Quick Start Guide
Forcepoint V10000 G4
TRITON RiskVision Appliance

⚠️ Before you begin...

Plan your deployment before setting up the appliance. See the **Setup Guide** for more information about deployment options.

1 Verify Contents

1 Accessory Kit

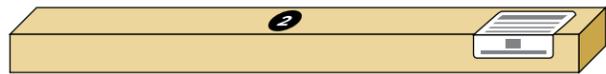Power Cables (2)   Ethernet Cables (2)   Serial Cable

Bezel (faceplate)

2 Sliding Ready Rail Kit

- Left Ready Rail
- Right Ready Rail
- Velcro Straps (2)
- Rack Installation Instructions

3 Cable Management Arm Kit

- Cable Management Arm
- Static Support Tray
- Status Indicator Cable
- Cable Tie Wraps
- CMA Installation Instructions

Contact Forcepoint Technical Support if any items are missing.

2 Rack Appliance

See the ***Rack Installation Instructions*** included in the Sliding Ready Rail kit.

3 Connect Network Cables

Connect the appliance interfaces. Cat 5E cables (or better) are required. Do not use crossover network cables.

Required Ports: C   N

Interface	Function
C	• Enables Local Manager communication • Used for subscription verification, analytic and category database downloads, product updates, and sending feedback • Used for communication with cloud-based components, including the File Sandbox
N	• Capture port, used to monitor network traffic • Connect to a port mirror or network tap

4 Power On Appliance

Secure power cables using velcro straps and plug power cables into an appropriate power source.

Power on the appliance and check the following indicators:

Front
- Power button is illuminated.
- Hard drive LEDs are green.

Rear
- Power supply LEDs are green.
- LEDs for connected interfaces (NICs) are green.
- System status indicator (LED left of power supplies) is solid blue.

Contact Forcepoint Technical Support if any indicators are not illuminated correctly.

5 Installation Overview

Refer to the TRITON RiskVision **Setup Guide** for complete installation instructions.

1. Connect a keyboard and mouse to the appliance. (You can alternatively cable the appliance iDRAC interface, then connect to the appliance iDRAC via a web browser.)

2. Log in as **root** with password **websense123**, then create a new root password when prompted.

3. The installation process attempts to acquire an IP address for the C interface via DHCP.
   - If DHCP is enabled in your network, use the **ifconfig** command to find the IP address assigned to **eth0**.
   - If DHCP is not enabled in your network, use the **system-config-network** command to assign an IP address to **eth0**, then use the **service network restart** command to restart your network interfaces.

     After setting the IP address, use the **/opt/websense/ rvadmin.sh restart** command to restart all of the RiskVision services.

4. Use the **timezone** command to update system time settings on the appliance.

5. From another machine, use Firefox or Chrome to log in to the RiskVision Local Manager as **admin** (password **admin**):

   https://<c_interface_ip_address>:8443

6. To change the admin password, select **admin** in the tool bar at the top of the page, then click **Change Password**.
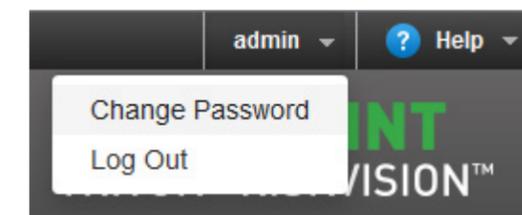
   Enter and confirm a new password when prompted.

7. Follow the steps in the **Setup Guide** to finish configuring RiskVision and start analyzing traffic.