FORCEPOINT
POWERED BY Raytheon

Getting Started

X-Series™ Modular Chassis Family X10G™

v8.2.x

Published 2016 Revision C
Printed in the United States and Ireland

R042816820

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

Every effort has been made to ensure the accuracy of this manual. However, Forcepoint LLC, makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint LLC shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Forcepoint is a registered trademark and TRITON is a trademark of Forcepoint LLC, in the United States and certain international markets. Forcepoint has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Windows, Windows NT, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Mozilla and Firefox are registered trademarks of the Mozilla Foundation in the United States and/or other countries.

eDirectory and Novell Directory Services are a registered trademarks of Novell, Inc., in the U.S and other countries.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries. Linux is a trademark of Linus Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (http://www.apache.org).
Copyright (c) 2000. The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Contents

1 Hardware Setup for the X-Series Modular Chassis

The X-Series™ modular chassis is a high-performance network security system that consists of:

- **X10G™ blade chassis**: The chassis is an energy-efficient blade enclosure from Dell™ that holds up to 16 security blades optimized for TRITON AP-WEB and TRITON AP-EMAIL (installed on separate security blades).
- **X10G security blades**: These Dell blade servers are equipped with a hardened operating system and TRITON web or email protection software.

The following illustration shows a back view (left) and front view of the Dell chassis, with on-chassis switches enlarged (at lower left) and security blades (at lower right).

Receiving and racking the hardware

The chassis and security blade hardware are manufactured by Dell. All blades are accessible through a web-based Dell Integrated Remote Access Controller (iDRAC). Blades run optimized security software provided by Forcepoint LLC.

Unloading at your shipping dock

The chassis can weigh up to 400 pounds (182 kilograms) with all hardware components loaded. It is shipped with pre-installed cooling fans, 4 power supply units, 2 switches, and 1 Chassis Management Controller (CMC).

Security blades are typically shipped separately. Insert the security blades *after* racking the chassis.

You need a loading dock to receive the chassis, or a delivery vehicle with a lift gate. Dell recommends having 4 people available to lift the chassis into the rack in your computer room.

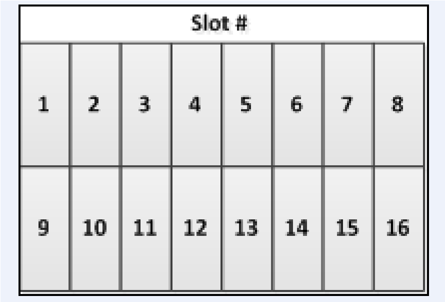
- Unpack and rack the chassis before you insert the security blades. Save the handled cardboard lifter, if a future chassis move is likely.
- Security blades are packaged separately. After installation, blades are imaged with the TRITON software you ordered as described later in this guide.
- A few TRITON components are Windows-only and must be installed and run off the chassis. The installer for these components is named **TRITON82xSetup.exe**. This installer is located on the Downloads page at www.forcepoint.com.

X10G Quick Start poster

The **X10G Quick Start Poster**, included in the chassis shipping box and also available on Forcepoint.com here, shows all items included in each X-Series chassis shipment. The Quick Start poster shows how to set up the hardware and how to connect cables to the X10G chassis and to your network.

Security blade slots

Blade slots across the top half of the chassis front are numbered from 1 to 8, beginning at the left as viewed from the front. Bottom slot numbers begin with slot 9 at the left, ending at slot 16.



Slot #							
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16

- **Slot 1**: After racking the chassis, insert the first blade into slot 1. Ensure that any blade inserted into an upper slot is engaged on the hanging rail just inside the top of the slot. When properly engaged, the blade slides easily into the slot. Do not force a blade into a slot. The metal flap covering the backplane in each slot retracts automatically when the blade is inserted.
- **Slots 2 through 16:** Insert blades into consecutive slots, with no empty slots between blades.

iDRAC and interface IP address planning

The Chassis Management Controller (CMC) must be assigned an IP address so that you can communicate with the chassis. This gives you web-based access to the CMC, as shown in this section.

You may need to reserve as many as 51 IP addresses for communication with a single X10G chassis and all of its blade servers.

Most sites use a pattern similar to this: **`xxx.xxx.xxx.100`** for the IP address of the CMC; **`xxx.xxx.xxx.101`** for the Integrated DELL Remote Access console (iDRAC) for the blade in slot 1; **`xxx.xxx.xxx.102`** for the iDRAC of the blade in slot 2; and so on. After the CMC has an IP address assigned, you use a web interface to assign iDRAC IP addresses to all 16 slots as a range. All slots (even empty ones) will have an iDRAC address.

Chassis location	IP address example
CMC	`xxx.xxx.xxx.100`
Slot 1 Integrated Dell Remote Access Console (iDRAC)	`xxx.xxx.xxx.101`

Chassis location	IP address example
Slot 2 iDRAC	`xxx.xxx.xxx.102`.
Slot 3 iDRAC	`xxx.xxx.xxx.103`
Slot 4 iDRAC	`xxx.xxx.xxx.104`
Slot 5 iDRAC	`xxx.xxx.xxx.105`
Slots 6 through 15	`consecutive IP addresses`
Slot 16 iDRAC	`xxx.xxx.xxx.116`

Plan to have a sequential range of IP addresses reserved for the interfaces you plan to use on every blade server (such as P1 (eth0), and optionally P2 (eth1)).

Here is an example for a fully provisioned X10G:

- IP address of CMC might be: `10.8.0.100`
- IP address range (remote access) for 16 blade iDRACs: `10.8.0.101 - 10.8.0.116`
- Subnet mask: `255.255.0.0`
- Gateway IP address: `10.8.0.1`
- The P1 (eth0) interfaces on the 16 blades might use this IP address range: `10.8.10.201` through `10.8.10.216`
- The optional P2 (eth1) interfaces on the 16 blades might use IP address range: `10.14.0.101` through `10.14.0.116`
- The IP address of on-chassis switch A1 might be: `10.15.0.121`
- The IP address of on-chassis switch A2 might be: `10.15.0.122`

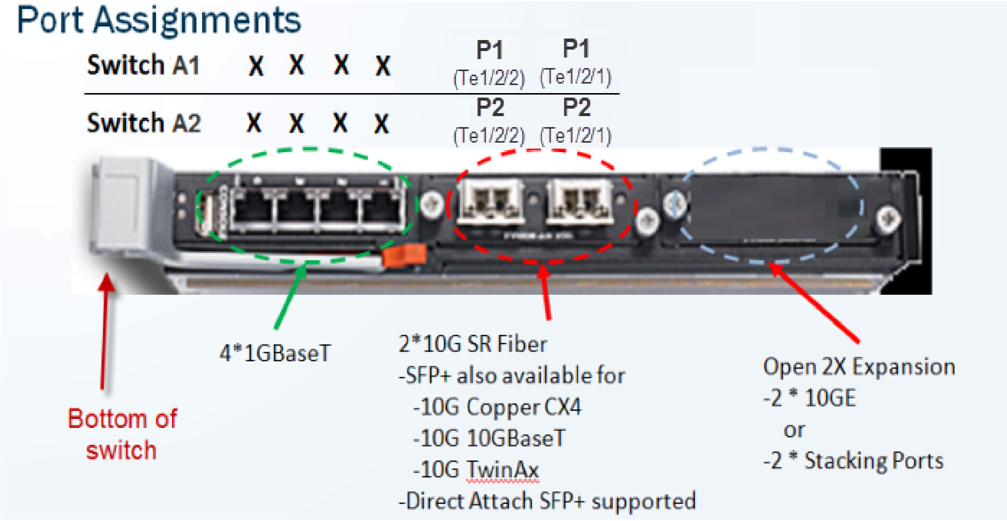
X10G chassis cabling

How you cable the X10G depends on your planned deployment. Cabling and deployment options are discussed in detail in the X-Series Switch Configuration guide. X10G switches can be configured to support VLAN and switch high availability. By default, the switches are not VLAN-aware.

Before finalizing your cable connections, consult with your Forcepoint partner to ensure that your deployment plans are appropriate for your network traffic. See *Big picture* for related deployment topics and links to other deployment materials.

Power cables, Ethernet cables, a serial cable, and SFP+ cables are shipped with the X10G chassis.

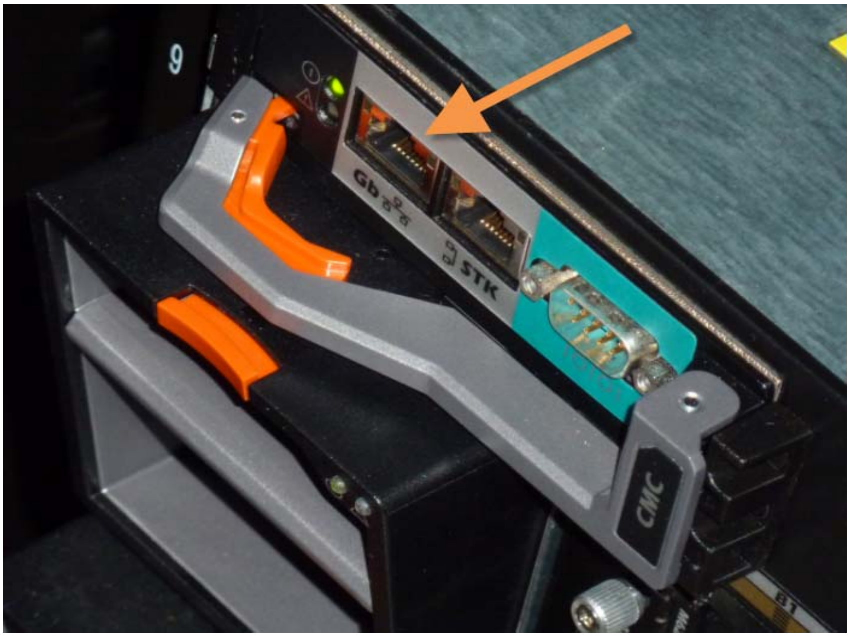
1. Note that the 2 on-chassis switches are oriented vertically at the back of the chassis. The switch on the left side is switch A1. The bottom of the switch is shown at the left in the diagram below. Use an SFP+ cable or install an optical transceiver and use your own fiber optic cable if desired (see details below).



   - Fiber optics: If you ordered an optical transceiver kit with your chassis, see the instructions provided here. This allows you to use fiber optic cables to connect the chassis switches to your network. Begin by connecting the P1 interface on switch A1 to your network. The X10G switch requires an **LC** connector at the end of the optical cable.
   - If you are not using fiber optic cables, no transceiver kit is required. Connect an SFP+ cable (provided) to the P1 interface on switch A1.
   - Note that while several ports may be labeled on both switches, the only port required for deployment is the P1 port on switch A1. The P2 port on switch A2 is optional and dependent upon your network topology. To ensure correct cabling for your deployment, see the X-Series Switch Configuration guide.

2. Next, cable the Chassis Management Controller (CMC). Connect a Category 5 network cable (do not use a crossover cable) from the left-most CMC network port, labeled **Gb** in the illustration, to a switch on the subdomain where the CMC IP address is located.

   The CMC is located at the back of the chassis at the upper left side. Connect the **Gb** port to the network.



- Use the power cables to connect the 4 on-board power supply units (PSUs) at the bottom (back of chassis) to the power outlets on your computer rack. Ensure that the power cables are fully inserted into the PSUs and the power source. Confirm that the power lights are illuminated on the PSUs.

Power on

Power on the chassis at the front (recessed button at the lower left corner below slots 9 and 10). This powers on all blades. Blades can also be turned off and on individually.

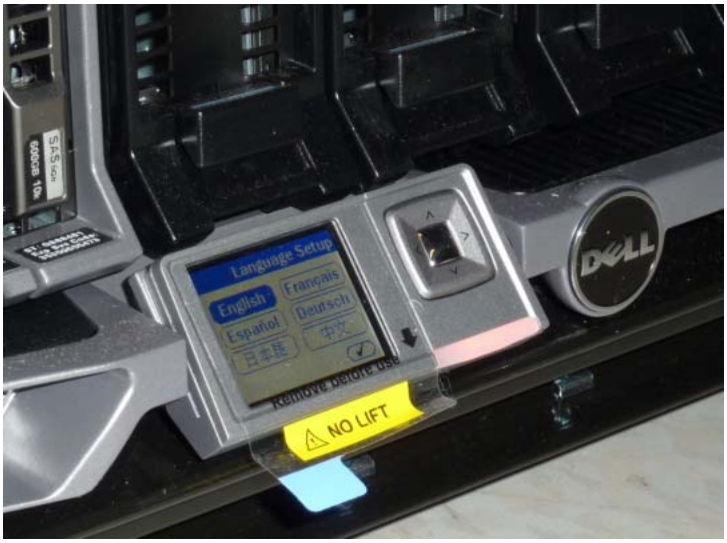
Set up the CMC IP Address

The X10G chassis includes a small, built-in LCD screen at the lower left front.

With the chassis powered on, pull out the LCD screen and use it to:

1. Set your language preference
2. Specify the IP address of the Chassis Management Controller (CMC)

Setting the CMC IP address enables you to communicate with the controller through a browser, from which you can quickly set remote access (iDRAC) addresses for the blades. The following illustration shows the built-in LCD screen and its associated keypad.



Use the silver arrow pad to the right of the LCD screen to move to a selection. Press the center of the silver pad when you are ready to confirm your choice.

After you choose a language, you are ready to configure the CMC.

LCD Prompt	**Recommended response**
Configure CMC?	YES
Set Network Speed	Auto (1Gb)
Specify Protocol Type	IP4 Only
IP Addressing Mode	Static
Enter static IP address of CMC	xxx.xxx.xxx.xxx
Enter subnet mask for this IP address	xxx.xxx.xxx.xxx
Enter default gateway address for this IP address	xxx.xxx.xxx.xxx
Confirm your settings	(Confirm)
Register DNS?	NO (choose X)
Configure iDRACs?	NO (choose X) You will set these from the web interface.
Apply All Enclosure Settings?	YES

Assigning blade slot iDRAC addresses

Move to a laptop and open a browser that has connectivity to the network where the CMC IP address resides.

Point the browser to the IP address you assigned to the CMC:

```
https://CMC_IP_Address
```

Use the user name **root** and the password **calvin** to access the CMC.

This enables you to quickly assign consecutive IP addresses for the iDRACs for all 16 blade servers. You will also change the CMC password.

1. Select **Server Overview** at the left and choose the **Setup** tab.

2. Ensure that the **QuickDeploy** check box is enabled.
3. Set **Starting iDRAC IPv4 Address (Slot 1)** from your chosen IP address range for slot iDRACs. (Check the Netmask and Gateway shown on screen, and change if needed.)
4. Click **Save QuickDeploy Settings**.
5. Scroll down, to locate the button labeled **Auto-Populate Using QuickDeploy Settings**. Click it. Contiguous IP addresses are assigned consecutively to all 16 individual slots for iDRACs.
6. **Click Apply iDRAC Network Settings** at the bottom of the screen
7. In the left navigation, select **Chassis Overview** > **User Authentication**.
8. Select **User ID 1**.
9. Change the password for the CMC and click **Apply**.

2 Deployment Planning for X10G Chassis and Blades

After the X10G hardware is set up and IP addresses are assigned, confirm and implement your decisions about how TRITON components will be allocated across the domains in your network (discussed below).

Ensure optimal coverage for all machines to be managed or monitored, and provide sufficient capacity for the reporting data you wish to retain.

Important

Software modules running on the X10G are at version 8.2.x and are compatible with off-chassis modules at the same version.

Topics include:

Big picture

Every X10G deployment includes one or more chassis, including security blades, and several off-chassis servers that host additional components.

Blade servers

Security blades can host an instance of either TRITON AP-WEB or TRITON AP-EMAIL. A chassis can host a mix of web and email security blades. Blade maintenance may be simplified if blades are physically grouped by function (adjacent slots).

Off-chassis servers

In addition to security blades, a deployment includes at least 3 off-chassis servers.

- A Windows Server (specifications below) to host the TRITON Infrastructure, including the TRITON Manager. TRITON Manager supports configuration and management of your TRITON solutions (discussed below).
- AP-WEB deployments locate several core components on the TRITON management server, or on a separate Windows or Linux server.
- A Windows Server to host the Log servers (web or email, as needed). The Log Server manages the handling of log data with the SQL Server database and with TRITON reporting services.
- A Windows Server to host an instance of Microsoft SQL Server 2008 or 2012. SQL Server supports the TRITON Log Database (discussed below).
- For an email deployment, a Windows mail exchange server

Windows servers must be:

- Windows Server 2008 R2 or R2 SP1 or later, or Windows Server 2012 or 2012 R2 Standard Edition

For detailed specifications of off-chassis servers, see System requirements.

TRITON Manager

The TRITON Manager is the Web-browser-based, graphical management application for your entire deployment. It consists of three modules: Web, Data, and Email. Each module is used to configure and manage its respective features.

Depending on your subscriptions, some or all of these modules will be enabled in your network.

You must install TRITON Manager on a Windows Server 2012 or 2008 R2 (64-bit) machine. TRITON Manager must be able to reach each blade’s P1 interface.

For more information about the TRITON Manager and its modules, see the Forcepoint Technical Library.

TRITON Infrastructure

TRITON Infrastructure is comprised of common user interface, logging, and reporting components required by the TRITON modules.

TRITON Infrastructure also (optionally) includes SQL Server 2008 R2 Express that may be used for logging data. As a best practice, SQL Server 2008 R2 Express should be used only in evaluation environments. Full SQL Server should be used in all production environments.

TRITON Infrastructure services include:

- TRITON Manager
- TRITON Central Access
- TRITON Settings Database
- TRITON Reporting Database (if using SQL Server 2008 R2 Express)

Web module of TRITON Manager

The Web module of TRITON Manager is used to perform general configuration tasks, set up security policies, assign policies to users and groups, run reports, and other management tasks.

Web services include:

- Web Security
- Web Reporting Tools
- Investigative Reports Scheduler
- Reports Information Service
- RTM Client
- RTM Database
- RTM Server

Email module of TRITON Manager

The Email module of TRITON Manager is used to perform general configuration tasks, set up email security policies, assign policies to users and groups, monitor mail queues, run reports, and other management tasks.

The Email module of TRITON Manager also facilitates the following activities:

- Cloud hybrid service registration and synchronization
- Registration with TRITON AP-DATA DLP functions
- Integration with Forcepoint Master Database URL analysis

The console can also be used to configure these Email end-user features:

- Personal Email Manager
- Secure Message Delivery portal

Database management software

Web and email products require Microsoft SQL Server to host the reporting database, called the Log Database. The Web Log Database and the Email Log Database can be hosted by the same database engine instance. Information stored in the Log Database is used to create reports.

Before you install Web or Email Log Server, SQL Server 2008 or 2012 must be *installed and running* on a machine in your network. Note that SQL Server must be obtained separately; it is not included with your subscription. Refer to Microsoft documentation for installation and configuration instructions.

If you do not have SQL Server, you can use the TRITON installer to install SQL Server 2008 R2 Express for evaluations. SQL Server 2008 R2 Express can be installed either on the same machine as TRITON Manager or on a separate machine. See the Deployment and Installation Center for installation instructions.

Note

Use full SQL Server in production environments. SQL Server 2008 R2 Express is appropriate only for non-production, evaluation environments.

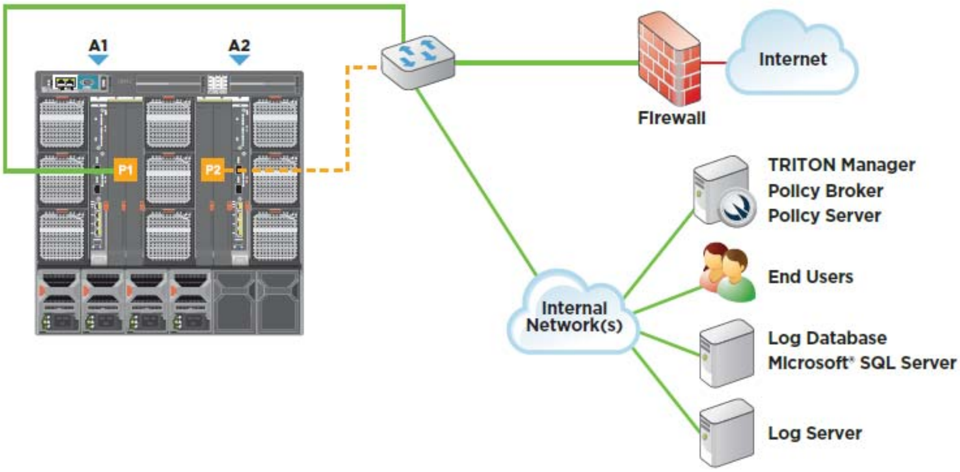
Web protection deployment

Locating the *policy source* in your deployment

One of your earliest deployment decisions is your selection of the *policy source* machine. One security blade or off-chassis server, at your choice, must be chosen and configured to host the Policy Database and Policy Broker for your network. This server is known as the *policy source*.

If the policy source is located off-chassis, you have the option to configure replicated policy source servers. See Managing Policy Broker Replication.

If you use a blade server for the policy source, the best practice is to use the blade in Slot-1. **IMPORTANT**: The policy source server must be installed, configured, and running before you run the *firstboot* script on other blades. In this configuration, policy source replication is not supported.



X10G Network Diagram

What distinguishes your policy source machine is that (in addition to other security components) it runs two TRITON components that do not run on any other server or blade: TRITON **Policy Database** and **Policy Broker**. Although multiple servers can be used for Web security, only a single **Policy Database** holds policy and general configuration data for your organization. Your primary instance of **Policy Server** also runs on the policy source machine.

All machines running TRITON Web protection components need up-to-date policy information obtained from the policy source machine.

Most sites install the policy source on a Windows server (off-chassis). An alternative is to place it onto the blade in Slot-1. The software for remaining blades is easily chosen during each blade's firstboot. Here's how it works:

1. The policy source machine is set up, either off-chassis or the blade in Slot-1. If it is installed on the blade in Slot-1, then during firstboot you select the policy mode *Full policy source*.
2. The remaining blades are set to *User directory and filtering mode* (selected during firstboot) or *Filtering only mode* (selected during firstboot).

User directory and filtering

A **User directory and filtering** appliance is a lightweight version of the policy source machine.

Whenever you make a policy change, that change is immediately updated on the policy source appliance. The change is pushed out to user directory and filtering appliances within 30 seconds.

If the connection with the policy source machine is interrupted, user directory and filtering appliances can continue handling traffic for as long as 14 days. So even if a network connection is poor or is lost, traffic processing continues as expected.

A **User directory and filtering** appliance is configured to point to the *full policy source* for updates.

A **User directory and filtering** blade runs:

- Policy Server
- User Service
- Usage Monitor
- Filtering Service
- Control Service
- Directory Agent
- Content Gateway module (if TRITON AP-WEB is used)

Filtering only

A **Filtering only** appliance is configured to point to a Policy Server. This works best when the appliance is close to the Policy Server and on the same network.

These appliances require a continual connection to the centralized Policy Server, not only to stay current, but also to continue handling traffic. If the connection to the Policy Server becomes unavailable for any reason, traffic on a **Filtering only** appliance can continue to be handled for up to 3 hours.

A **Filtering only** appliance does not run Policy Server. It runs only:

- Filtering Service
- Control Service
- TRITON Content Gateway module (if TRITON AP-WEB is used)

Understanding the Policy Database

TRITON Policy Database stores both policy data (including clients, filters, security components, and delegated administration settings) and global settings configured in the Web module of TRITON Manager. Settings specific to a single Policy Server instance (like its Filtering Service and Network Agent connections) are stored separately.

In multiple Policy Server environments (such as an X10G chassis deployment), a single Policy Database holds policy and general configuration data for all Policy Server instances.

1. At startup, each TRITON component requests applicable configuration information from the Policy Database via the Policy Broker.
2. Running components frequently check for changes to the Policy Database.

3. The Policy Database is updated each time administrators make changes in the Web module of the TRITON Manager and deploy them.
4. After a change to the Policy Database, each component requests and receives the changes that affect its functioning.

Back up the Policy Database on a regular basis to safeguard important configuration and policy information.

- Decide before you configure the X10G where the *policy source* will be located. Best practice is an off-chassis Windows server.
- All security blades must know the IP address of the *policy source* machine.

Your network's size, traffic load, and reporting needs help to determine the optimal allocation of TRITON components in your network.

Software that runs off-chassis

The TRITON components mentioned in this section must be installed off-chassis. Additionally, Microsoft SQL Server 2008 or 2012 must be installed off-chassis.

Use the TRITON installer v8.2.x from the Downloads page at www.forcepoint.com to install any of the components mentioned here. See the Forcepoint Technical Library for more information about components and installation details.

If the X10G will host Web protection solutions, the following Web components should be installed off-chassis. Some are Windows-only components.

- Web Log Server (on its own server)
- Real-Time Monitor
- Sync Service (for sites using the Web Hybrid Module)
- Linking Service (for sites using any integrated TRITON AP-DATA features)
- Transparent identification agents (to apply user, group, or domain [OU] policies without prompting users for credentials)
  - DC Agent
  - Logon Agent
  - eDirectory Agent
  - RADIUS Agent

Table of Web components

Following is a brief description of TRITON Web components.

For component limits and rations, see this article in the Forcepoint Technical Library. Also see the release notes for v8.2.x.

The individual components required for these modes are automatically enabled on the blade when firstboot completes. You do not need to choose components individually.

Component	Description
Policy Database	Stores TRITON software settings and policy information. Installed automatically with Policy Broker. Runs on the *policy source* machine only. Typically installed on Windows server off-chassis.
Policy Broker	Manages requests from TRITON components for policy and general configuration information. Runs on *policy source* machine only. Typically installed on Windows server off-chassis.
Policy Server	Can run on every Web blade. Primary copy runs on *policy source* machine. ● Identifies and tracks the location and status of other TRITON components. ● Stores configuration information specific to a single Policy Server instance. ● Communicates configuration data to Filtering Service, for use in handling Internet requests. Configure Policy Server settings in the Web module of the TRITON Manager. Policy and most configuration settings are shared among all Policy Servers that share a Policy Database.
Filtering Service	Can run on every blade. Provides Internet traffic management in conjunction with Network Agent or a third-party integration product. When a user requests a site, Filtering Service receives the request and determines which policy applies. ● Filtering Service must be running for Internet requests to be handled and logged. ● Each Filtering Service instance downloads its own copy of the Forcepoint Master Database. Configure policy enforcement policies and Filtering Service behavior in the Web module of TRITON Manager.
Network Agent	Is deployed off-chassis. ● Enhances security and logging functions ● Enables non-HTTP and non-HTTPS protocol management
Master Database	● Includes more than 36 million websites, sorted into more than 95 categories and subcategories ● Contains more than 100 non-HTTP protocol definitions for use in managing protocols After all modules are set up, download the TRITON Master Database to activate Internet management, and schedule automatic updates. If the Master Database is more than 2 weeks old, no traffic management occurs.

Component	Description
Web module of TRITON Manager	Runs off-chassis on a Windows server. Serves as the configuration, management, and reporting interface for TRITON software. Use the Web module of TRITON Manager to define and customize Internet access policies, configure TRITON software components, report on Internet activity, and more. The Web module of TRITON Manager is made up of the following services: ● TRITON Web Security ● TRITON Web Reporting Tools ● TRITON Explorer Report Scheduler ● TRITON Information Service for Explorer ● TRITON Reporter Scheduler ● TRITON Real-Time Monitor
Usage Monitor	Can run on every blade. ● Enables alerting based on Internet usage. ● Provides Internet usage information to Real-Time Monitor. Usage Monitor tracks URL category access (shown in Real-Time Monitor) and protocol access, and generates alert messages according to the alerting behavior you have configured.
Content Gateway	Can run on every blade. ● Provides a robust proxy and cache platform. ● Can analyze the content of websites and files in real time to categorize previously uncategorized sites. As part of a TRITON AP-WEB deployment, also: ● Analyzes HTML code to find security threats (for example, phishing, URL redirection, web exploits, and proxy avoidance). ● Inspects file content to assign a threat category (for example, viruses, Trojan horses, or worms). ● Strips active content from certain web pages.
Remote Filtering Client	● Resides on client machines outside the network firewall. ● Identifies the machines as clients to be managed, and communicates with Remote Filtering Server.
Remote Filtering Server	● Allows management of clients outside a network firewall. ● Communicates with Filtering Service to provide Internet access management of remote machines.

Web security solution Default policy

TRITON AP-WEB includes a Default policy, in effect 24 hours a day, 7 days a week. Initially, this policy monitors Internet traffic without blocking. When you first install the Web solution, the Default policy applies to everyone on the network. To customize the policy, use the Web module of the TRITON Manager and its embedded Help system.

TRITON AP-EMAIL deployment

Important

If you deploy TRITON AP-EMAIL on an X10G chassis that also hosts Web protection blades, you must choose a location for and configure a web policy server machine first, before configuring any other Web or Email blades. See *Locating the policy source in your deployment*, page 13, for details.

The rest of this section covers information specific to a TRITON AP-EMAIL deployment.

Email blade server components

The following services run on an Email blade server:

- Configuration service
- Authentication service
- Quarantine service
- Log service
- Update service
- Filtering service
- Mail Transfer Agent

The appliance also provides access to the Personal Email Manager and Secure Message Delivery end-user portals.

Software that runs off-chassis

Microsoft SQL Server 2008 or 2012 must be installed off-chassis and must be running before you install the TRITON Manager.

Use the TRITON installer v8.2.x from the Downloads page at www.forcepoint.com to install the following off-chassis components:

- Email module of TRITON Manager
- Email Log Server (Windows-only component)
- The TRITON AP-DATA module of TRITON Manager (Windows-only component)

  The TRITON AP-DATA module is required for data loss protection features.

See the Forcepoint Technical Library for more information about components and installation details.

General installation sequence

1. Plan your coverage. Every security blade server should be assigned an appropriate domain, based on traffic volume.
2. Ensure that one copy of Microsoft SQL Server is *installed and running* off-chassis (for TRITON reporting). Keep at hand the location and the authentication information for this database server.
3. For Web security deployments, choose your policy source machine before running firstboot on any blade servers.

   If your policy source will be located off-chassis, you will need to install TRITON components on that policy source server before you run firstboot. This is because firstboot will ask you for the IP address of the policy source machine and will try to connect to it. Therefore, the policy source machine needs to be set up on the network, and Policy Broker needs to be running before you run firstboot on the blades.

   If you plan to use the blade in Slot-1 for your policy source, then all you need to have running before booting the blade in Slot-1 is your SQL Server database.
4. Download the TRITON unified installer version 8.2.x for installing off-chassis components (see below).
5. Run firstboot and select the security mode, Email or Web, and then complete the configuration for all other blades that will run TRITON policy enforcement components.
6. Use the Custom installation option of the TRITON Windows installer to install additional components (if desired) off the chassis.
7. To install the TRITON management console and associated components, use the Custom installation option of the TRITON Windows installer and select the TRITON Manager installation option and mark the Email and/or Web check box.
8. Use the Custom installation option to install the Log Server off the chassis.

TRITON unified installer

The installer for off-chassis components to be hosted on a Windows server is: **TRITON82xSetup.exe**

The installer for off-chassis components to be hosted on a Linux server is: **Web82xSetup_Lnx.tar.gz**

To download the installers:

1. Go to My Account and log in to your account. If you don’t have an account, create one and then contact Forcepoint Technical Support to link your account to your Web and/or Email solution subscription key.
2. Click the **Downloads** tab.
3. Under **Download Product Installers**, select your Product and Version 8.2.x. The available installers are listed under the form.
4. Click the plus sign (“+”) next to an installer entry for more information about the installer.
5. Click the download link to download an installer.

3 Setting Up X10G Security Blades

Important

Web deployments must set up the Policy Broker and Policy Database server (may be an off-chassis server) before setting up other security blades. See *Big picture*, page 11 for details.

Before configuring your X10G blades, you must:

1. Install the X10G chassis and insert the blades, as described in *Hardware Setup for the X-Series Modular Chassis*, page 1.
2. Evaluate deployment options and plan your deployment.
   a. For a Web protection deployment, install your *policy source* machine. See *Deployment Planning for X10G Chassis and Blades*, page 10. If the *policy source* host is the security blade in Slot-1, install and configure that blade first using the instructions in this chapter.
   b. For an Email deployment, if your chassis will also host Web protection blades, you must install a policy source machine first. If you have already configured your policy source, see *Deployment Planning for X10G Chassis and Blades*, page 10, for information about Email protection components.
3. Install off-chassis components, as described in the topic titled *Software that runs off-chassis* in the appropriate Web or Email deployment sections:
   - *Web protection deployment*, page 13
   - *TRITON AP-EMAIL deployment*, page 19

Blade installation and configuration summary:

After SQL Server is running off-chassis and the Policy Broker is running (Web deployments), security blades are ready for power up and configuration. Follow these steps:

1. Power on each blade.
2. *Run firstboot*, page 23.
3. Perform *Additional security blade configuration*, page 27.

Off-chassis components require installation and configuration. See the topic titled *Software that runs off-chassis* in the appropriate web or email deployment sections:

- *Web protection deployment*, page 13
- *TRITON AP-EMAIL deployment*, page 19

The Deployment and Installation Center in the Forcepoint Technical Library has more information.

Run firstboot

Security blades are delivered ready to run the **firstboot** script, which completes the software installation and establishes basic blade configuration.

The firstboot script prompts you to:

- Select the security mode – Email or Web.
- If Web, select the policy mode for the blade: *Full policy source*, *User directory and filtering*, or *Filtering only.* If you're not certain about the correct choice, see *Web protection deployment*, page 13.
- Specify settings for the primary network interface (P1/eth0)
- Define some general items, such as the hostname and system password

You have an opportunity to change these settings before you exit firstboot. Later, if you want to change settings, you can do so through the security blade command-line interface (CLI).

Important

After firstboot has run to completion, it's not possible to change the security mode or policy mode of the blade without first re-imaging it. See *Recovering a Blade Server to a fresh image*, page 31 for details.

Gather the following information before running the firstboot script. Some of this information may have been written down on the Quick Start poster during hardware setup.

Hostname (example: appliance.domain.com) 1 - 60 characters long. The first character must be a letter. Allowed: letters, numbers, dashes, or periods. The name cannot end with a period. If this is a TRITON AP-WEB appliance and Content Gateway will be configured to perform Integrated Windows Authentication, the hostname cannot exceed 11 characters (excluding the domain name). For more information, see the section titled Integrated Windows Authentication in Content Gateway Manager Help.	
IP address for network interface P1 P1 handles all traffic to and from the chassis. After firstboot, the P2 network interface can be configured to handle egress traffic. See *Network interface P2*, page 28. NOTE: Consider using sequential IP addresses for sequential blades in the chassis	
Subnet mask for network interface P1	
Default gateway for network interface P1 (IP address)	
VLAN ID (optional; can be configured in later in the CLI). VLAN deployment should be carefully planned in advance of deployment.	
Primary DNS server for P1 and all active network interfaces on the security blade (IP address)	

Unified password. This password is used for this blade, and for: ● Security blade command-line interface (CLI) ● If a TRITON AP-WEB blade, the Content Gateway manager Some sites use the same password for all blades. The choice is yours. The password must be 8-15 characters. Include at least one of each of the following: ● Uppercase character ● Lowercase character ● Number ● Special character, such as ! # % & + / [ ] < = > Exclude all of the following: ● The user name of any appliance service account (e.g., admin, root, websense-ts, audit) ● Common appliance-related terms (e.g., appliance, filtering) ● The name of TRITON services (e.g., PolicyBroker or NetworkAgent) ● The device’s hostname ● The special characters: space $: ` \ " ● Must not repeat the previous 3 passwords for the account.	
If a Web blade: Send usage statistics?	Usage statistics from Web blade modules can optionally be sent to Forcepoint servers, to help improve the accuracy of traffic management and categorization.

To run the configuration script (firstboot):

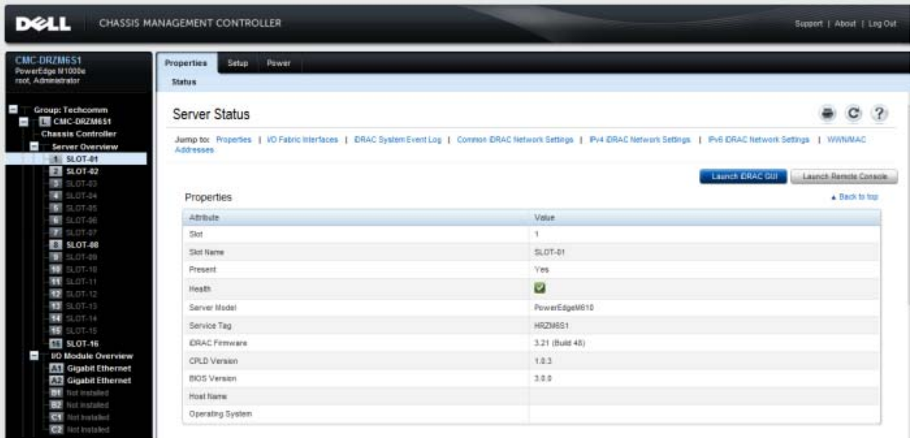
1. Power on the blade.
2. Log on to the CMC.
   a. Enter the IP address of the CMC into a browser that has connectivity to the network the chassis is on.

      ```
      http://<CMC IP address>
      ```

      Replace <CMC IP address> with the address assigned to the CMC during initial configuration of the chassis.

   b. If there is a security warming, continue to the address and enter the CMC log on credentials.

3. On the home screen, select SLOT-*N* from the list on the left, where “N” is the slot of the blade being configured. For Web deployments, if the *policy source* machine will be a blade server (Slot-1 recommended), configure it first.



Properties

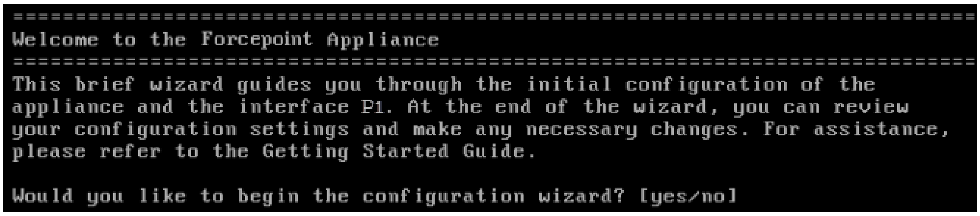
Attribute	Value
Slot	1
Slot Name	SLOT-01
Present	Yes
Health	✓
Server Model	PowerEdgeM610
Service Tag	HRZM6S1
iDRAC Firmware	3.21 (Build 48)
CPLD Version	1.0.3
BIOS Version	3.0.0
Host Name	
Operating System	

4. Select **Launch Remote Console** on the upper right. A new command-line window opens.

   If it fails to open, look in the blade iDRAC window (launched when you attempted to open the console), go to **Overview** > **Server** > **Console** and change the **Plug-in Type** from **Native** to **Java** or **Java** to **Native**. Click **Apply** and then **Launch Virtual Console** (upper left).

5. In the console, accept the subscription agreement if prompted.

6. Enter **yes** to launch the firstboot activation script when asked if you want to begin.



```
================================================================================
Welcome to the Forcepoint Appliance
================================================================================
This brief wizard guides you through the initial configuration of the
appliance and the interface P1. At the end of the wizard, you can review
your configuration settings and make any necessary changes. For assistance,
please refer to the Getting Started Guide.

Would you like to begin the configuration wizard? [yes/no]
```

Important

If you enter ‘no’, or exit firstboot before completing it (by pressing ‘Ctrl+c’), you are placed in the *view* context of the CLI. It is not possible to restart firstboot from the CLI. To restart firstboot you must restart the blade. In the Virtual Console, select the **Power** toolbar option and then select **Reset System (warm boot)**. The reboot completes with launching the firstboot script.

7. Follow the on-screen instructions to provide the information collected above.

8. In each section, type **yes** if you are satisfied with the settings. Type **no** if you want to change any.

After the activation script completes successfully, proceed to *Additional security blade configuration*.

Additional security blade configuration

After firstboot, complete security blade configuration using the command-line interface (CLI). In the CLI you can view system status, configure network and communication settings, and perform general security blade administration tasks. For complete information, see the X-Series v8.2.x CLI guide.

To complete security blade configuration:

- Optionally, *Enable SSH access to the command-line interface*, page 27
- Optionally, enable *Network interface P2*, page 28
- Optionally, configure *Static routes*, page 30
- Complete switch configuration. See the X-Series Switch Configuration guide.

When configuration of these items is complete, set up the next blade.

After all blades have been configured and all off-chassis components have been installed:

- Complete the switch configuration. See the X-Series Switch Configuration guide.
- Configure your TRITON solution.
  - TRITON AP-WEB initial configuration
  - TRITON AP-EMAIL initial configuration

Enable SSH access to the command-line interface

You can access the CLI through the security blade's iDRAC Virtual Console, which you used to complete firstboot.

Additionally and optionally, you can enable SSH access to the CLI. SSH access is disabled by default.

To enable SSH access:

1. Log on to the security blade's iDRAC and launch the Virtual Console to log on to the CLI. Use the **admin** account and the password you established at firstboot (or the most recent setting, if it has changed).
2. Change to the **config** context by entering 'config' on the command line, and enter the **admin** password again.
3. In config mode, check the status of SSH access by entering the command:

   ```
   show access ssh --status
   ```

   If SSH access is disabled, the response will be similar to:

   ```
   SSH access is disabled.
   ```
4. Enable SSH access with the command:

   ```
   set access ssh --status on
   ```

Confirm that SSH access has been enabled.

```
show access ssh --status
```

The response will be similar to:

```
SSH access is enabled.
```

5. Test SSH access. On a Windows system, use **PuTTY** or a similar tool to log on to the CLI. Use the admin credentials. On a Mac system use **iTerm** or **Terminal**, or similar.

Network interface P2

Primary network interface P1 (eth0) is configured during firstboot. P1 handles all communication among TRITON components, as well as traffic routed to the Content Gateway proxy (Web solution) or message transfer agent (Email solution).

Secondary network interface P2 (eth1) is disabled by default, but can be enabled to handle egress traffic.

If you want to use P2, prior to configuration gather the following information.

IP address for network interface P2	IP address:
Subnet mask for network interface P2	Subnet mask:
Default gateway for network interface P2 **Note:** The default gateway must be in the same subnet as the IP address of the interface used for communicating with the Internet (outbound traffic). If you use both P1 and P2 and they are located in different subnets, the default gateway is assigned to the interface that shares the same subnet. If P1 and P2 are on the same subnet, the default gateway is automatically assigned to P2. Ensure that outbound packets can reach the Internet.	IP address:
VLAN ID. VLAN deployment should be carefully planned for the entire deployment. Once VLAN is assigned it's possible to change the assignment, but the blade cannot be made VLAN-unaware without reimaging the blade.	VLAN ID:

To configure P2:

1. Access the security blade using its iDRAC.

   Open a supported browser and enter the following URL in the address bar:

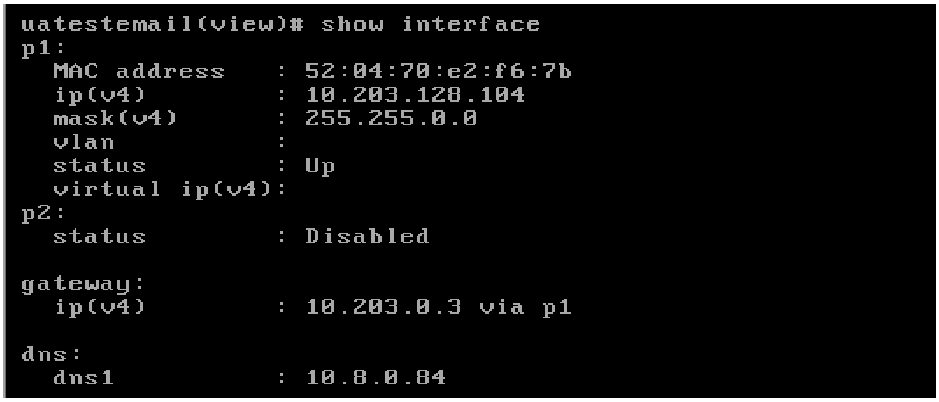
   ```
   http://<iDRAC IP address>
   ```

   Replace <iDRAC IP address> with the IP address assigned during CMC configuration. See *Assigning blade slot iDRAC addresses*, page 8.

2. On the home page, in the **Virtual Console Preview** area, click **Launch**.

3. Log on to the CLI with user name **admin** and the password set during firstboot.
4. Change to the **config** context by entering ‘config’ on the command line, and then the **admin** password again.
5. Check the status of the P1 and P2 network interfaces:

   ```
   show interface
   ```



```
uatestemail(view)# show interface
p1:
   MAC address     : 52:04:70:e2:f6:7b
   ip(v4)          : 10.203.128.104
   mask(v4)        : 255.255.0.0
   vlan            :
   status          : Up
   virtual ip(v4):
p2:
   status          : Disabled

gateway:
   ip(v4)          : 10.203.0.3 via p1

dns:
   dns1            : 10.8.0.84
```

6. Enable network interface P2:

   ```
   set interface p2 --status on
   ```

7. Set the IP address and mask of interface P2:

   ```
   set interface ipv4 --interface p2 --ip 10.203.128.105
         --mask 255.255.0.0
   ```

Important

The P1 interface is bound to the eth0 interface; the P2 interface is bound to the eth1 interface. This is important if you are using the Web solution.

For example, suppose you are using a transparent proxy deployment, and the P1 interface is connected to a WCCP router. In this case, you must configure Content Gateway to use the eth0 interface for WCCP communications (in the Content Gateway manager, see the **General** tab of the **Configure** > **Networking** > **WCCP** page).

When you use both P1 and P2, it is recommended that P1 be connected to the network so that it handles inbound traffic and P2 is positioned to handle outbound traffic. To enable this configuration, be sure to set appropriate routing rules for P1 and P2. See *Static routes*, page 30.

Static routes

You can define static routes if needed. Route configuration is described in detail in the X-Series v8.2.x CLI guide.

Route configuration is performed in the CLI. IPv4 and IPv6 address routing is supported for Web security blades. Only IPv4 address routing is available for email security blades. For basic information, in the CLI enter **help set route**, **help set route6**, **help load route**, and **help load route6**.

Load route/route6 (Web only) supports the loading of static routes contained in a plain text file. Routes are defined one per line. The format is

```
<destination_ip> <netmask> <gateway> <interface>
```

A blank space separates parameters on a single line. The characters "\r\n" serve as separators between lines (routes).

For example:

```
11.100.100.0 255.255.255.0 10.226.0.1 p1
11.200.100.0 255.255.255.0 10.226.0.1 p2
```

The usage for **load route** (IPv4 addresses) is:

```
load route --file <file_name>
           --location <filestore_alias>
           --action <add | del>
```

Set route/route6 (Web only) allows you to define one static route at a time.

The usage for **set route** (IPv4 addresses) is:

```
set route --dest <IPv4_address> --mask <IPv4_mask>
          --gateway <IPv4_address> --interface <p1 | p2>
```

✓ **Note**

An existing route cannot be edited. If you want to edit a route, delete it and then add (set) the desired route.

To remove a static route use **delete route/route6** (Web only).

The usage is (IPv4):

```
delete route --dest <IPv4_address> --mask <IPv4_mask>
       [--gateway <IPv4_address>] [--interface <p1 | p2>]
```

“--gateway” and “--interface” are optional.

Recovering a Blade Server to a fresh image

Should it become necessary to recover a blade server to a fresh installation of the current version, follow the direction in the knowledge base article titled How to Reimage an X10G Blade Server.