN router for a walkthrough of its configuration menu.

Step-by-Step Guidance: Disabling DHCP for the Single-WAN Router

1. Using a web browser, navigate to the single-WAN router's local GUI. This is most often the same address as the **Default Gateway.**
2. Identify the menu option that houses TCP/IP or LAN settings.
3. Disable the router's DHCP-Server functionality.
4. Finalize the configuration by clicking the "apply" or "save" button.
5. Wait for the device to reboot before continuing.

NOTE: Without DHCP enabled, the router will reboot and can still be reached via the local GUI through connected devices will no longer receive an IP address automatically (until the 6300-CX is configured per this document).

Enable Router Mode on the Accelerated 6300-CX

With DHCP routing disabled on the single-WAN device, the Accelerated 6300-CX must be configured to take over the assignment of IP addresses. It cannot do so, however, until IP Passthrough is disabled on the Accelerated device. Reconfiguring the 6300-CX in this manner places the CX in "Router Mode." The settings outlined below should be applied from the Configuration tab of Accelerated View™ although local administration is also possible if the need arises.

Please refer to the 6300-CX User Manual for an in-depth walkthrough of both remote and local administration.

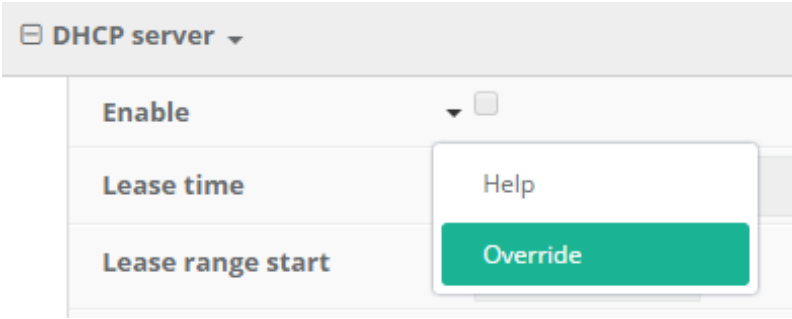
Step-by-Step Guidance: Enable Router Mode on the 6300-CX

1. Sign in to Accelerated View and locate the 6300-CX by entering its **MAC address** in the **Search** field. The MAC address is a 12-character code included on the 6300-CX's bottom label.
2. Click on link in the **MAC** column to bring up the device's profile.
3. Navigate to the **Configuration** tab.
4. When configuring Accelerated devices, it is best to utilize **Group Configuration** profiles so that settings can be centrally stored and later applied to additional devices. Click the **Edit group configuration** link to proceed with the device setup.
5. **Settings** in Accelerated View are categorized and nested according to their scope of configuration. The "-->" symbol denotes nested categories. **Network --> Interfaces --> LAN**, for example, points to the **LAN** menu nested inside the **Interfaces** section within the **Network** category:
6. **Modem --> Passthrough:** deselect the **Enable** checkbox
7. **Network --> Interfaces --> LAN:** select the **Enable** checkbox
8. **Network --> Interfaces --> LAN --> IPv4:** set **Interface type** to **Static IP address**
9. **Network --> Interfaces --> LAN --> IPv4:** specify the **Address** of the LAN DHCP network as X.X.X.65/26 *
10. **Network --> Interfaces --> LAN --> IPv4 --> DHCP server:** select the **Enable** checkbox and set the **lease range** to **start** at 66 and **end** at 126
11. **Network --> Interfaces --> LAN --> IPv4 --> DNS servers:** enter a pair of DNS servers to use by clicking the **Add** button; 8.8.8.8 and 4.2.2.4 are suitable defaults if no specific DNS address is preferred
12. Click **Update** to finalize the new settings.
13. To apply the new settings immediately, reboot the CX or reference the step-by-step guidance for issuing remote commands.

*The first three values of the IP address MUST match those belonging to the single-WAN router's default gateway. The fourth value corresponds to the lease range; use the values provided above unless otherwise notified.

Devices sync with Accelerated View once a day by default; pending configuration updates will apply at this time.

Changes made to a group configuration are applied to ALL devices assigned to that group. To adjust settings for individual devices, select the **Override** button from the pull-down menu situated next to each field/ setting in question and make any necessary changes without editing the group config.



Add a New WAN Interface

The Accelerated 6300-CX can be configured to interface with additional uplinks outside of the connectivity established by its cellular modem. When deployed with a single-WAN broadband modem, the 6300-CX is capable of acting as the network's DHCP server while still leveraging the coaxial WAN interface as its primary means of Internet access. The cellular connection then serves as a failover uplink that only becomes active if the broadband connection becomes unavailable. This functionality requires the creation of a new WAN interface in Accelerated View™.

Please refer to the 6300-CX User Manual for an in-depth walkthrough of both remote and local administration.

Step-by-Step Guidance: Adding a New WAN Interface

1. Sign in to Accelerated View and locate the 6300-CX by entering its **MAC address** in the **Search** field.
2. Click on link in the **MAC** column to bring up the device's profile.
3. Navigate to the **Configuration** tab.
4. When configuring Accelerated devices, it is best to utilize **Group Configuration** profiles so that settings can be centrally stored and later applied to additional devices. Click the **Edit group configuration** link to proceed with the device setup.
5. **Settings** in Accelerated View are categorized and nested according to their scope of configuration. To create a new interface, first expand the **Network** menu and then expand the **Interface** section.

6. Use the **Add Interface** field to enter a name for the connection coming from the single-WAN router (e.g. “Primary WAN”).
7. Set the **Zone** to “External” and the **Device** to “LAN” using the corresponding menu selections.
8. The **Default gateway** will be the same IP address used to connect to the single-WAN router (when disabling DHCP on the device as explained on page 6 of this document).
9. In the **Address** field, enter X.X.X.2/27*
10. Set the **Metric** to 1. The 6300-CX attempts to connect to the Internet using its active WAN uplink with the lowest metric value first before failing over to the cellular connection, which has a higher metric.
11. Click **Update** to finalize the new settings.
12. To apply the new settings immediately, reboot the CX or reference the step-by-step guidance for issuing remote commands.

*The first three values of the IP address **MUST** match those belonging to the single-WAN router’s default gateway. The fourth value corresponds to the lease range; use the values provided above unless otherwise notified.

Devices sync with Accelerated View once a day by default; pending configuration updates will apply at this time.

Changes made to a group configuration are applied to ALL devices assigned to that group. To adjust settings for individual devices, select the **Override** button from the pull-down menu situated next to each field/ setting in question and make any necessary changes without editing the group config.

Initialize Active Recovery

Active Recovery allows the 6300-CX to recognize when an interface has reconnected to the Internet in order to failback to the intended primary uplink. Connections can be monitored by a handful of preconfigured testing conditions, though the most common choice is to perform a ping test. Once the router recognizes that connectivity has been restored, based off of user-defined success conditions, the device can be configured to automatically restart the interface. The 6300-CX will then utilize the active WAN connection with the lowest metric value, per

Please refer to the 6300-CX User Manual for an in-depth walkthrough of both remote and local administration.

Step-by-Step Guidance: Initializing Active Recovery

1. Sign in to Accelerated View and locate the 6300-CX by entering its **MAC address** in the **Search** field.

2. Click on link in the **MAC** column to bring up the device's profile.
3. Navigate to the **Configuration** tab.
4. When configuring Accelerated devices, it is best to utilize **Group Configuration** profiles so that settings can be centrally stored and later applied to additional devices. Click the **Edit group configuration** link to proceed with the device setup.
5. **Settings** in Accelerated View are categorized and nested according to their scope of configuration. To create a new interface, first expand the **Network** menu and then expand the **Interface** section.
6. Expand the **WAN** interface (created per the previous page of this document) and expand **Active Recovery**.
7. Select the **Enable** and **Restart interface** checkboxes both must be checked.
8. Set the **Interval** to 1m or however often the 6300-CX should check on the interface.
9. Adjust the **Success condition** and its corresponding **Attempts** and **Response timeout** if necessary.
10. Expand **Test targets** and click the **Add** button.
11. Set the **Test type** to "Ping test" and point the **Ping host** to 8.8.8.8
12. Click the **Add** button.
13. Set the **Test type** to "DNS Test" and point the **DNS server** to 8.8.4.4 - **Note:** 2 different tests are recommended to prevent false positives.
14. Click **Update** to finalize the new settings.
15. To apply the new settings immediately, reboot the CX or reference the step-by-step guidance for issuing remote commands.

*The first three values of the IP address MUST match those belonging to the single-WAN router's default gateway. The fourth value corresponds to the lease range; use the values provided above unless otherwise notified.

NOTE: Best practices dictate that redundant tests (with divergent failure conditions) will be the best way to ensure proper connectivity monitoring/active recovery. With only a single test type, false positives could be reported.

Devices sync with Accelerated View once a day by default; pending configuration updates will apply at this time.

Changes made to a group configuration are applied to ALL devices assigned to that group. To adjust settings for individual devices, select the **Override** button from the pull-down menu situated next to each field/ setting in question and make any necessary changes without editing the group config.

Configuration for AT&T VPN Gateways

Overview

The Accelerated 6300-CX LTE Router provides a reliable, high-speed cellular connection that is compatible with existing wireline infrastructure. While its 4G LTE speeds are capable of operating as a primary WAN uplink, the 6300-CX can also be configured as a backup. This network redundancy solution delivers the ultimate flexibility to minimize expenses when it comes time for upgrading equipment to the latest wireless standards.

Business continuity depends on the seamless integration of failover-connectivity solutions to prevent service interruptions. Now more than ever, contingency networks play a strategic role in sustaining business operations. Unplanned outages can cost companies significant time and money, frustrating employees and clients alike, which creates a negative perception that is difficult to overcome.

Cellular data (4G LTE) bypasses wireline Internet service providers (ISPs) to facilitate the best redundancy possible. Additionally, in some situations it may be a challenge to acquire access to wired circuits or an event may call for temporary online access. For these reasons, Accelerated Concepts designed its 6300-CX LTE router to offer comprehensive, flexible cellular network integrations for small businesses, retail, government, remote sites, and branch offices.

The AT&T U110 is an eighth-generation AT&T VPN Gateway that has been developed by AT&T since 2001. As a customer premises equipment (CPE) hardware device, it serves as a centrally managed firewall, router, VPN device, and VLAN switch that acts as a fully managed security device. Networks that leverage the U110 are protected from the Internet while still having secure access to an enterprise environment through a secure IPSec VPN tunnel that supports the highest level of encryption (256-bit AES).

Leveraging the 6300-CX's flexible mounting options, the Accelerated LTE router can be deployed in a location with strong cellular reception and deliver LTE connectivity to the VPN Gateway via Ethernet cabling. Power-over-Ethernet extends the CX's reach to optimize signal strength without necessitating the relocation of the U110 or other client appliances.

Please refer to the AT&T VPN Gateway Datasheets for more information.

(Access to the URL linked above is private. Reach out to your AT&T rep for documentation if the link doesn't work.)

Interoperability Matrix

This section covers interoperability information of the hardware tested for this solution. It includes the firmware versions of both devices as well as the date of testing.

Date	U110 Firmware	6300-CX Firmware
05/2017	6.4.X	17.2.22

Caveats

IMPORTANT: U110s distributed for use in the United States are outfitted with an embedded LTE modem. This cellular connection may be leveraged for primary or backup Internet access, though the U110 can only be configured to recognize 2 WAN connections simultaneously. Interoperability with the 6300-CX implies that the VPN Gateway has been staged for single-WAN connectivity (either wireline or embedded cellular). Please refer to the U110 Install Guide for setup guidance.

The delivery of wireless services varies depending on the carrier and may lead to differences in the area of coverage, type of service (3G, 4G, LTE, etc.), availability of bandwidth, and IP address designation (Private or Public) among other factors. The interoperability test designed for this solution guide included LTE service, maximum coverage availability, and a public IP address assigned to each device.

Using the 6300-CX as a secondary connection assumes that a primary WAN is available, either via an Ethernet cable plugged into the WAN 1 port on the AT&T VPN Gateway or its embedded cellular connection. Connect the 6300-CX's Ethernet cable to port WAN 2 and proceed to the configuration described herein.

Accelerated 6300-CX LTE Router Setup

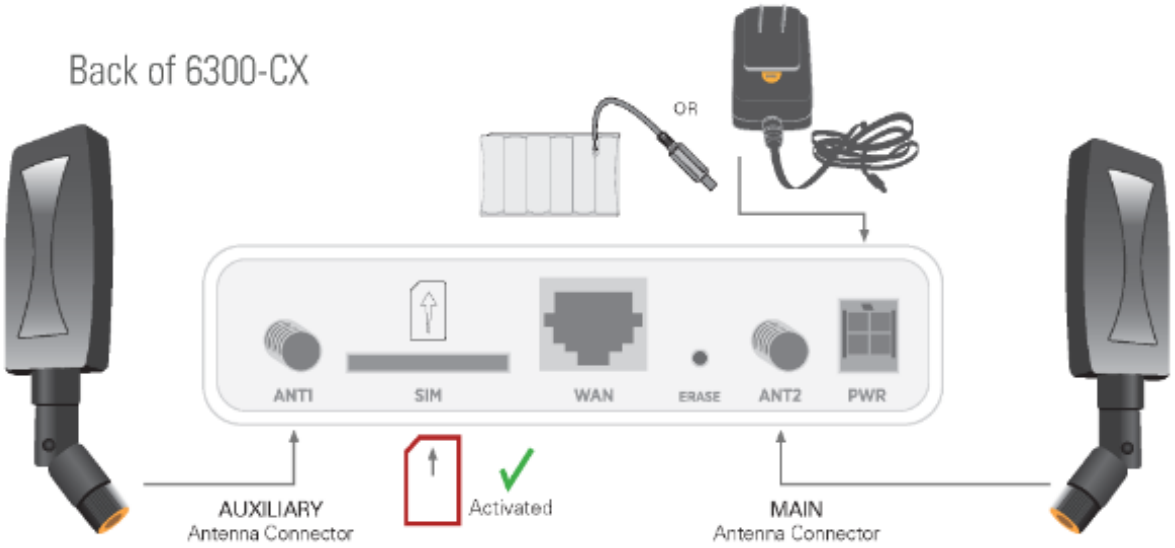
Initial Setup

Affix both antennas to the router and insert an activated SIM card before deploying the device. Be sure to select a location with optimal signal strength. For detailed instruction, refer to the tables that follow. Subsequent sections will outline site selection, powering options, and other device functionality.

Step-by-Step Guidance: Initial Setup

1. Insert the activated 2FF SIM card provided by your cellular network operator (putting the cut corner in first with metal contacts facing down). The card clicks into place when completely inserted.
2. Attach the two included antennas; both should be installed for optimal operation. Do this by gripping the metal connector section with your thumb and forefinger, tightening until secure. Do not tighten the antenna by holding any part of the plastic antenna housing.
3. To determine the optimal location for the 6300-CX, please see the "Site Survey" section.

4. Refer to the section(s) for Remote or Direct Power Installations when ready to connect the 6300-CX to the permanent power supply unit.
5. The 6300-CX uses DHCP with IP passthrough by default, which satisfies the setup requirements for most environments. If required, please use Accelerated View™ or the 6300-CX local GUI to configure the 6300-CX for router mode.



Site Survey

If you are unsure of the available cellular signal strength, or are choosing between several locations, please follow the instructions to identify the ideal installation site.

Step-by-Step Guidance: Site Survey

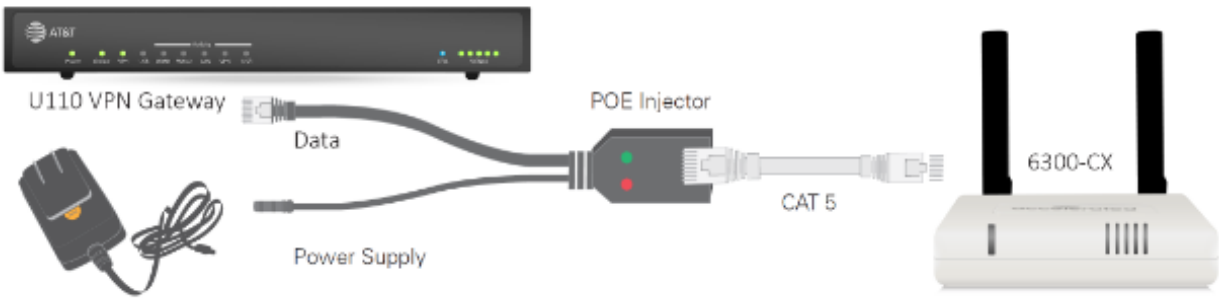
1. After following steps 1 and 2 in the “Initial Setup” section, connect the battery pack to temporarily power the Accelerated 6300-CX. The charge lasts two to four hours – it is not rechargeable and should be properly disposed of after use.
2. Move the 6300-CX to different locations within your site to determine the best compromise between signal strength and installation constraints. Since cellular signal strength may fluctuate, it is important to **wait at each location for 1 minute while observing the signal strength indicator on the front of the device.** Minimum cellular signal strength for operation is 2 bars (3+ is preferred).
3. After determining the optimal location, remove the battery pack and connect the main power supply unit or Ethernet cable connected to the PoE injector (per the power option outlined below).

Remote Power Installation – Power Option #1

The included Power-over-Ethernet (PoE) injector allows the device to be positioned away from power outlets to simplify its installation needs. The adaptor consolidates the DC power and Ethernet connections so that both can be run to the 6300-CX via a single Ethernet cable. Distances of 300 ft have been tested on CAT6 and 250 ft on CAT5e. Note that cable conditions and the number of splices will impact actual distance.

Step-by-Step Guidance: Remote Power Installation

1. Plug the 6300-CX's power supply unit (PSU) into an AC power outlet.
2. Connect the end of the PSU into the DC input (4 pin connector) of the PoE injector.
3. Insert the male RJ45 connector of the PoE injector cable into the VPN Gateway.
4. Connect an Ethernet cable from the RJ45 socket on the PoE injector cable to the Ethernet port of the 6300-CX. (See diagram.)

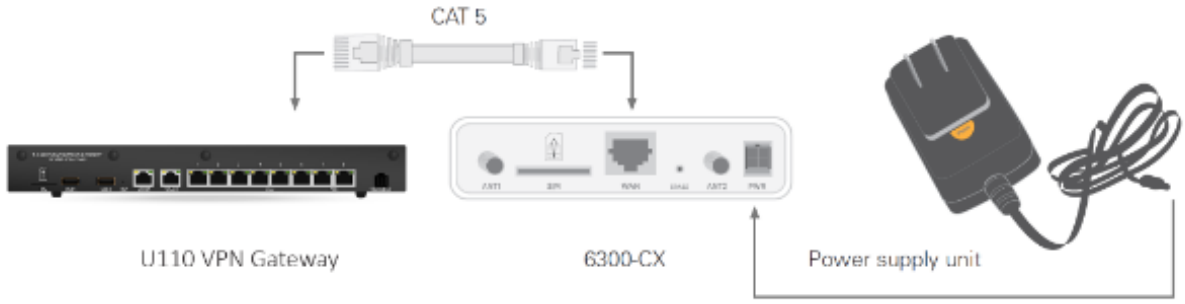


Direct Power Installation – Power Option #2

If you plan to collocate the 6300-CX with the VPN gateway, you can directly power the 6300-CX without the PoE cable.

Step-by-Step Guidance: Direct Power Installation

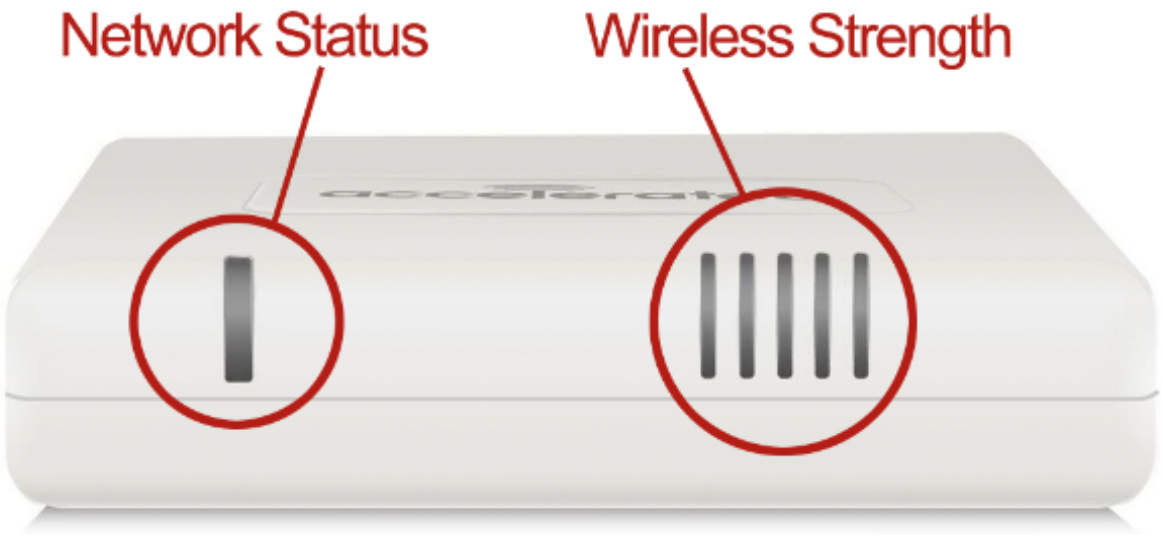
1. Use an Ethernet cable to connect the 6300-CX to the security appliance using port Internet 1 (to use the cellular network as the primary connection) or port Internet 2 (to configure a failover).
2. Plug the 6300-CX power supply unit (PSU) into an AC power outlet.
3. Connect the PSU into the 4-pin power connector of the 6300-CX. (See diagram.)



Understanding the 6300-CX LEDs

Once power has been established, your device will initialize and attempt to connect to the network. Device initialization may take 30-60 seconds. Indicator lights on the **Wireless Strength Indicator** show you the cellular network signal strength. The **Network Status Light** on the front left of the device displays connectivity information.

Please visit accelerated.com for additional information and troubleshooting tips.



Network Status LED

Solid Yellow
Initializing or starting up.

Flashing Yellow
In the process of connecting to the cellular network and to a device on its Ethernet port.

Flashing White
Has an Ethernet connection and is in the process of connecting to the cellular network.

Flashing Green
Connected to 2G or 3G and is in the process of connecting to a device on its Ethernet port (or nothing is connected to the port).

Solid Green
Connected to 2G or 3G and also has an Ethernet connection.

Flashing Blue
Connected to 4G LTE and in the process of connecting to a device on its Ethernet port.

Solid Blue
Connected to 4G LTE and also has an Ethernet connection.

Alternating Red/ Yellow
Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Wireless Strength LEDs

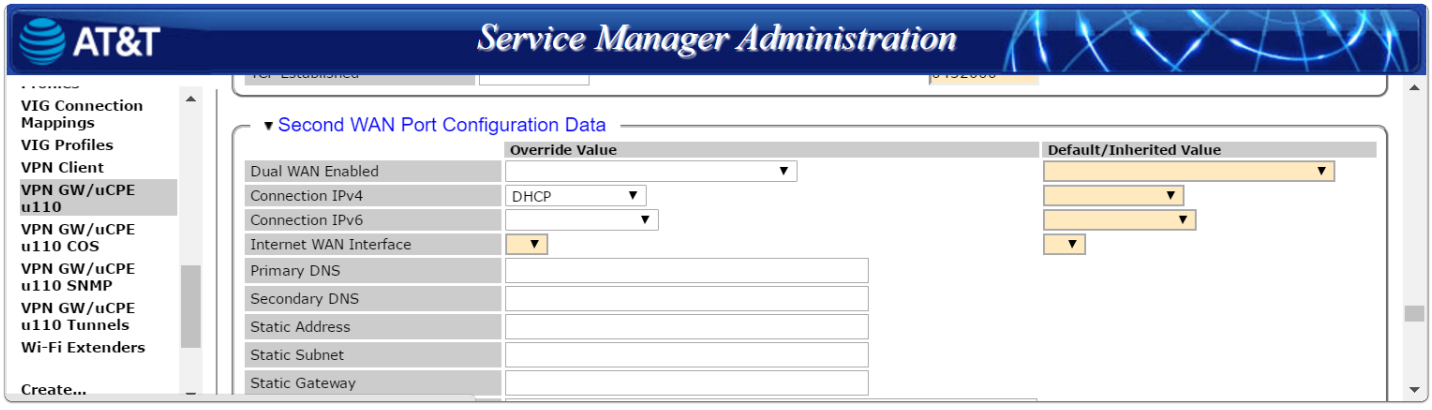
Signal Bars	Weighted dBm	Signal Strength %	Quality
	-113 to -99	0 - 23%	Bad
	-98 to -87	24 - 42%	Marginal
	-86 to -76	43 - 61%	OK
	-75 to -64	62 - 80%	Good
	-63 to -51	81 - 100%	Excellent

AT&T VPN Gateway Configuration with the 6300-CX

Cellular as Failover/ Backup WAN

After the 6300-CX is online with an activated cellular data plan, connect it to the WAN 2 port of the AT&T VPN Gateway via an Ethernet cable. The gateway is configured to recognize WAN 2 as a backup connection by default though additional settings must be enabled for optimal failover. These changes can be implemented using AT&T's Service Manager web-based administration GUI or via the x3270 terminal emulator, which offers a text-based user interface for managing devices.

Access to AT&T Service Manager Administration is available at this URL.



Step-by-Step Guidance: DHCP Client Configuration

1. From the **Navigation Menu**, select **VPN GW/uCPE u110**.
2. Enter your device's **Account** and/ or **Device ID** and filter through available devices by clicking the **List AT&T VPN Gateways** button.
3. Select the intended **Device ID** to open its **Gateway Profile**.

4. Set **NAT-T Negotiation** to "Yes" using the corresponding pull-down menu.
5. Under the **Common Dial Settings** section, both **Initiate Dial Connection** and **Initiate VPN Backup Connection** should be set to "Persistent."
6. Scroll down to the **Second WAN Port Configuration Data** section and set the **Connection IPv4** pull-down menu to "DHCP."
7. Change the **WAN2 via Cell Extender** field to "NetBridge from Accelecon."
8. Enter "1410" for the **MTU Size**.

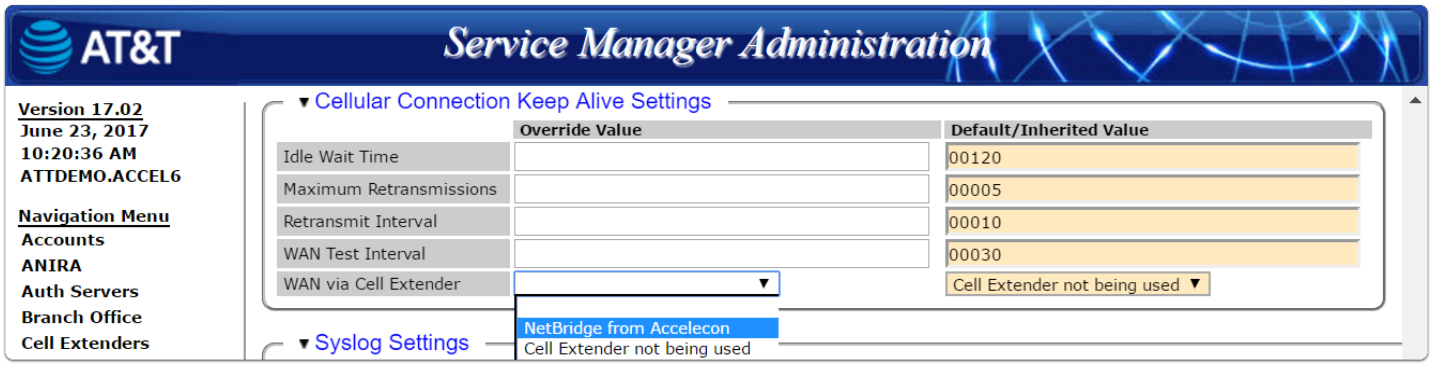
NOTE:*The last 8 fields of the **Second WAN Port Configuration Data** section establish the relevant keep-alive parameters used to establish failover intervals. These should never be changed unless Tier 4 support has been consulted.*

Cellular as Primary WAN

The back panel of the U110 features an array of LAN ports and two dedicated WAN interfaces. To utilize the 6300-CX's LTE Wireless WAN (WWAN) connectivity as the primary means of Internet access, connect the Accelerated LTE router to port WAN 1 on the VPN Gateway using an Ethernet cable. A solid blue light on the 6300-CX confirms that its 4G LTE modem is online and an Ethernet connection has been established with another device. Similarly, the U110's front panel features an Online indicator that will stay green to show that the device is connected to the Internet via the LTE router.

Please refer to the AT&T VPN Gateway Install Guides for an in-depth walkthrough.

(Access to the URL linked above is private. Reach out to your AT&T rep for documentation if the link doesn't work.)



Step-by-Step Guidance: Primary WWAN

1. From the **Navigation Menu**, select **VPN GW/uCPE u110**.
2. Enter your device's **Account** and/ or **Device ID** and filter through available devices by clicking the **List AT&T VPN Gateways** button.
3. Select the intended **Device ID** to open its **Gateway Profile**.

4. Set **NAT-T Negotiation** to “Yes” using the corresponding pull-down menu.
5. Enter “1410” for the **WAN MTU Size**
6. NOTE: *These fields are located under the **Basic Settings** section of the device administration portal.*
7. Under the **Cellular Connection Keep Alive Settings** section, change the **WAN via Cell Extender** field to “NetBridge from Accelcon.”

NOTE:*The first 4 fields of the **Cellular Connection Keep Alive Settings** section establish the relevant keep-alive parameters used to establish failover intervals. These should never be changed unless Tier 4 support has been consulted.*

Accelerated View Ports and URL Access

IP Address

128.136.167.120 with Ports (UDP: 123, 514 TCP: 443, 500/4500 IPsec)

URLs

time.accns.com; logs.accns.com; syslog.accns.com; certs.accns.com; configuration.accns.com; remote.accns.com

Optional IP

8.8.8.8 with UDP Port 53 – DNS backup and ping testing (customer can customize this value)

Data Usage Estimates

The 63xx LTE Routers are designed to be sensitive to the data usage on a customer's wireless data plan. Careful consideration was applied to add reporting, alerting, and remote control features through the best-of-breed Accelerated View™ cloud management system. Please note that even though the service was designed with standard reporting/ control intervals these values can be adjusted downward to obtain near-zero data utilization or, conversely, remote services can be tuned up for more aggressive monitoring at the expense of additional data utilization. The current Accelerated View architecture requires that all devices have a minimum of 1 publicly reachable IP address to access cloud-based features (see below).

NOTE: These values are estimates to be used for planning purposes -- the actual carrier data measurement may vary.

Data Consumption for Accelerated View Services

Service/ Function	Status/ Interval	Usage	Notes
Cloud-based Reporting/ Configuration	Standard (every 30 min)	3MB (per month)	Includes one startup sequence
Remote Control (IPSec tunnel)	Central management is enabled by default	25MB (per month)	Minimum keep-alive traffic

For deployments with heightened sensitivity toward data usage, the IPSec remote control tunnel can be disabled. Cloud-based reporting and configuration can still be accomplished via SMS commands that are not subject usage metering on mobile data plans. Please consult Accelerated for more information before leveraging this approach, "Option 2" in the table below.

NOTE: Charges for SMS messages may apply. Please consult your cellular carrier for billing details.

Service/ Function	Status/ Interval	Usage	Notes
Option 2 (Contact Accelerated for help)	IPSec disabled	2MB	Uses SMS on demand

Itemized Breakdown of Services via Accelerated View

Service/ Function	Status/ Interval	Usage per status/interval	Notes	Protocol/port used
Syslog check-in	Every 30 minutes	1KB	Used for reporting and alerts	UDP 514 (syslog)
Configuration check-in	Once nightly -- 1am (UTC)	12KB	Recommended for remote management	TCP 443 (HTTPS)
Boot-up sequence	Each device reboot	24KB	Used for reporting and remote management	UDP 123 (NTP) UDP 514 (syslog)
Device firmware upgrade	As needed (~8 releases per year)	10MB	Updates device firmware upon new release	TCP 443 (HTTPS)
Modem firmware upgrade	As needed (less frequent than device firmware updates)	60MB	Updates firmware on the embedded cellular modem	TCP 443 (HTTPS)
Remote control tunnel	Always-on, if enabled	25MB per month	Minimum keep-alive traffic	UDP 500 and 4500 (IPSec)

Signal Bars Explained

The cellular signal strength bars of Accelerated LTE routers are calculated using various algorithms based on the network type it is connected to. For 4G LTE, the RSRP, SNR, and RSSI values are all factored in to determine the reported signal strength bars. For 3G networks (including HSPA+) and 2G networks, the signal strength bars are determined by the RSSI value.

4G LTE algorithm

Determine RSRP, SNR, and RSSI values separately, using the following

```
RSRP > -85, rsrp_bars=5
-95 < RSRP <= -85, rsrp_bars=4
-105 < RSRP <= -95, rsrp_bars=3
-115 < RSRP <= -105, rsrp_bars=2
-199 < RSRP <= -115, if we're connected to the cellular network, rsrp_bars=1, if not
rsrp_bars=0
```

If RSRP <= -199, then use RSSI as the value and run it through the same algorithm described above.

```
SNR >= 13, snr_bars=5
4.5 <= SNR < 13, snr_bars=4
1 <= SNR < 4, snr_bars=3
-3 < SNR < 1, snr_bars=2
-99 < SNR <= -3, if we're connected to the cellular network, snr_bars=1, if not
snr_bars=0
```

Once the snr_bars and rsrp_bars are determined, use the lesser of the two. That is the reported signal strength bars.

3G algorithm

Determine RSSI signal strength.

```
RSSI > -80, bars=5
-90 < RSSI <= -80, bars=4
-100 < RSSI <= -90, bars=3
-106 < RSSI <= -100, bars=2
RSSI <= -106, if we're connected to the cellular network, bars=1, if not bars=0
```

bars is then reported as the signal strength bars.

2G algorithm

Determine RSSI signal strength.

```
RSSI > -80, bars=5
-89 < RSSI <= -80, bars=4
-98 < RSSI <= -89, bars=3
-104 < RSSI <= -98, bars=2
RSSI <= -104, if we're connected to the cellular network, bars=1, if not bars=0
```

bars is then reported as the signal strength bars.

Firewall Capabilities

Number of Supported Firewall Rules

There is no software-defined limit to the number of rules that may be created. A safe upper limit, due to potential hardware constraints, would be **25,000 lines**.

Encrypted Throughput Capacity

AES-128 was used for testing encrypted throughput on Accelerated LTE routers, yielding the following results:

	Download	Upload
CX Series	150 Mbps	50 Mbps
SR Series	100 Mbps	50 Mbps

Concurrent Sessions

Default settings allow **8,192 concurrent sessions** though this value can be adjusted via custom configuration.

The maximum is 65,536 -- though this assumes sessions are short lived and/ or low-bandwidth -- a good upper limit is 10,000.

New Sessions per Second

No limit exists in the software, though a safe upper limit would be **150** sessions.

Wildcard IP Support

Wildcard IPs are supported via **custom firewall rules** (iptables), which leverage CIDR networking to set up a range of IPs (e.g. 192.168.0.1/24).

FQDN Support

FQDN is supported via **custom firewall rules** (iptables).

However, the FQDN is resolved at the time of process/applying the firewall rule, not with each packet inspected. Meaning, if the IP of a domain changes, the firewall rule will not apply to the

new IP address. You would have to reload the firewall for the device to resolve the domain to the new IP. It is better to stick with IP addresses in firewall rules instead of FQDNs.

Sprint Activation

SIM Setup

Sprint grants devices access to their network using specific SIM cards that correspond to the LTE modem being used, as well as the category of that modem. Special attention should be paid to matching up the SIM card to the type of modem.

The Cat-3 Sierra MC7354 modem uses a USIM card and the Cat-6 Sierra MC7455 modem uses the ISIM card. The part number printed on the SIM card indicates its type (see chart below for reference).

The **6300-CX LTE Router** and **1002-CM03 Plug-in Modem** use the *Sierra MC7354* and the **1002-CM06 Plug-in Modem** uses the *Sierra MC7455*.

NOTE: It is not recommended to move an active Sprint SIM card between modems because the Sprint network may disconnect the connection due to a mismatch between the SIM and the device ID. SIMs should always be activated to the unique device being used. The ID used to identify the device is the IMEI, which should be printed on the device. If the MEID is required instead, this can be calculated by removing the last digit from the IMEI.

Accelerated products support the 2FF SIM standard.

MC7354 module's UICC cards (USIM)

	2FF	3FF
SKU	CZ2100LWR	CZ2102LWR
OEM Part No.	SIMGLW106R	SIMGLW206R
UPC	760494000091	760492013536

MC7455 module's UICC cards (ISIM)

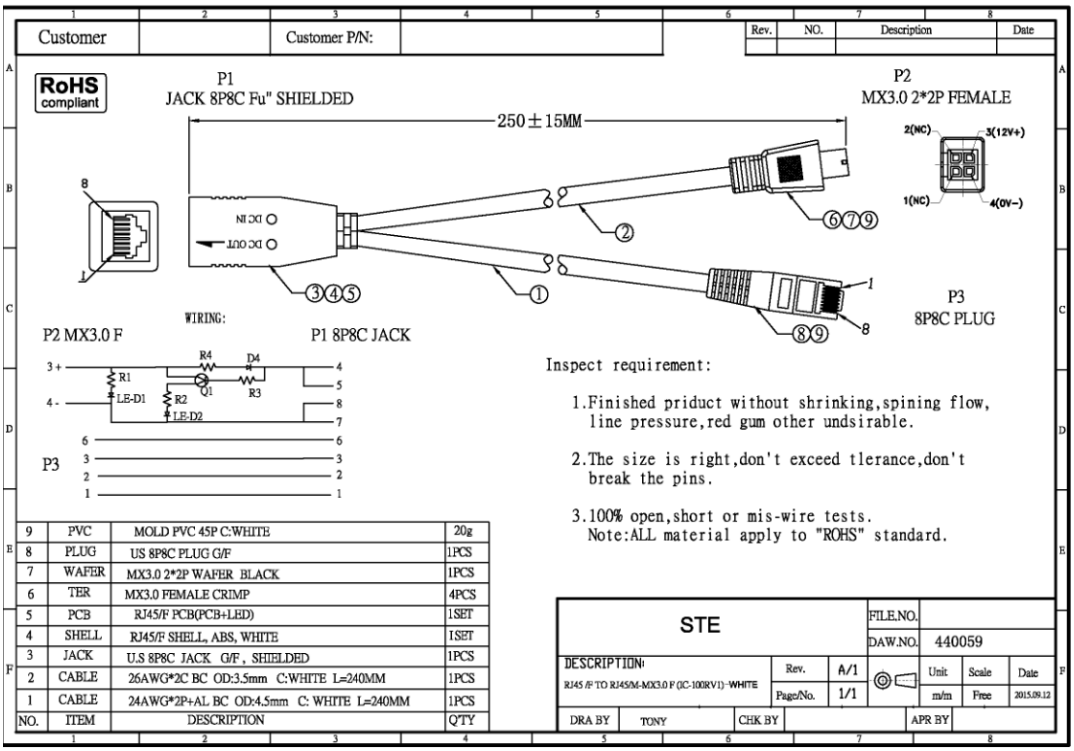
	2FF	3FF
SKU	CZ2100LWQ	CZ2112LWQ
OEM Part No.	SIMGLW106Q	SIMGLW216Q
UPC	019962040740	019962040948

Default LTE APNs

r.ispsn

n.ispsn

PoE Injector Schematic



6300-CX intermittent connectivity with static Verizon APNs [SOLVED]

Background

We've noticed a growing issue with some of our 6300-CX units that are connecting with Verizon SIM cards with static APNs (e.g. we01.vzwstatic, so01.vzwstatic, etc.). The problem is when bots or people on the internet try to attack the 6300-CX's passthrough IP, the 6300-CX is rejecting the attacks, which is good, but it's reject them with the wrong IP address, which Verizon doesn't like so they kill our cellular connection. The result is the 6300-CX's cellular connection will be bouncing up and down (evident by the fact that the LED on the 6300-CX goes from solid blue to flashing white, then solid blue for a few minutes and back to flashing white, rinse, repeat).

Solution

Firmware versions 17.2.22.5 or higher resolves the connectivity issues on the Verizon static APNs. You can use the following instructions to upgrade a 6300-CX or 6300-LX to the new 17.2.22.5 firmware:

https://accelerated.com/support/6300_CX/users_guide_web/#par-21

6300-CX provides intermittent connection to Cisco or Sonicwall Router [SOLVED]

Problem

Cisco or Sonicwall routers connected to the 6300-CX receive an IP address from the 6300-CX, but can only send packets for a few seconds before the connection drops.

Background

We've been running into this issue where 6300-CX units are sending out ARP requests with the default 192.168.210.1 IP address instaed of the gateway IP we get as part of the passthrough connection from the cellular network. I've encountered this issue while working with a Cisco Router and Sonicwall routers. In these cases, the routers would get a passthrough connection from the CX and work for a minute or so. However, when the CX sent an ARP request to the router to verify the IP and routes, the routers would not respond to the ARP request since the CX sent the ARP request with a source IP of 192.168.210.1. Since the routers weren't responding to the ARP request, the CX would not route packets to the router anymore, since it didn't know which interface/MAC to send those packets to.

Below are some links to articles I found from Sonicwall and Cisco as to why they don't respond to these ARP requests.

http://www.techrepublic.com/blog/smb-technologist/sonicwall-routers-and-dropped-arp-packets/

https://supportforums.cisco.com/document/100896/asa-843-arp-response-behavior-change

Solution

Firmware versions 17.5.108.6 or higher resolves the connectivity issues. The 6300-CX will use a gateway IP in the same subnet as the passthrough IP it gives to the Cisco/Sonicwall router for all ARP requests.

You can use the following instructions to upgrade a 6300-CX or 6300-LX to the new 17.5.108.6 firmware:

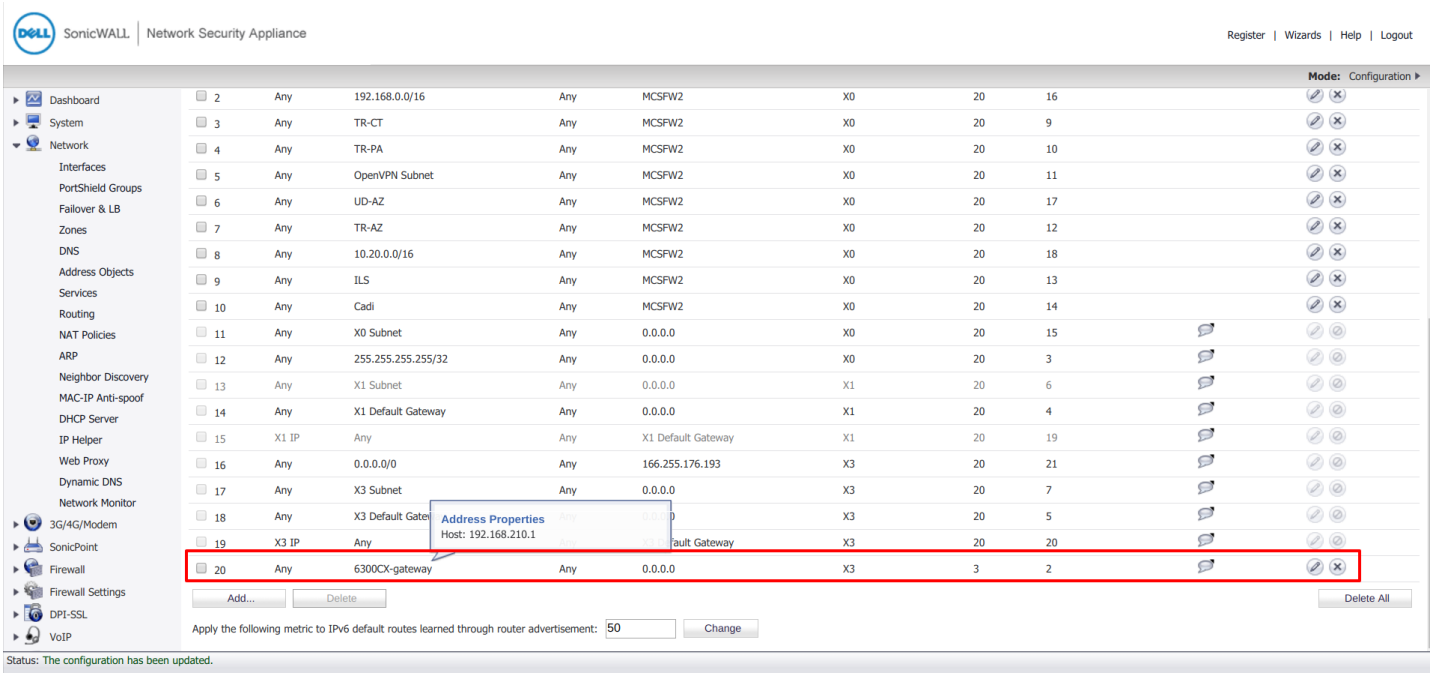
https://accelerated.com/support/6300_CX/users_guide_web/#par-21

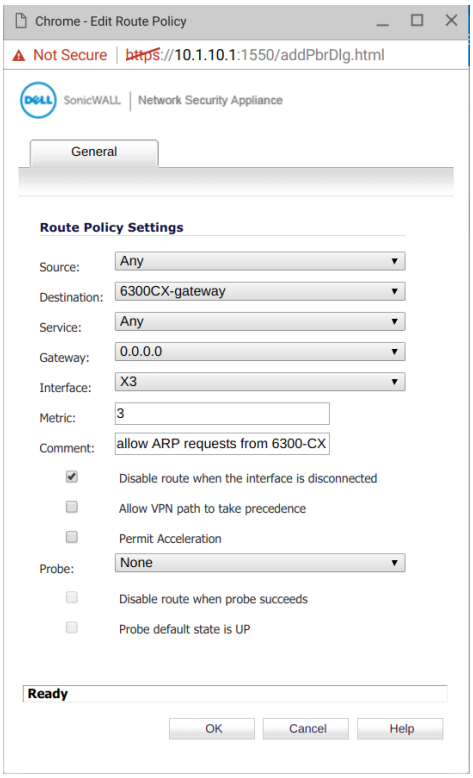
Manual Solution for Sonicwall

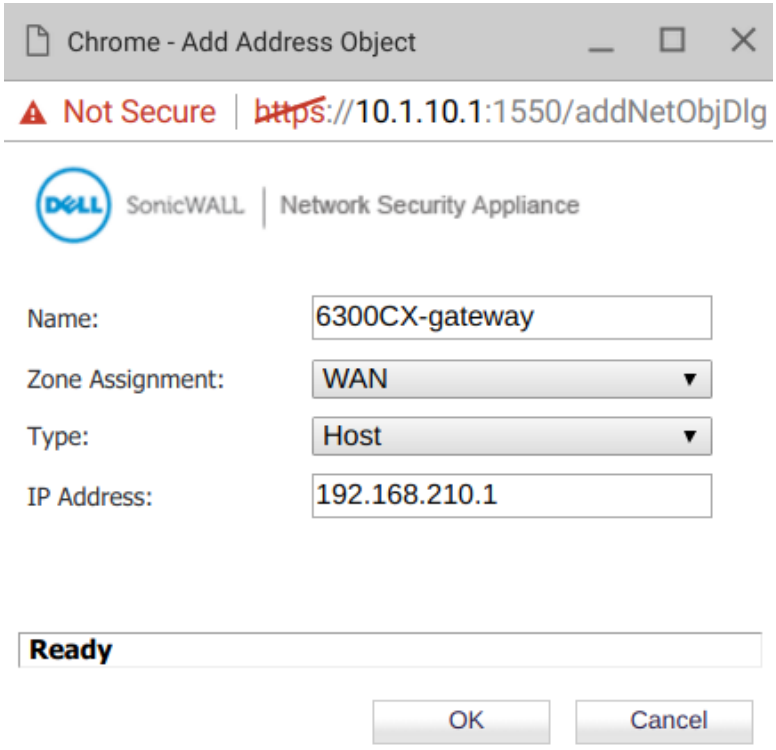
If you do not wish to upgrade the firmware on your 6300-CX, you can work around the issue by adding a manual route into the Sonicwall or Cisco router for the 192.168.210.1 address of the 6300-CX.

Follow the instructions here to resolve the issue by adding a route for 192.168.210.1 to the Sonicwall. I've also listed some screenshots below of when I added this route to a test TZ300 we have in the Tampa office

https://support.software.dell.com/sonicwall-e-class-nsa-series/kb/sw7587







I do not have an exact walkthough for adding a route for 192.168.210.1 to a Cisco router, but it should be very similar.

6300-CX provides invalid subnet for passthrough IP address [SOLVED]

Problem

The 6300-CX receives a passthrough IP address that is invalid with a /30 subnet, which prevents certain client routers connected to the 6300-CX from utilizing the passthrough connection due to an invalid gateway IP address.

Background

In firmware versions 16.7.49.12 or older, the 6300-CX always uses a /30 subnet in passthrough mode. However, not all cellular IP addresses are valid with a /30 subnet. As a result, the client device received a passthrough connection with a gateway IP address that did not match the ranger of the passthrough IP address and subnet.

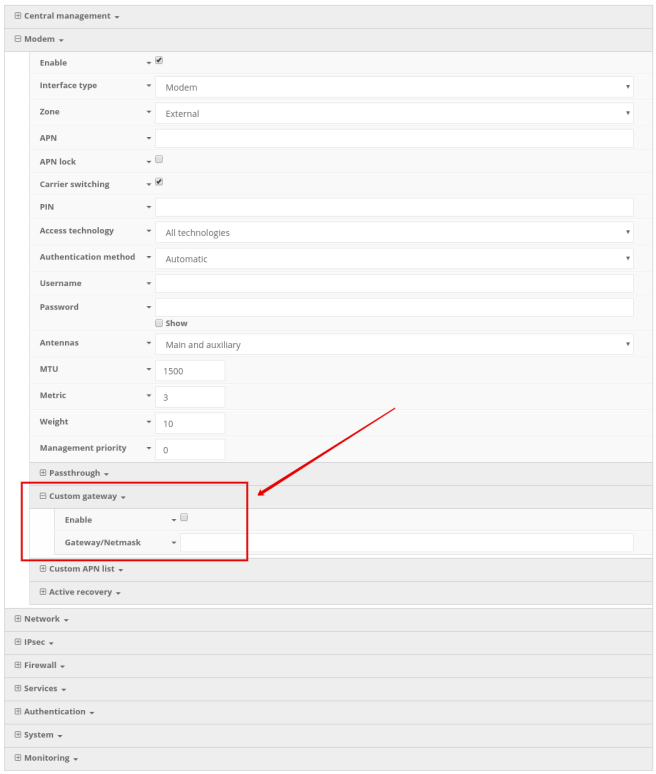
Solution

Firmware versions 16.10.32 or higher resolves the connectivity issues. The 6300-CX will automatically adjust the subnet if the /30 subnet does not match a valid range for the passthrough IP address. So as long as your 6300-CX devices are running firmware version 16.10.32 or higher, you should not see any subnet issues while in passthrough mode.

You can use the following instructions to upgrade a 6300-CX or 6300-LX to the new 16.10.32 firmware:

https://accelerated.com/support/6300_CX/users_guide_web/#par-21

Firmware versions 16.10.32 or higher also include extra options in the 6300-CX's configuration to manually set the subnet in passthrough mode, if desired. See screenshot below for reference.


Central management
Modem
Enable
Interface type
Modem
Zone
External
APN
APN lock
Carrier switching
PIN
Access technology
All technologies
Authentication method
Automatic
Username
Password
Show
Antennas
Main and auxiliary
MTU
1500
Metric
3
Weight
10
Management priority
0
Passthrough
Custom gateway
Enable
Gateway/Netmask
Custom APN list
Active recovery
Network
IPsec
Firewall
Services
Authentication
System
Monitoring

6300-CX only connects on 3G with Rogers SIM [SOLVED]

Problem

The 6300-CX is only able to establish a 3G cellular connection when using a Rogers SIM card.

Background

Rogers SIM cards with ICCIDs starting with 893027 were not properly recognized as Rogers SIMs by the 6300-CX device. As a result, the *Carrier Smart Select* tool would load the Generic carrier firmware onto the embedded modem inside the 6300-CX instead of the Rogers-specific carrier firmware. The generic carrier firmware only provides a 3G connection on the Rogers cellular network.

Solution

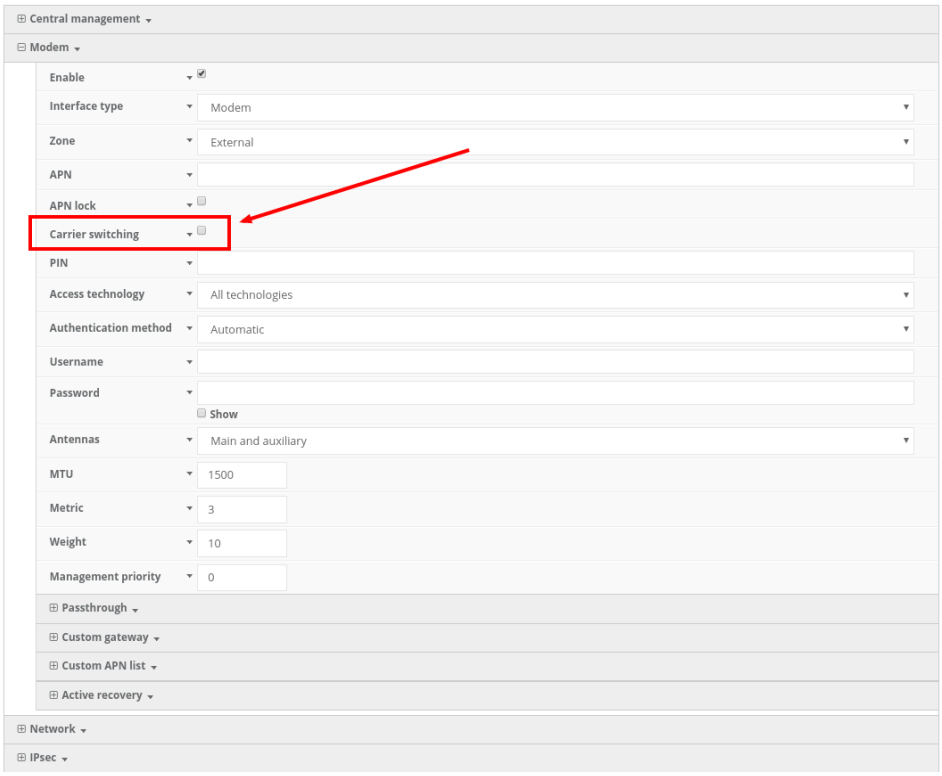
Firmware versions 17.8.128.24 or higher resolves the connectivity issues. You can use the following instructions to upgrade the 63xx-series router to the new 17.8.128.24 firmware:

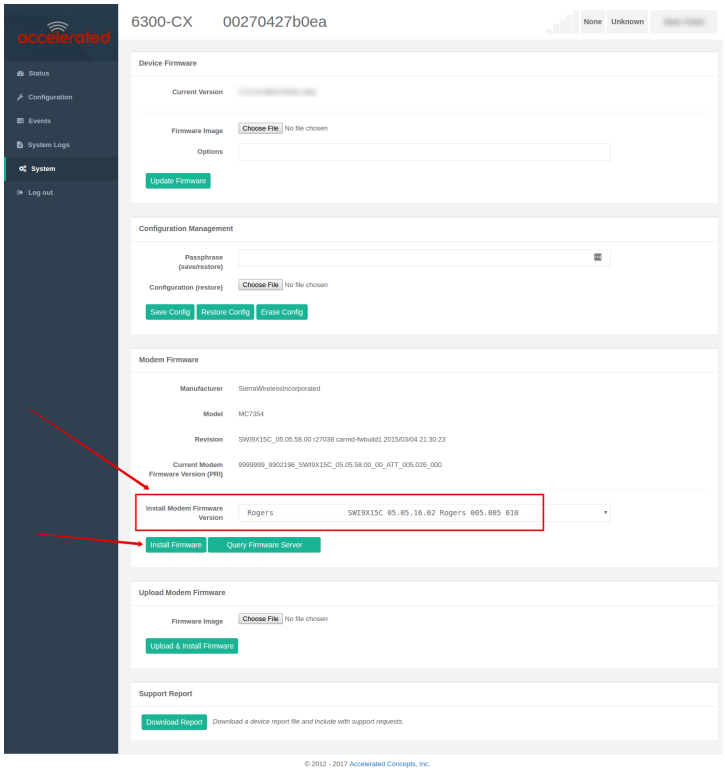
http://kb.accelerated.com/m/67492/l/742488-advanced-configuration-using-accelerated-view#upgrading_firmware

Manual Solution

Users can lock the 6300-CX LTE router to use the Rogers-specific carrier firmware. This will allow the 6300-CX to connect on the Rogers LTE network. To implement this manual solution:

1. Update the configuration profile of the Accelerated 6300-CX to disable the check-box under *Modem -> Carrier switching*.
2. Login to the local web UI of the 6300-CX, and access the *System* page. Use the drop-down in the *Modem firmware* section to select *Rogers,* and click *Install firmware*.


Central management
Modem
Enable
Interface type
Modem
Zone
External
APN
APN lock
Carrier switching
PIN
Access technology
All technologies
Authentication method
Automatic
Username
Password
Show
Antennas
Main and auxiliary
MTU
1500
Metric
3
Weight
10
Management priority
0
Passthrough
Custom gateway
Custom APN list
Active recovery
Network
IPsec


6300-CX
00270427b0ea
Status
Configuration
Events
System Logs
System
Log out
Device Firmware
Current Version
Firmware Image
Choose File
No file chosen
Options
Update Firmware
Configuration Management
Passphrase (save/restore)
Configuration (restore)
Save Config
Restore Config
Erase Config
Modem Firmware
Manufacturer
SierraWirelessIncorporated
Model
MC7354
Revision
Current Modem Firmware Version (PRI)
Install Modem Firmware Version
Rogers
SWI9X15C 05.05.16.02 Rogers 005.005 010
Install Firmware
Query Firmware Server
Upload Modem Firmware
Upload & Install Firmware
Support Report
Download Report
Download a device report file and include with support requests.
© 2012 - 2017 Accelerated Concepts, Inc.

Verizon SIM with static APN registers but doesn't connect [SOLVED]

Problem

A newly activated Verizon SIM with a static APN (e.g. ne01.vzwstatic) is inserted into a 63xx-series router. The 63xx-series router is able to detect the SIM and seeing an available Verizon network, but the 63xx-series router is unable to establish a cellular connection. The LED behavior on the front of the 63xx-series router will be a flashing white status/LTE LED, and intermittent 5 bars of signal strength.

Background

It can sometimes take longer than the 63xx-series router anticipates for the Verizon SIM to finish its registration process on the Verizon network. As a result, the 63xx-seris router tries establishing a cellular connection before this SIM finishes registering, which results in a failed connection. The 63xx-series router interprets this failed connection as it not using the correct APN, so it resorts to its fallback list of APNs to try alternate Verizon APNs with the SIM. Since the correct APN was already tried, this fallback list of APNs will try APNs that are not provisioned with the SIM. The result is the 63xx-series router gets stuck trying a fallback list of APNs, of which none will work with the given SIM.

Solution

Firmware versions 17.8.128.37 or higher resolves the connectivity issues. You can use the following instructions to upgrade the 63xx-series router to the new 17.8.128.37 firmware:

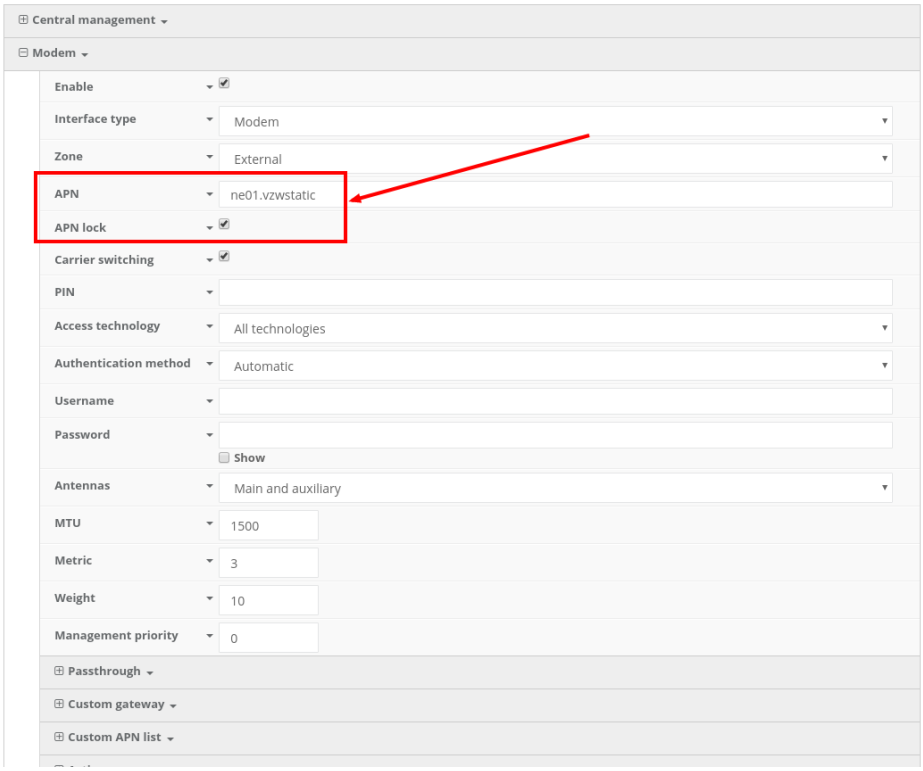
http://kb.accelerated.com/m/67105/l/729960-getting-started-with-accelerated-view#UpgradingFirmware

Manual Solution

Users can lock the 63xx-series router to keep trying the same APN. This allows the 63xx-series router to retry the same APN that the SIM card is provisioned with. Even if the 63xx-series router cannot establish a cellular connection with the SIM initially, it will keep trying with the same APN until it connects.

To implement this manual solution, update the configuration profile of the Accelerated 63xx-series router with the following configuration changes:

1. In ***Modem -> APN***, set the appropriate static APN (e.g. *ne01.vzwstatic*).
2. Enable the ***Modem -> APN lock*** checkbox.


Central management
Modem
Enable
Interface type
Modem
Zone
External
APN
ne01.vzwstatic
APN lock
Carrier switching
PIN
Access technology
All technologies
Authentication method
Automatic
Username
Password
Show
Antennas
Main and auxiliary
MTU
1500
Metric
3
Weight
10
Management priority
0
Passthrough
Custom gateway
Custom APN list

U110 unable to perform proactive monitoring through 63xx-series router [SOLVED]

Problem

An AT&T VPN Gateway or U110 is configured to perform Proactive Monitoring, but the monitoring tests fail when performed through a 63xx-series router.

Background

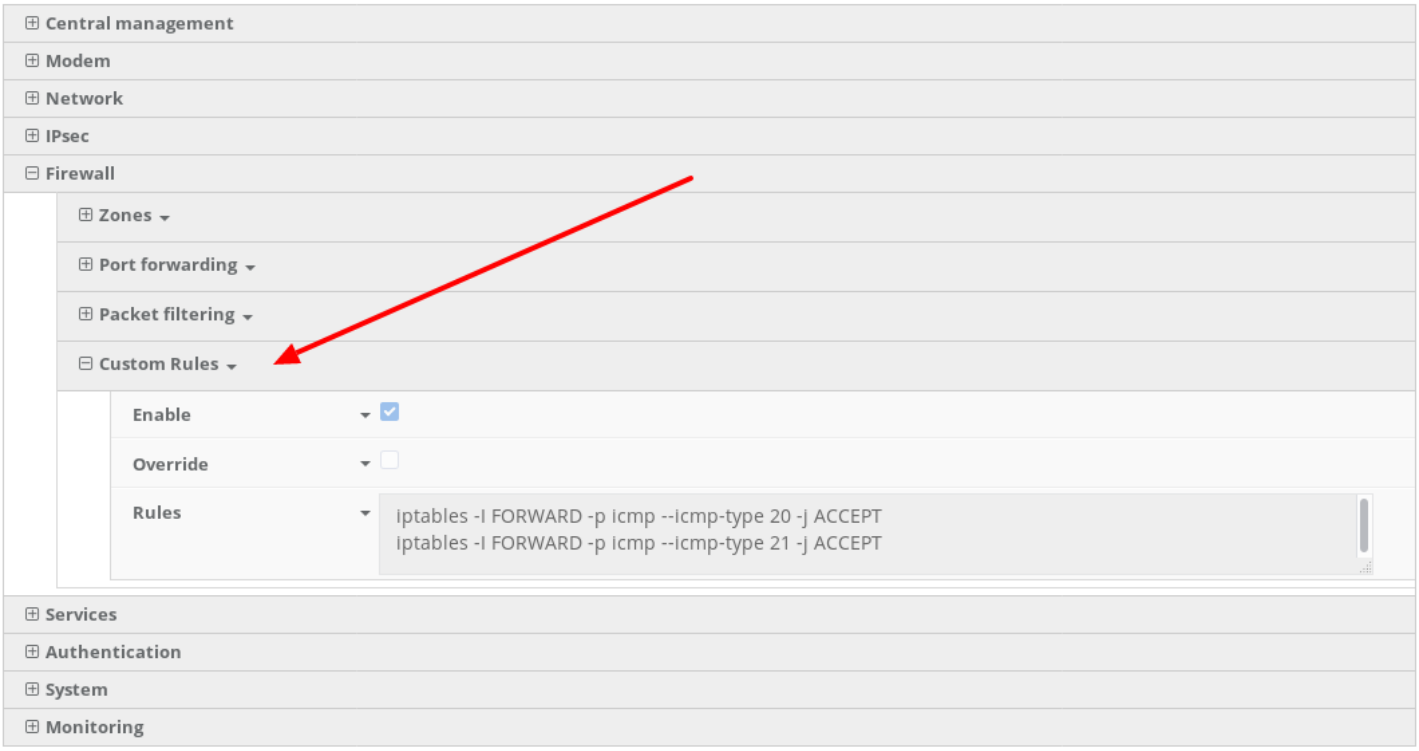
The Proactive Monitoring feature of the AT&T VPN Gateway performs a connectivity test on its WAN2 backup connection. This connectivity test employs a unique type of ICMP packet with type 20 outbound, and the response ICMP packet is of type 21. Since this is a non-standard ICMP packet, the 63xx-series router's firewall drops the packet, which results in the AT&T VPN Gateway failing its Proactive Monitoring test.

Solution

The firewall of the 63xx-series router must be updated to allow the unique ICMP packets through the cellular connection. To implement this solution, update the configuration profile of the Accelerated 63xx-series router with the following configuration changes:

1. Select the *Firewall -> Custom rules -> Enable* checkbox
2. Enter the following two firewall rules into the *Firewall -> Custom rules -> Rules* option:

```
iptables -I FORWARD -p icmp --icmp-type 20 -j ACCEPT
iptables -I FORWARD -p icmp --icmp-type 21 -j ACCEPT
```


Central management
Modem
Network
IPsec
Firewall
Zones
Port forwarding
Packet filtering
Custom Rules
Enable
Override
Rules
iptables -I FORWARD -p icmp --icmp-type 20 -j ACCEPT
iptables -I FORWARD -p icmp --icmp-type 21 -j ACCEPT
Services
Authentication
System
Monitoring

Upgrading Modem Firmware

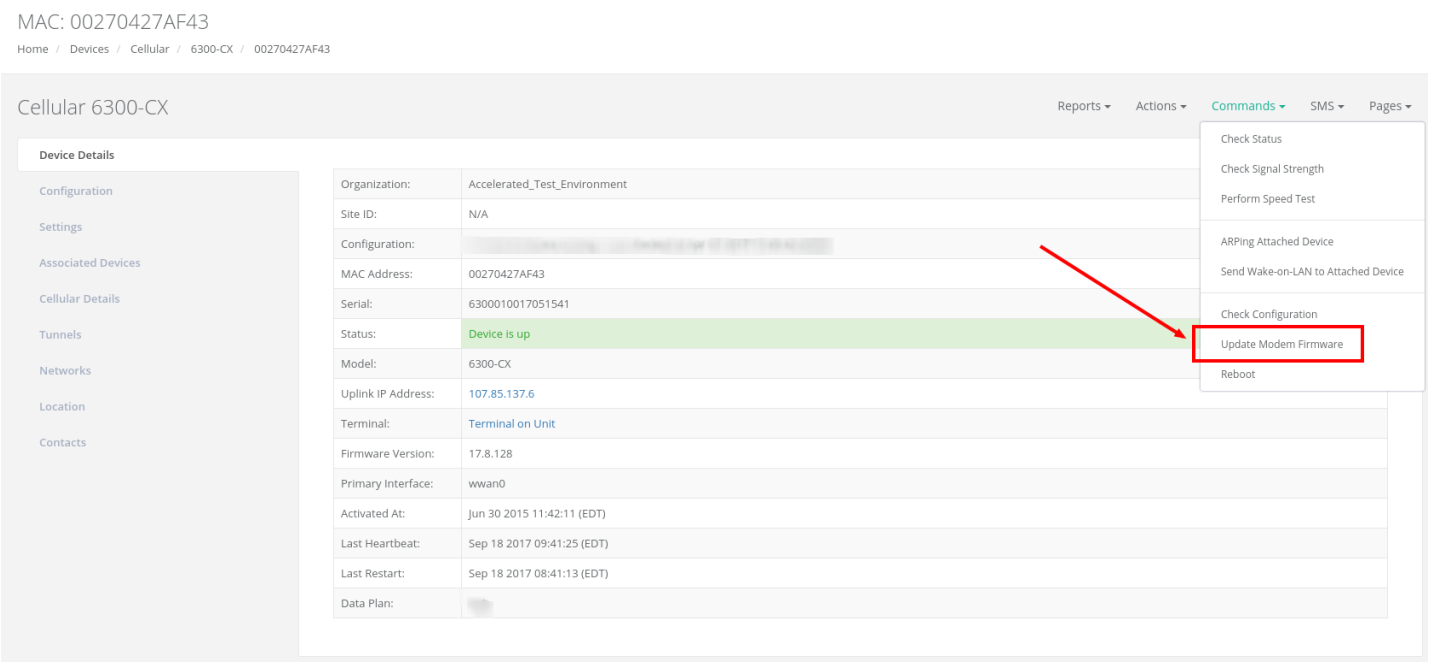
There are several options for upgrading the firmware on the modem inside your 63xx-series router. Users can upgrade the firmware on this modem either through the Accelerated View portal or the local web UI of the 63xx-series router, depending on the level of access and network connectivity the LTE router has and how the user has chosen to manage their devices.

OTA Update using Accelerated View

Upgrading the modem firmware using either of the options below requires the device to be online and in sync with Accelerated View.

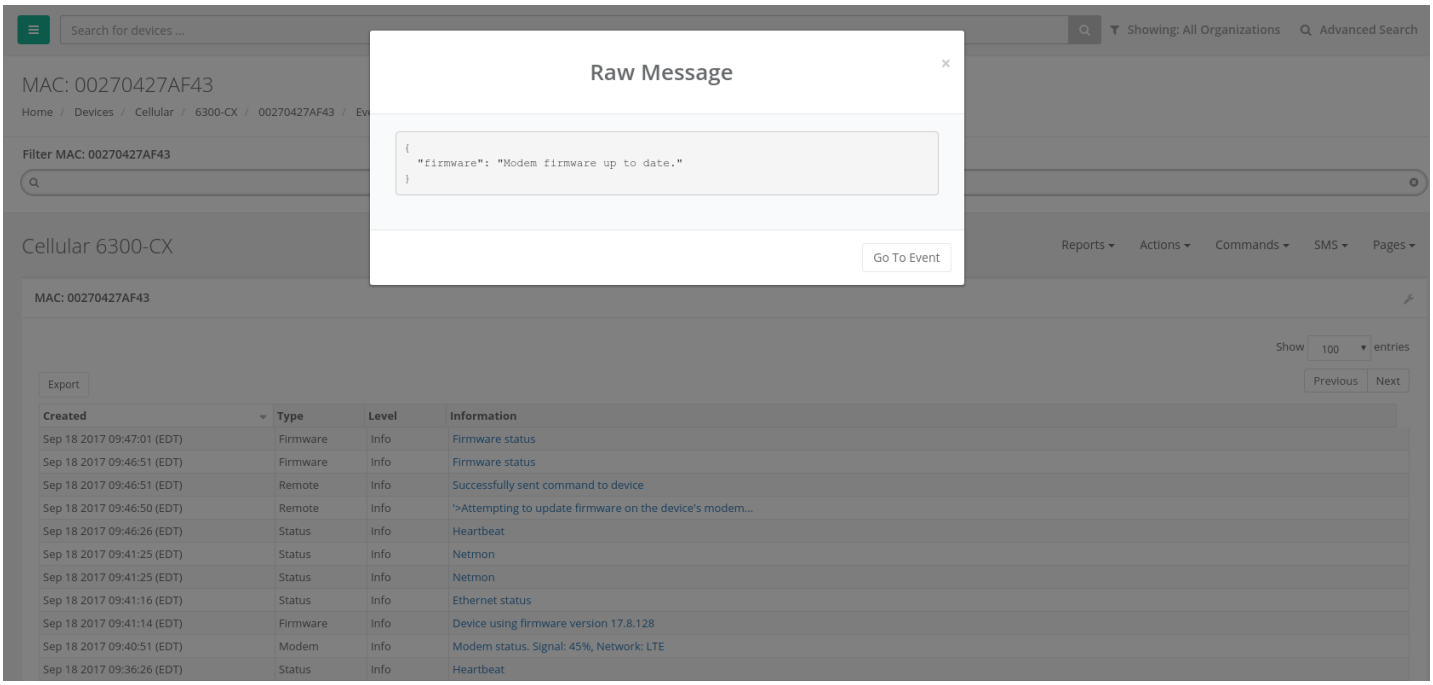
Option 1 - OTA command

If the 63xx-series router is on firmware version 17.8.128 or higher, users can send the ***Update Modem Firmware*** command from Accelerated View. Details on how to send a remote command from Accelerated View to a 63xx-series router can be found here.



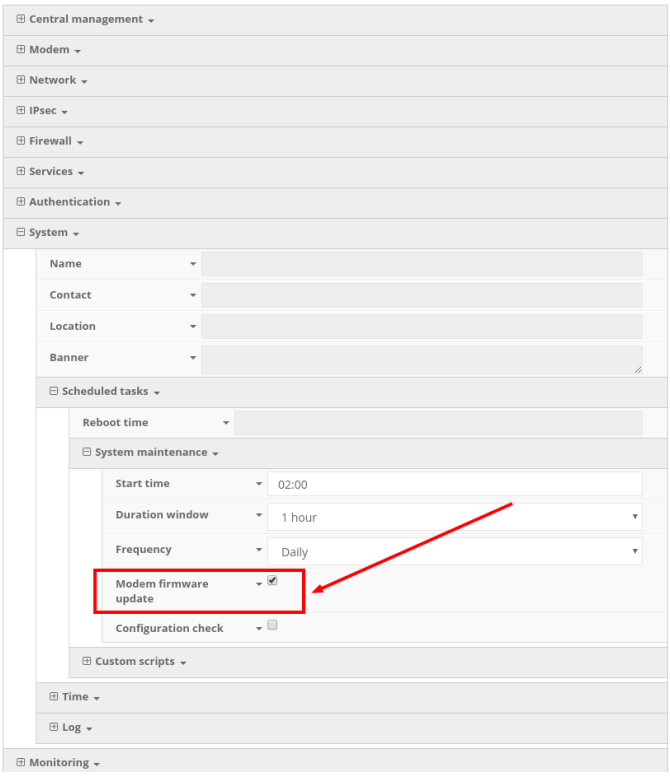
This command will trigger the 63xx-series router to query the Accelerated firmware server. If a newer modem firmware version is found for the current carrier-specific firmware used on the modem in the 63xx-series router, the 63xx-series router will automatically download the new firmware and flash it onto the modem.

If no new firmware is found, the 63xx-series router will send an event to Accelerated View stating that the modem firmware is up to date.



Option 2 - Scheduled OTA check/update

If the 63xx-series router is on firmware version 17.8.128 or higher, users can configure the router to check for modem firmware updates at a scheduled interval. This option is found under the *System -> Scheduled tasks -> System maintenance* section of the 63xx-series router's configuration profile. Details on configuring your 63xx-series router using Accelerated View can be found here.



Once the *Modem firmware update* scheduled task is enabled, the 63xx-series router will query the Accelerated firmware server at the specified timeframe. If a newer modem firmware version is found for the current carrier-specific firmware used on the modem in the 63xx-series router, the 63xx-series router will automatically download the new firmware and flash it onto the modem.

Manual Upgrade using the Local Web UI

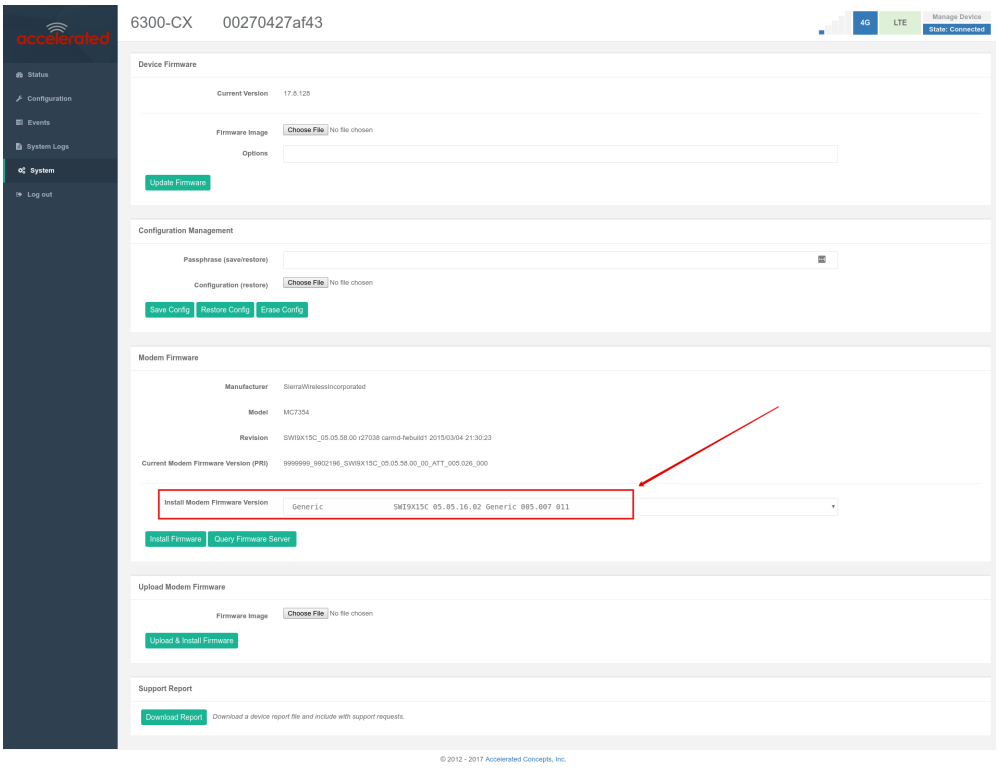
Upgrading the modem firmware using any of the following options requires the user to directly access the web UI of the 63xx-series router.

Option 1 - Select from pre-loaded firmware list

The Category 3 series of cellular modems have smaller firmwares that our 63xx-series routers have pre-loaded inside their flash memory. Users can update the modem in their 63xx-series router to one of these pre-loaded firmwares using the following steps:

1. Login to the web UI of the 63xx-series router.
2. Click on the *System* link on the left navigation bar of the site.
3. Under the *Modem firmware* section of the page, click the drop-down next to *Install Modem Firmware Version* and select the desired carrier firmware.

4. Click *Install Firmware*. A progress bar will appear indicating the status of the modem's firmware upgrade. Once the upgrade completes, the 63xx-series router will automatically reconnect to the cellular network.



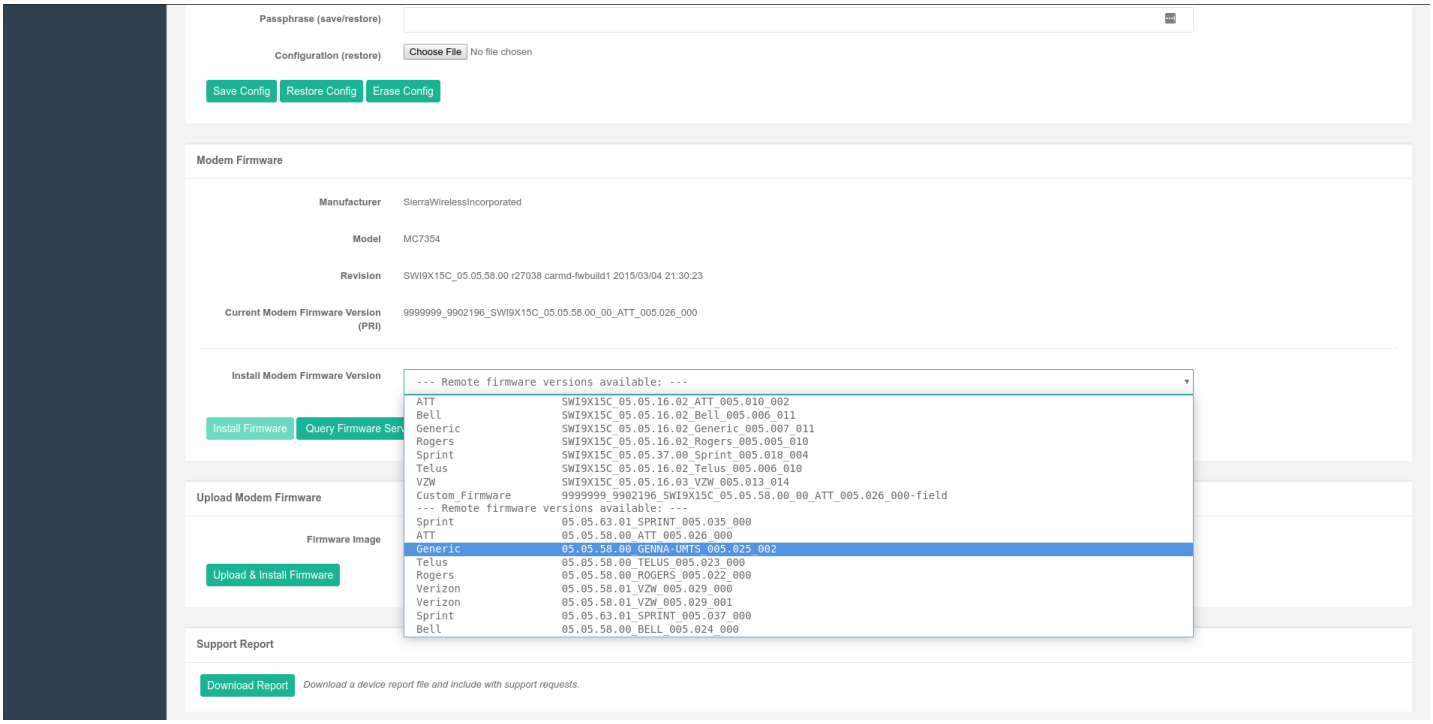
Option 2 - Query Firmware Server

If the desired modem firmware version is not listed in the pre-loaded firmware drop-down mentioned in option 1 above, users can query the Accelerated firmware server for additional firmwares for the modem inside the 63xx-seris router.

> Note, your 63xx-series router must be online and have access to the Accelerated firmware.accns.com server in order for this query to work. As part of this process, the 63xx-series router will download the new firmware file over the Internet (approximately 30-60MB) and onto the device.

To perform this query and upgrade the firmware on the modem:

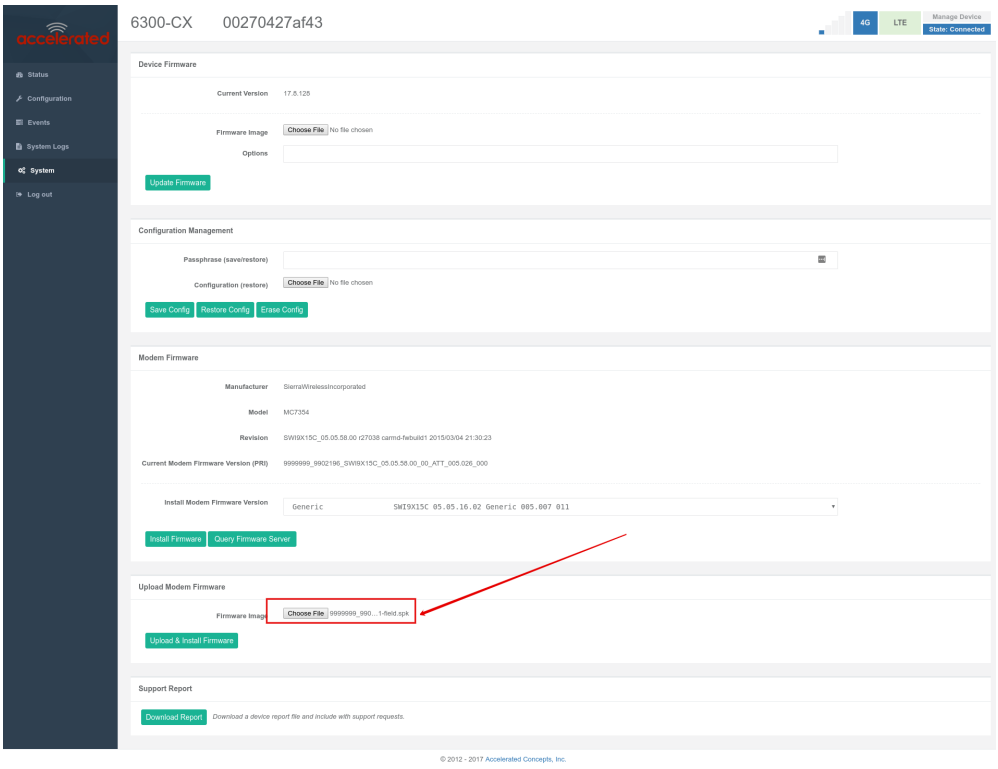
1. Click on the *Query Firmware Server* button.
2. Once the query completes, the drop-down will list the available remote firmware versions.
3. Select the desired firmware version from the list
4. Click the *Install Firmware* button. A progress bar will appear indicating the status of the modem's firmware upgrade. Once the upgrade completes, the 63xx-series router will automatically reconnect to the cellular network.



Option 3 - Manual Firmware Upload

Some vendors supply direct firmware images for their cellular modems. If you have a specific firmware file you would like to apply to the modem, you can use the *Upload Modem Firmware* section on the 63xx-series router's *System* web UI page to upload the firmware onto the modem. To manually upload a firmware file onto the modem inside a 63xx-series router:

1. Select the *Choose File* button under the *Upload Modem Firmware* section.
2. Select the desired firmware file from your file system.
3. Click *Upload & Install Firmware*. A progress bar will appear indicating the status of the modem's firmware upgrade. Once the upgrade completes, the 63xx-series router will automatically reconnect to the cellular network.


6300-CX 00270427af43
4G LTE
Manage Device
State: Connected
Status
Configuration
Events
System Logs
System
Log out
Device Firmware
Current Version 17.8.126
Firmware Image Choose File No file chosen
Options
Update Firmware
Configuration Management
Passphrase (save/restore)
Configuration (restore) Choose File No file chosen
Save Config
Restore Config
Erase Config
Modem Firmware
Manufacturer SierraWirelessIncorporated
Model MC7354
Revision SWI9X15C_05.05.58.00 r27038 carmd-fwbuild1 2015/03/04 21:30:23
Current Modem Firmware Version (PRI) 9999999_9902196_SWI9X15C_05.05.58.00_00_ATT_005.026_000
Install Modem Firmware Version Generic SWI9X15C 05.05.16.02 Generic 005.007 011
Install Firmware
Query Firmware Server
Upload Modem Firmware
Firmware Image Choose File 9999999_990...1-field.spk
Upload & Install Firmware
Support Report
Download Report
Download a device report file and include with support requests.
© 2012 - 2017 Accelerated Concepts, Inc.

Updating Firmware

Using Accelerated View

1. Log in to Accelerated View and use the **Search** tool to find the device by searching for its **MAC address**.
2. Select the MAC address of the device to bring up its **details** page.
3. Click on the **Configuration** tab, then select the **Edit Configuration** link in the **Group Configuration** section of the page.
4. Select the appropriate firmware version from the **Firmware** drop-down list.
5. Click the **Update** button.
6. All devices associated with that configuration profile will upgrade to the new firmware the next time the device syncs with Accelerated View (by default, once every 24 hours around 1AM UTC). If you want to apply the firmware upgrade immediately, please perform the following:

- Go back to the details page of the router (see steps 1 & 2 above).
- Select the **Commands** drop-down at the top-right of the page.
- Select **Check Configuration** option from the **Commands** drop-down.
- Once the command is received by the router, the device will automatically upgrade to the new firmware and then reboot.

Managing the Device Locally

1. **Download** the firmware file from Accelerated using the provided link:

- **CX**: https://accelerated.com/support/6300_CX/firmware/
- **SR**: https://accelerated.com/support/6350_sr/firmware/
- **MX**: https://accelerated.com/support/6330_mx/firmware/
- **LX**: https://accelerated.com/support/6300_LX/firmware/
- **RM**: https://accelerated.com/support/5400_RM/firmware/

2. **Connect** to the device's **web UI** by connecting your PC to the WAN Ethernet port of the device and then going to http://192.168.210.1. Click here for assistance with local device access.
3. Select the **System** tab on the left side of the page.
4. Select the **Browse** button next to the Firmware image section.
5. Browse for and select the downloaded firmware file.
6. Click the **Update Firmware** button.

Remote Control Tunnel Unresponsive [RESOLVED]

6300-CXs configured for IP Passthrough lose access to Remote Commands on 17.8 firmware

Available Workaround: Downgrade to 17.5 (available for download here)

Firmware Fix: 17.8.128.63 - November 9, 2017

RESOLUTION: Remote commands are once again available to devices provisioned for IP passthrough on firmware version *17.8.128.63 or later*. Upon upgrading firmware, please give the remote control tunnel 10 to 20 minutes to rebuild itself.

Antenna Terminology

Electronics require antennas to convert data into RF signals (and vice versa). They are coupled with radio transmitters and/or receivers to process the information that is carried over cellular bands. Antenna design and functionality has evolved over time:

Internal Antennas: An antenna can be concealed within the casing of a device, as seen with most smart phones. Internal antennas are potentially more prone to interference due to the close grouping of electrical components.

External Antennas: Situating antennas further away from the rest of the circuit board can help alleviate this problem by maximizing a device's natural reach. Instead of sitting inside the device directly next to the modem or transceiver, they screw into place using SMA connectors and protrude from the equipment (think "rabbit ears").

MIMO: Multiple-Input and Multiple-Output (MIMO) technology expands the throughput capacity of a transceiver by leveraging multiple antennas to simultaneously convert RF signals into data (or vice versa), providing faster transfer speeds as a result. Think of it (loosely) as Carrier Aggregation for antennas -- once again combining individual lanes into a single, coordinated superhighway. Networks must leverage MIMO antenna transmission to be technically considered 4G.

Physical Specifications

Accelerated LTE Routers use industry-standard, female SMA connectors to affix antennas to the internal cellular radio. External antennas improve clarity when compared to internal antennas, which are prone to electromagnetic interference. An extension coaxial cable can also enhance

the reach of a device; however, that cabling causes **attenuation** -- or a degradation in signal quality -- due to the distance the signal travels. Significant attenuation typically begins at 30 feet of cabling.

Certain Accelerated products, e.g. the 6300-CX and 6330-MX LTE Routers, are designed to provide the ability to place the cellular router where reception is best (moving the "radio" is always preferred). This allows the device to "capture" optimal Radio Frequency (RF) before converting it to IP packets and transmit data via Ethernet cabling, an approach that yields increased performance and cost savings over coax cabling. Accelerated can also provide a battery pack for site surveys, creative mounting options, and a (passive) Power-over-Ethernet injector to provide an efficient, flexible deployment at the lowest possible cost. Most Accelerated clients will not require third-party antennas unless deploying a more traditional LTE router (without PoE). It is always preferred to mount a PoE router on an external wall via Ethernet and use the shortest coax cable required to run the external antenna to the outside of a building.

CRITICAL NOTE: Please test the signal strength outside of the building to ensure you have cellular coverage in the area prior to any cabling work. (Tip: Use the site survey battery to do this.)

Best Practices for PoE Deployments

Most LTE specifications recommend (or even require) the use of dual antennas for a MIMO configuration. Many antennas include a MIMO configuration in a single antenna housing, which can be confirmed if there are two cellular coax connections running from the housing. A single-housing MIMO antenna would also require the use of dual coax extension cables. If you select a non-MIMO antenna it is recommended that two separate antennas are used, though this configuration doubles the cost of the antenna unit itself as well as the coax extension cabling. It is typically recommended to include some "separation" when mounting antennas to prevent interference (the antenna manufacturer may provide a recommendation but 18 to 24 inches should be sufficient).

Please consider the following when mounting your PoE LTE Router or third-party antennas:

1. Maximize Ethernet vs. coax extensions (e.g. inside vs. outside the building)
2. Avoid mounting inside metal enclosures or even near large metal objects
3. Within reason, maximize the distance from any other electronic equipment
4. Mount the device near an exterior wall or window (or run the antenna outdoors)
5. If possible, mount to the ceiling vs. the wall (the wall can introduce interference)
6. Generally mounting higher is better (but consider future serviceability)
7. Try to always use a MIMO antenna solution for the best results / RF performance

Accelerated has tested the following antenna solutions for performance and compatibility purposes. Please use this information as a reference to assist in determining the right antenna solution for your specific use case. It is important to test the antennas you select in your specific application environment (meaning your deployment site).

Please note that a booster, repeater, or amplifier may be another strategy to improve RF sensitivity. However, these technologies can also introduce issues because they may "amplify" bad signal. The focus of this chapter is on antennas but more information on boosters can be found on-line.

Antennas Tested by Accelerated

PLEASE NOTE: The below information has been compiled by Accelerated to assist clients in finding and sourcing an antenna solution to best meet their application and business needs. The information on availability and pricing is for planning purposes only and may vary. Clients should test and validate their own applications prior to selecting an antenna for their project.

These antennas are "Omni-Directional" or offer the ability to send/receive signals from any direction. Directional antennas may improve RF sensitivity, but they will require an expert knowledge to find a specific cellular tower and maintain the ongoing fine-tuning that may be required to keep the antenna positioned properly. Due to the challenges of directional antennas, Accelerated typically focuses on *MIMO omni-directional models*.

Extra-Small IoT "Paddle" Antennas

Manufacturer: Taoglas Antennas Solutions

Product: TG.08.0113 and the Product Datasheet

Sample Retailers: Accelerated; Digi-Key; Mouser; Tessco

MSRP: $12 per antenna ($24 for a pair)

NOTE: Use of 2 antennas is recommend for full MIMO Operation

Deployment Notes:

This is an antenna recommended for consideration when a project requires antennas with a small form factor (e.g. digital signage, small enclosures, rack mounted, in-vehicle, etc). The

performance of these antennas is surprisingly good considering the size. Although testing has shown they may slightly underperform compared to the antennas included with your Accelerated router, these smaller may provide the perfect balance between form factor and performance in your IoT application.

Large External MIMO Antenna (Outdoor Rated)

Manufacturer: EAD

Product: LMO7270 and the Product Datasheet

Sample Retailers: Accelerated

MSRP: $129 with dual 5M coax cabling (sold for use with Accelerated Routers)

Deployment Notes:

This is a hardened antenna designed to be mounted outdoors. This is a MIMO antenna with two short “pig tail” connectors and the overall dimensions are 187 mm in height and 106 mm at the base. Accelerated will typically provide this antenna with a kit including dual coax cables at 5M in length. If you are using this antenna with an Accelerated PoE router (e.g. the 6300-CX LTE Router) we typically recommend you mount the Accelerated router on the inside and run the “short” 5M cables to the outside. Meaning you save costs and eliminate attenuation (signal loss) by running Ethernet as far as possible and minimize the coax cable length. Accelerated testing of this antenna reveals performance gain.

Flat MIMO Antenna #1

Manufacturer: Taoglas Antennas Solutions

Product: Gemini LMA100 and the Product Datasheet

Sample Retailers: Accelerated

MSRP: $99 with dual 5M cables

Deployment Notes:

This is an easy-to-use MIMO antenna. It offers a low-profile form factor that accommodates simple mounting. This model is manufactured by Taoglas and showed solid RF performance in our testing. The antenna has a square shape, sized at 164 mm x 164 mm x 36.5 mm. The antenna cabling is built into the antenna, and typically reaches only one meter, but it can be built (sized) to order (lead time can take up to 8 weeks). This antenna typically includes a stand that can be used instead of mounting. The pricing above is based on 5M cables (~15 feet) and the antenna is rated for indoor and outdoor use.

Flat MIMO Antenna #2

Manufacturer: Mobile Mark

Product: PNM2-LTE and the Product Datasheet

Sample Retailers: Sold through Distribution

MSRP: PNM2-LTE-1C1C-WHT-180 (includes Cabling @ 15 feet) $176.40

Deployment Notes:

This is an additional easy-to-use MIMO antenna with a low-profile form factor and simple mounting. This model is manufactured by Mobile Mark and showed solid RF performance in our testing. With a square form factor of 146 mm x 146 mm x 18 mm, the antenna cabling is built into the antenna and can be sized to order (typically lead time from the manufacturer is 2 weeks).

Paddle Extender

Built for Accelerated

Product SKU:

Sample Retailers: Sold through Accelerated

Deployment Notes:

This unique product (termed "the paddle extender") is designed to “move” the standard LTE router antennas to a more optimal spot to obtain better RF connectivity. A typical use can may be where the router is installed in a metal enclosure or rack (think of a data center or digital signage enclosure). The “paddle antennas” can be mounted to the top SMA connector, escaping the limitations of having to stay affixed to the device's chassis. Remote mounting is then simplified thanks to the paddle extender's magnetic base (diameter of 48mm [1.9 inches]). The length of the cable 50cm (19.7 inches).