Configuration for Fortinet FortiGate Series

6300-CX

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.

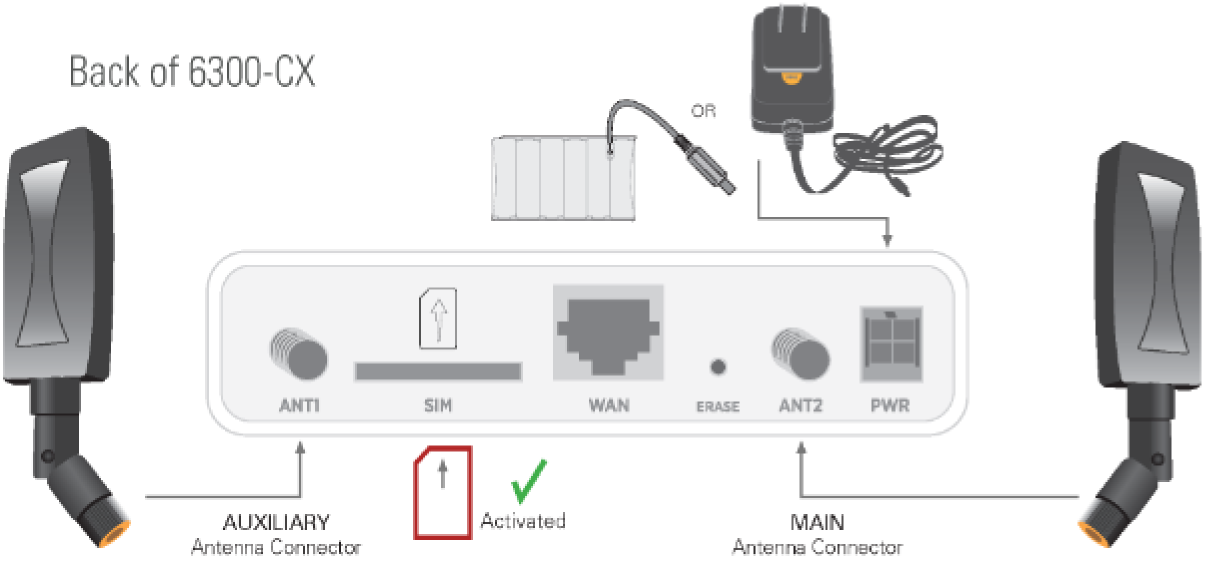
Using the 6300-CX as a secondary connection assumes that a primary WAN Ethernet cable is plugged into port WAN 1 on the Fortinet device. Connect the 6300-CX's backup Ethernet cable to port labeled WAN 2 and proceed to the configuration described herein. (Compatible with all FortiGate Series Firewalls.)

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. <!--[if !vml]-->
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

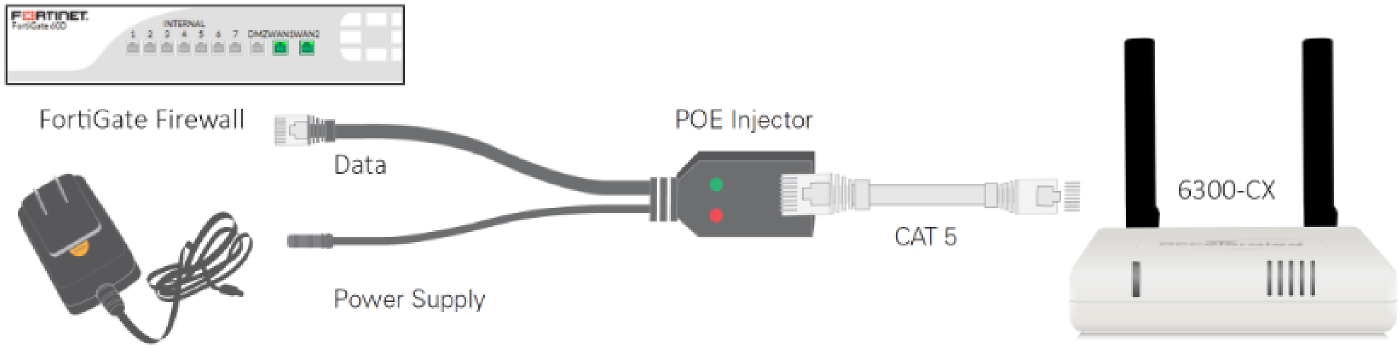
1. After following steps 1 and 2 in the “Initial Setup” section, connect the battery pack to temporarily power the Accelerated 6300-CX. The charge lasts two to four hours – it is not rechargeable and should be properly disposed of after use.
2. Move the 6300-CX to different locations within your site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

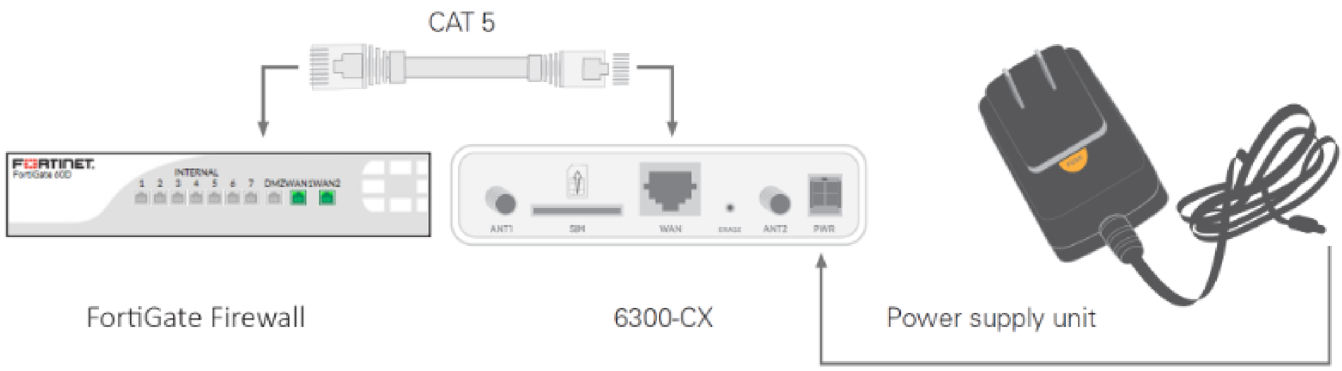


Direct Power Installation – Powering Option #2

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

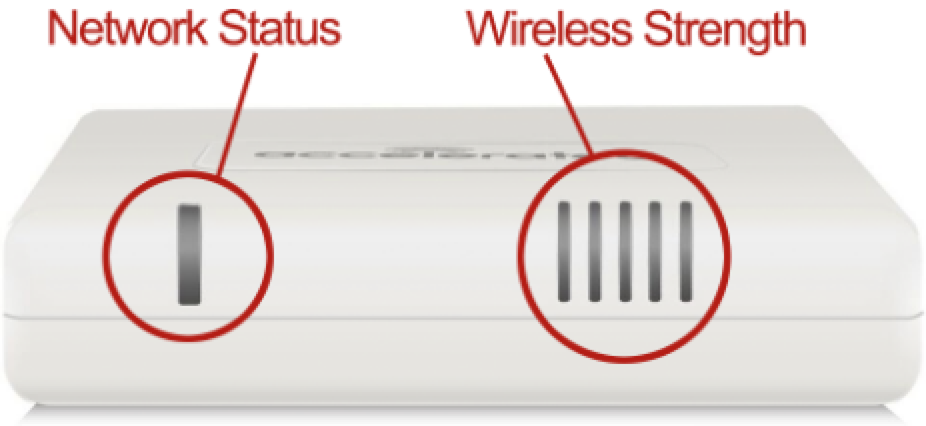
1. Use an Ethernet cable to connect the 6300-CX to the security appliance using port wan1 (to use the cellular network as the primary connection) or port wan2 (to configure a failover).
2. Plug the 6300-CX power supply unit (PSU) into an AC power outlet.
3. Connect the PSU into the 4-pin power connector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

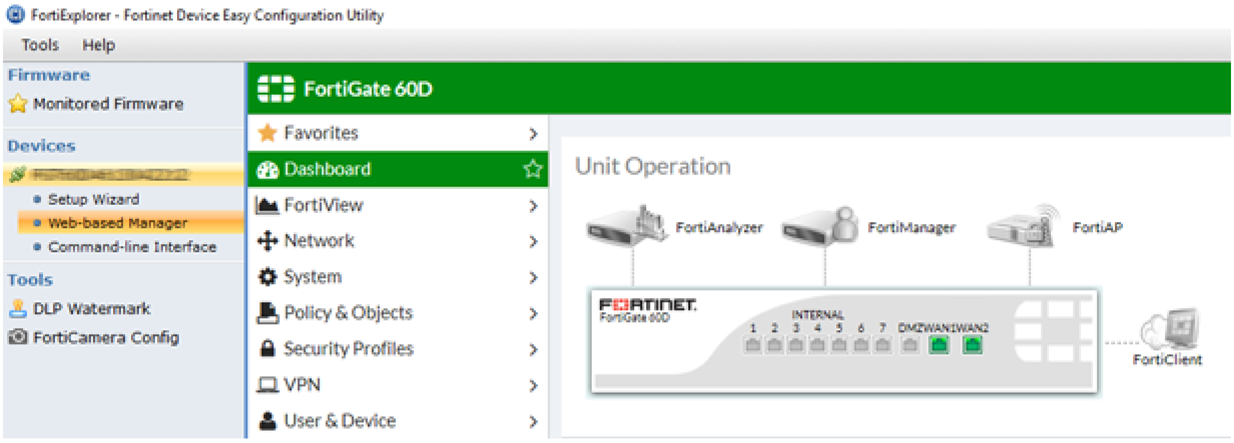
Signal Bars	Weighted dBm	Signal Strength %	Quality
▮	-113 to -99	0 - 23%	Bad
▮▮	-98 to -87	24 - 42%	Marginal
▮▮▮	-86 to -76	43 - 61%	OK
▮▮▮▮	-75 to -64	62 - 80%	Good
▮▮▮▮▮	-63 to -51	81 - 100%	Excellent

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.

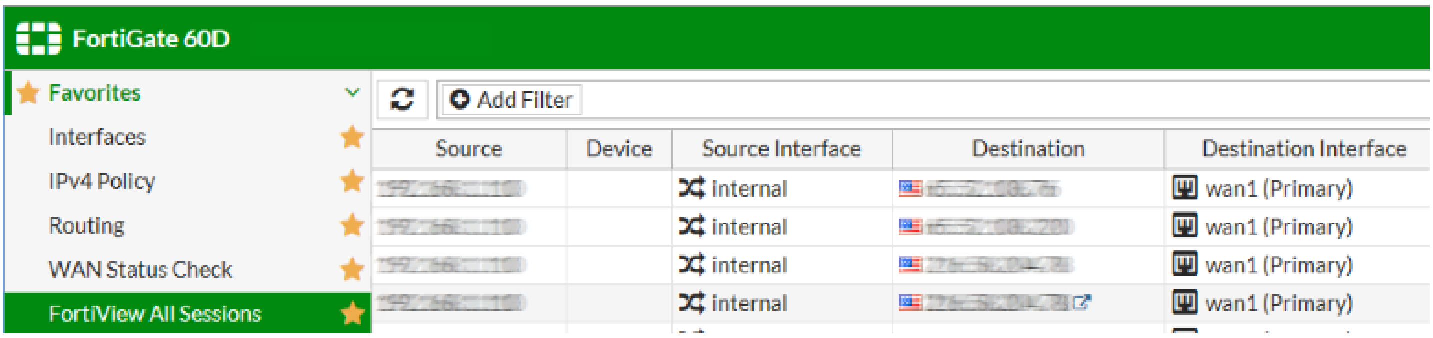
For an in-depth walkthrough of how to manage your FortiGate device, please refer to Fortinet's [FortiOS Handbook](#).

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.



Source	Device	Source Interface	Destination	Destination Interface
[redacted]		Internal	[redacted]	wan1 (Primary)
[redacted]		internal	[redacted]	wan1 (Primary)
[redacted]		internal	[redacted]	wan1 (Primary)
[redacted]		internal	[redacted]	wan1 (Primary)

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.