Getting Started

Websense® X-Series™· Modular Chassis Family
X10G™

v7.6.4

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2011 Revision A
Printed in the United States and Ireland

Trademarks

Contents

1 Hardware Setup for the X-Series Modular Chassis

The Websense® X-Series™ modular chassis solution is a high-performance network security system running on:

- **Websense X10G™ blade chassis**: The chassis is an energy-efficient blade enclosure from Dell™ that holds up to 16 security blades optimized for Web Security Gateway / Anywhere.
- **Websense X10G™ security blades**: These Dell blade servers are equipped with a hardened operating system and Websense Web security software. Blades are optimized for analyzing and filtering Web traffic and content in real time.

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 and configured by Websense, Inc.

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.

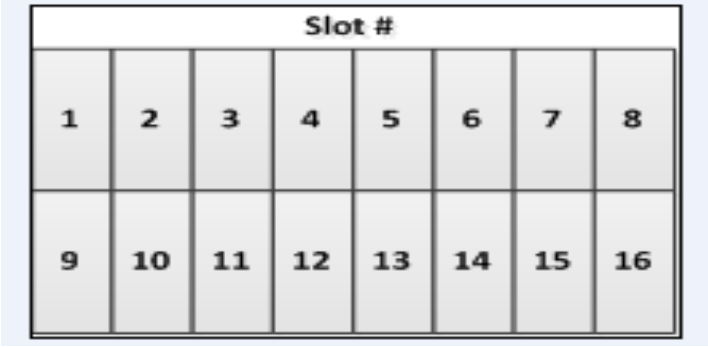
- Unpack and rack the chassis before you insert the security blades. Save the handled cardboard lifter, if a future chassis move is likely.
- Security blades are packaged separately, pre-loaded with Websense security software. You will run a firstboot script and enter a subscription key for each blade server, as described later in this guide.
- A few Websense components are Windows-only and must be installed and run off the chassis. The installer for these components is named **WebsenseTRITON762Setup.exe**. This installer is located on the Downloads page at www.websense.com. Be sure to read the one-page Save-Me-Time tips in the 7.6.2 downloads area.

X10G Quick Start poster

The Websense **X10G Quick Start Poster**, included in the chassis shipping box and also available at support.websense.com/x10g, shows all items included in each Websense 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. Bottom slot numbers begin with slot 9 at the left, ending at slot 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.
- **Slots 2 through 15**: Insert blades into consecutive slots, with no empty slots between blades, unless you are using Network Agent (slot 16 only).
- **Slot 16**: No matter how many blades you plan to insert, use only slot 16 for the blade that will run (optional component) Network Agent.
  - Network Agent is a Websense component that monitors and filters non-HTTP and non-HTTPS traffic (such as Instant Messaging and streaming media). It is also used to monitor bandwidth usage in your network.
  - You have the choice of running one copy of this component on the security blade in slot 16. You can also run one or more copies of Network Agent on off-chassis servers. No blade other than the blade in slot 16 can run the Network Agent component on the chassis.
  - If Network Agent will not be running on the chassis at your site, slot 16 may be filled after slots 1 through 15 are filled, and the blade in slot 16 can run the same configuration that runs on the blades in the other 15 slots (no Network Agent). You make this choice when you run a script called **firstboot** on the blade.

After the chassis is racked and the blades are all inserted properly, you are ready to cable the X10G into your network and connect the power units.

Before finalizing your cable connections, consult with your Websense 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.

iDRAC and interface IP address planning

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

Reserve at least 64 consecutive 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`
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 as well (such as C, A1.P1, and possibly A1.P2).

For example:

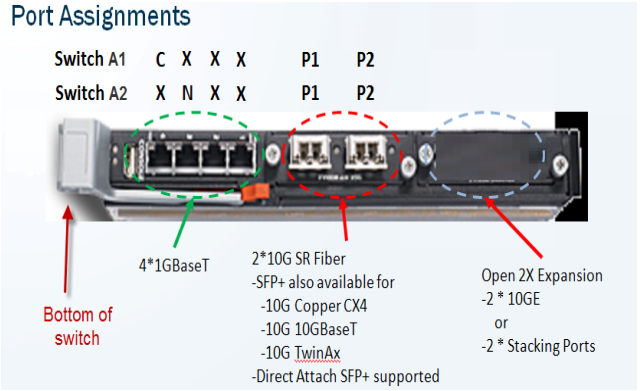
- IP address of CMC might be: `010.008.000.100`
- IP address range (remote access) for16 blade iDRACs: `010.008.000.101 - 010.008.000.116`
- Subnet mask: `255.255.000.000`
- Gateway IP address: `010.008.000.001`

- The C interfaces (typically interface C connects to the Internet) on the 16 blades might use this IP address range: `010.008.010.201` through `010.008.010.216`
- The A1.P1 proxy interface on the 16 blades might use IP address range: `010.014.000.100` through `010.014.000.116`
- IP address of on-chassis switch A1 might be: `010.015.000.121`
- IP address of on-chassis switch A2 might be: `010.015.000.122`

X10G chassis cabling

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 to connect the P1 interface on chassis switch A1 (left switch) to your network, or install an optical transceiver and then substitute your own fiber optic cable if desired (see details below).



   - Fiber optics: If you ordered an optical transceiver kit with your chassis, follow the instructions provided with the Websense X10G checklist to install the transceivers into the switches at the back of the chassis. (For a copy of the instructions, see support.websense.com/x10g.) 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.
2. Connect a Category 5 network cable (do not use a crossover cable) from the leftmost network port (**Gb**) of the Chassis Management Controller to a switch on the subdomain where the CMC IP address is located (see photo below).

The Chassis Management Controller (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.

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 power on, pull out the LCD screen and use it to:

1. set your language preference
2. specify one IP address: the address for 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.

LCD Prompt	Recommended response
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.

Use the username **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**...checkbox 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.

   Note: 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 **User Authentication** > **Chassis Overview**.
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 to it, confirm and implement your decisions about how Websense components will be allocated across the domains in your network.

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

Note that the software modules running on the X10G are at version 7.6.2 and are compatible with off-chassis modules at that version.

Big picture

You need an instance of Microsoft SQL Server 2005 or 2008 *installed and running* off-chassis in your network, for the Websense reporting database.

TRITON unified installer

A few Websense components (such as the TRITON management console and reporting Log Server) also run off the chassis and must be installed separately.

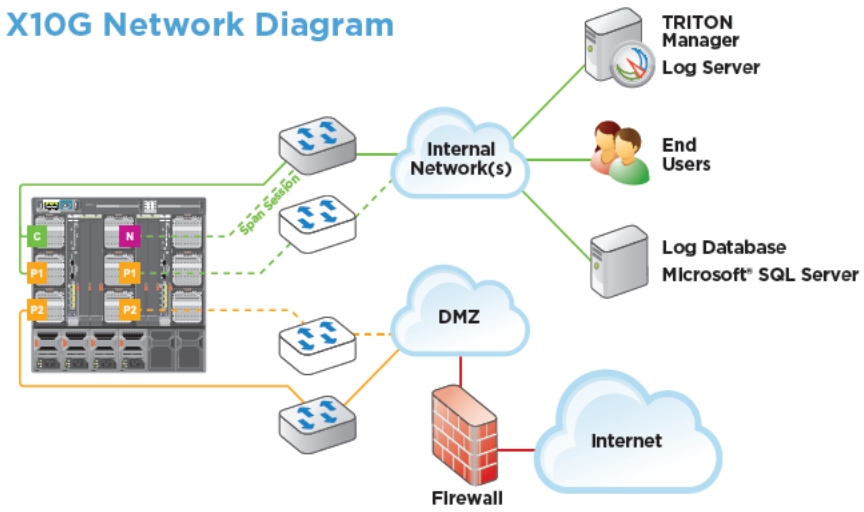
The installer for the off-chassis components is named **WebsenseTRITON762Setup.exe**.

This installer is located on the Downloads page at www.websense.com. Be sure to read the one-page Save-Me-Time tips in the 7.6.2 downloads area.

Policy source

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 you use a blade server for the *policy source*, best practice is to use the blade in slot 1.

Each security blade in the chassis must then be configured to point to the blade (or other server) that hosts **Policy Database** and **Policy Broker**.



The general sequence of events:

1. Plan your coverage. Each blade server should be assigned to filter an appropriate domain, based on traffic volume.
2. Ensure that one copy of Microsoft SQL Server is *installed and running* off-chassis (for Websense reporting). Keep at hand the location and the authentication information for this database server.
3. Download the Websense TRITON installer version 7.6.2 for installing off-chassis components.
4. Next, identify and configure the *policy source* machine for your network. You can use a blade for the *policy source*, or an off-chassis server. The *policy source* machine runs all filtering components, and is the *only* machine to run Policy Database and Policy Broker..
5. Configure all other blades that will run Websense filtering components.
6. Use the Custom installation option of the TRITON Windows installer to install additional copies of filtering compinents (if desired) off the chassis.
7. Use the Custom installation option to install the TRITON Web Security management console and associated components on a Windows server off the chassis.
8. Use the Custom installation option to install the Websense reporting components off the chassis. Log Server can be located on the same server with the TRITON management console.

Choosing a policy source machine

One of your earliest deployment decisions is your selection of the *policy source* machine. Only one computer must be designated as your *policy source*. Other servers look to this machine to obtain your current filtering policy.

You can select either a blade server or a server off the X10G chassis for this purpose.

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

All machines running Websense filtering components need up-to-date policy information obtained from the single *policy source* machine.

Following is a brief description of the key filtering components that you are deploying. You have several choices about which components will run on each security blade in your X10G chassis, and whether it would be advisable for your network to use additional off-chassis instances.

For component limits and rations, see this article in the Websense Technical Library.

Filtering components

Component	Description
Policy Database	Stores Websense software settings and policy information. Installed automatically with Policy Broker. Runs on *policy source* machine only.
Policy Broker	Manages requests from Websense components for policy and general configuration information. Runs on *policy source* machine only.
Policy Server	Can run on every blade. • Identifies and tracks the location and status of other Websense components. • Stores configuration information specific to a single Policy Server instance. • Communicates configuration data to Filtering Service, for use in filtering Internet requests. Configure Policy Server settings in the TRITON - Web Security console. Policy and most configuration settings are shared among all Policy Servers that share a Policy Database.

Component	Description
Filtering Service	Can run on every blade. Provides Internet filtering 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 filtered and logged. • Each Filtering Service instance downloads its own copy of the Websense Master Database. Configure filtering and Filtering Service behavior in the TRITON - Web Security console.
Network Agent	Can run only on the blade in slot 16, and can run off-chassis. • Enhances filtering and logging functions • Enables non-HTTP amd non-HTTPS protocol management
Master Database	• Includes more than 36 million Web sites, sorted into more than 90 categories and subcategories • Contains more than 100 non-HTTP protocol definitions for use in filtering protocols After all modules are set up, download the Websense Master Database to activate Internet filtering, and schedule automatic updates. If the Master Database is more than 2 weeks old, no filtering occurs.
TRITON - Web Security	Runs off-chassis on a Windows server. Serves as the configuration, management, and reporting interface for Websense software. Use the TRITON - Web Security console to define and customize Internet access policies, configure Websense software components, report on Internet filtering activity, and more. The TRITON - Web Security console is made up of the following services: • Websense - TRITON Web Security • Websense Web Reporting Tools • Websense Explorer Report Scheduler • Websense Information Service for Explorer • Websense Reporter Scheduler
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.

Component	Description
Content Gateway	Can run on every blade. (Not used on the blade in slot 16 if Network Agent is enabled.) • Provides a robust proxy and cache platform. • Can analyze the content of Web sites and files in real time to categorize previously uncategorized sites. • Enables protocol management As part of a Websense Web Security Gateway 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 filtered, and communicates with Remote Filtering Server.
Remote Filtering Server	• Allows filtering of clients outside a network firewall. • Communicates with Filtering Service to provide Internet access management of remote machines.

Understanding the Policy Database

Websense Policy Database stores both policy data (including clients, filters, filter components, and delegated administration settings) and global settings configured in the TRITON - Web Security console. 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 X-Series chassis deployment), a single Policy Database holds policy and general configuration data for all Policy Server instances.

1. At startup, each Websense 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 TRITON - Web Security console 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 whether you will use a security blade as the *policy source* machine, or an off-chassis 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 Websense components in your network. This chapter describes deployment options and best practices. Keep in mind that these will vary with each network's characteristics.

Software provided on the security blades

Web components

Each security blade has version 7.6.2 of the following core Web security components pre-loaded:

- Policy Database
- Policy Broker
- Policy Server
- Filtering Service
- User Service
- Usage Monitor
- Control Service
- Directory Agent (for sites using hybrid Web security)
- Demo version of TRITON - Web Security console (not for production use)
- Content Gateway (proxy)
- Network Agent (optional and used only on blade in slot 16)

Software that runs off-chassis

The Websense components mentioned in this section should be installed off-chassis. Additionally, Microsoft SQL Server 2005 or 2008 should be installed off-chassis.

Use the TRITON installer (version 7.6.2 or later from the Downloads page at www.websense.com) to install any of the components mentioned here. See the Websense Technical Library for more information about components and installation details.

Web components

The following Web components should be installed off-chassis. Some are Windows-only components.

- Web Security Log Server
- Real-Time Monitor
- Sync Service (for sites using hybrid Web security)
- Linking Service (for sites using any integrated Data Security 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

> **Note**
> If your subscription includes Websense Web Security Gateway Anywhere (hybrid cloud features), TRITON Unified Security Center must run on a Windows Server 2008 R2 machine.

TRITON Unified Security Center

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

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

To enable more than one module of the TRITON Unified Security Center—for example, both Web Security and Data Security—you must install TRITON Unified Security Center on a Windows Server 2008 R2 (64-bit) machine. TRITON Unified Security Center must be able to reach each blade's C interface.

For more information about the TRITON Unified Security Center and its modules, see the Websense 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 Websense 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:

- Websense TRITON Unified Security Center
- Websense TRITON Central Access
- Websense TRITON Settings Database
- Websense TRITON Reporting Database (if using SQL Server 2008 R2 Express)

TRITON - Web Security

TRITON - Web Security is the console used to perform general configuration tasks, set up filtering policies, assign policies to users and groups, run reports, and other management tasks.

TRITON - Web Security services include:

- Websense TRITON - Web Security (formerly ApacheTomcatWebsense)
- Websense Web Reporting Tools (formerly Apache2Websense)
- Investigative Reports Scheduler
- Reports Information Service
- Websense RTM Client (if Real-Time Monitor is used)
- Websense RTM Database (if Real-Time Monitor is used)
- Websense RTM Server (if Real-Time Monitor is used)

The TRITON console with the Web Security module only is pre-installed on blade servers as a convenience for evaluations.

Database management software

Websense Web security products (and Email security products on V-Series appliances) require Microsoft SQL Server to host the reporting database, called the Log Database. The Web Security Log Database and the Email Security 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 Security Log Server, SQL Server 2005 or 2008 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 Websense subscription. Refer to Microsoft documentation for installation and configuration instructions.

If you do not have SQL Server, you can use the Websense 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 Unified Security Center 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.

Modes

Each Websense X-Series blade server runs Web Security Gateway / Anywhere and can be configured in either of these modes:

Mode	Module name
Web Security Gateway without Network Agent	Web Security Gateway / Anywhere
Web Security Gateway, optimized for Network Agent	Web Security Gateway / Anywhere (This mode is optional. If used, it applies only to the blade in slot 16.)

You choose the mode of a blade server during initial *firstboot* configuration, as explained in Chapter 3. See *Run firstboot*, page 23, for more information about *firstboot*.

> **Important**
> In a fully-loaded chassis (all slots full), more than one instance of Network Agent is likely to be required to handle the traffic load. Deploy Network Agent off-chassis in this situation.

3 Setting Up Websense X10G Security Blades

Important

The blade (or other server) that runs Policy Broker and Policy Database should be set up before you configure remaining blades. See *Big picture*, page 14 for details.

After installing the X10G chassis and inserting the blades, as described in the prior chapter, you must configure each blade.

Configuration involves two tasks:

1. *Run firstboot*, page 23
2. *Configure the security blade*, page 26

Additional initial configuration steps and components may be necessary for your deployment. See *Software that runs off-blade server*, page 9 and the Deployment and Installation Center in the Websense Technical Library for more information.

Run firstboot

Run *firstboot* before using an X10G blade. Firstboot is a brief script that prompts you to:

- select the mode for the blade (slot 16 only)
- supply settings for the network interface labeled C
- enter a few other general items, such as hostname and password

You have an opportunity to change the settings before you exit firstboot. After you approve the settings, the security blade is configured.

Later, if you want to change settings (except the mode), you can do so through the Security Blade Manager user interface.

To change the mode, re-image the security blade and then run the firstboot script again. See *Restoring to Factory Image*, page 36 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.

Mode	Available only on blade in slot 16. Choose one: • Web Security Gateway without Network Agent (see *Switch configuration essentials* for one additional mandatory step) • Web Security Gateway optimized for Network Agent
Hostname (example: bladeserver.domain.com)	
IP address for network interface C NOTE: consider using sequential IP addresses for sequential blades in the chassis. For example, the blade in slot one could be 10.202.230.1, blade in slot two 10.202.230.2, and so forth.	
Subnet mask for network interface C	
Default gateway for network interface C (IP address) *Optional* NOTE: If you do not provide access to the Internet for interface C, use the TRITON - Web Security console to configure A1.P1 to download Master URL Database updates from Websense (Web mode) See the TRITON - Web Security Help for information about configuring Websense database downloads.	
Primary DNS server for network interface C (IP address)	
Unified password (8 to 15 characters, at least 1 letter and 1 number) This password is used for this one blade, for the following: • Security Blade Manager • Content Gateway Manager • TRITON - Web Security (demo console on blade) Some sites use the same password for all blades. This choice is yours.	
Send usage statistics?	Usage statistics from security blade modules can optionally be sent to Websense servers, to help improve the accuracy of filtering and categorization.

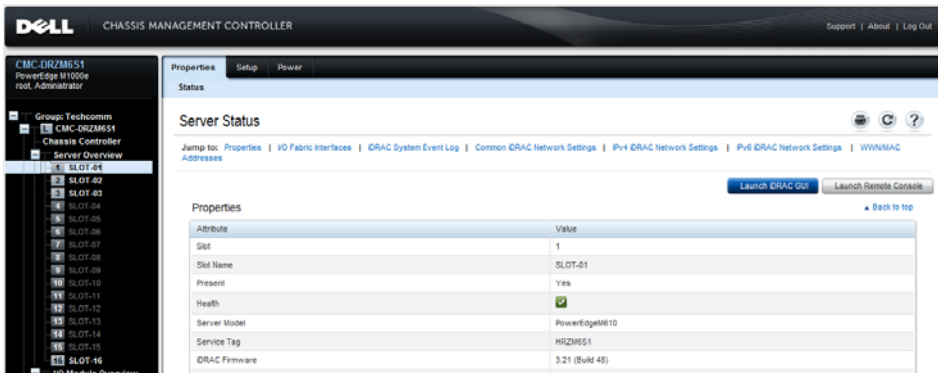
Run the configuration script (firstboot) as follows.

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

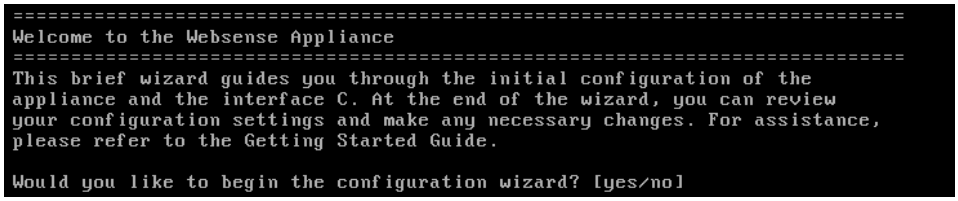
   ```
   http://<CMC IP address>
   ```

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

1. Log on to the CMC console.
2. Select SLOT-N from the list on the left, where “N” is the slot of the blade being configured.



3. Select “Launch Remote Console” on the upper right. A new command-line window opens.
4. Accept the subscription agreement if prompted.
5. Enter **yes** to launch the firstboot activation script when asked if you want to begin. Note: if you need to run firstboot again, simply enter the command `firstboot` at the command line.



6. For the blade in slot 16, select a mode:
   - Web Security Gateway without Network Agent (Requires switch A2 configuration. See *Switch configuration essentials*.)
   - Web Security Gateway optimized for Network Agent (Switch A2 is ready for this mode by default.)
7. Follow the on-screen instructions to provide the information collected above.
8. Type **yes** if you are satisfied with the settings. Type **no** if you wish to reset them.

After the activation script completes successfully, proceed to the next section to configure several additional settings on the blade with Security Blade Manager.

Configure the security blade

The next step is to configure the blade using the Web-based configuration interface called Security Blade Manager. Through it you can view system status, configure network and communication settings, perform general security blade administration tasks, and configure important settings for network interfaces A1.P1, A1.P2, and N (some interfaces are optional in some modes).

Gather information described in the following sections before running the Security Blade Manager:

- *Web Security Gateway without Network Agent*, page 26
- *Web Security Gateway optimized for Network Agent (Slot 16)*, page 32

Complete only the section that applies to your blade and security mode.

Web Security Gateway without Network Agent

For each blade that does not run Network Agent, after firstboot you will use the Security Blade Manager to configure important settings for network interfaces A1.P1 (and optionally A1.P2), which are used for communication by Websense Content Gateway.

Gather the following information before running the Security Blade Manager.

Primary NTP server *Optional* Be sure that interface C can access the NTP server. If interface C does not have Internet access, you can install an NTP server locally on a subnet that can be accessed by interface C.	Domain:
Secondary NTP server *Optional*	Domain:
Tertiary NTP server *Optional*	Domain:
IP address for network interface A1.P1	IP address:
Subnet mask for network interface A1.P1	Subnet mask:

Default gateway for network interface A1.P1 and A1.P2 (if used). The gateway must be in the same subnet as the IP address of the interface (A1.P1 or A1.P2) used for communicating with the Internet (outbound traffic). If you use both A1.P1 and A1.P2 and they are located in different subnets, the default gateway is assigned to the interface that shares the same subnet. If A1.P1 and A1.P2 are within the same subnet, the default gateway is automatically assigned to A1.P2 (which is bound to the virtual eth1 interface). Ensure that outbound packets can reach the Internet.	IP address:
Primary DNS server for network interface A1.P1 and A1.P2 (if used)	IP address:
Secondary DNS server for network interface A1.P1 and A1.P2 (if used) *Optional*	IP address:
Tertiary DNS server for network interface A1.P1 and A1.P2 (if used) *Optional*	IP address:
IP address for network interface A1.P2 *Required only if A1.P2 is enabled*	IP address:
Subnet mask for network interface A1.P2 *Required only if A1.P2 is enabled*	Subnet mask:
Full policy source IP address	This blade provides (choose one): • Full policy source (only one blade on a chassis, or one server off-chassis, should be selected to provide full policy) • User directory and filtering (you must specify the IP address of a security blade or other machine hosting Policy Database (*full policy source*) • Filtering only (you must specify IP address of a security blade or other machine running Policy Server, which can be a *full policy source* or *user directory and filtering* machine)

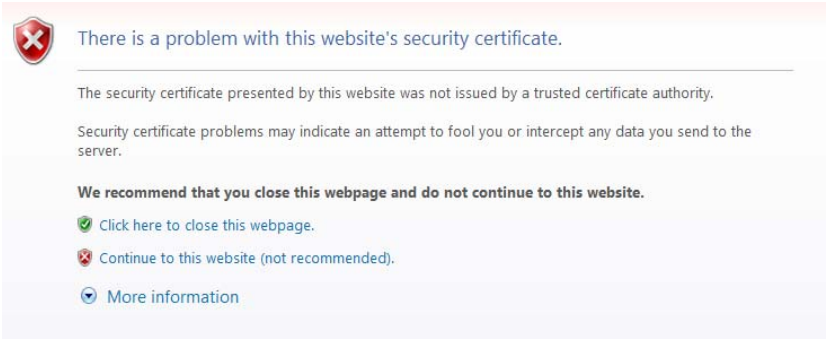
After collecting the information needed, access Security Blade Manager through a supported browser and follow the steps below to enable default proxy caching and Web filtering. See the Security Blade Manager Help for detailed instructions.

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

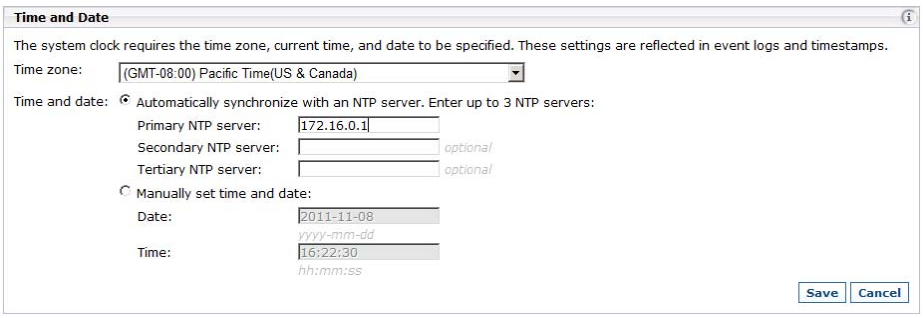
   ```
   http://<IP address>
   ```

Replace <IP address> with the address assigned to network interface C during firstboot.

2. Select Security Blade Manager.
3. Select Continue to this website.



4. Log on with the user name **admin** and the password set during firstboot.
5. In the left navigation pane, click **Configuration > System**.
6. Under **Time and Date**:

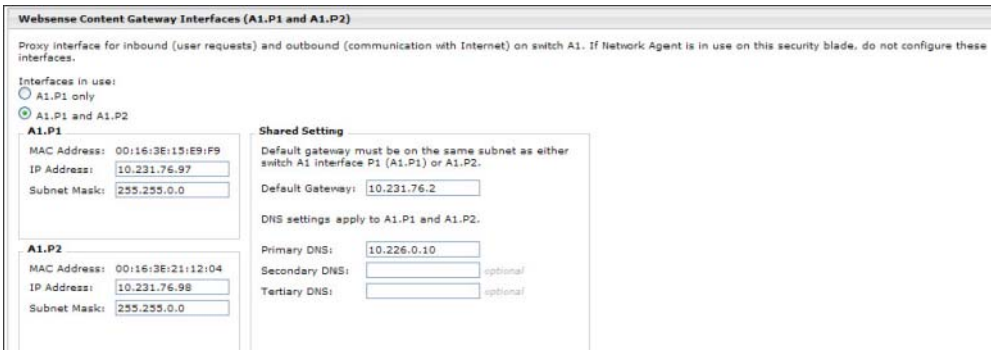


   a. Set the time zone.
   b. Set the time and date:

- **Automatically synchronize with an NTP server**: select this option to use a Network Time Protocol server. Specify up to three NTP servers. Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.
- **Manually set time and date**: select this option to enter a system time and date yourself.

c. Click **Save** in the Time and Date area.

7. In the left navigation pane, click **Configuration > Network Interfaces**.
8. Under **Websense Content Gateway Interfaces**, configure the A1.P1 and (optional) A1.P2 interfaces. The P interfaces are used to accept users' Internet requests (inbound traffic) and communicate with Web servers (outbound traffic).



To configure the P interfaces:

a. Select **A1.P1 only** or **A1.P1 and A1.P2**.

If you choose A1.P1 only, enter configuration information (IP address, subnet mask, default gateway, DNS IP addresses) under A1.P1.

If you choose A1.P1 and A1.P2, enter configuration information under both A1.P1 and A1.P2. Note that default gateway and DNS configuration (under **Shared Setting**) are shared between both A1.P1 and A1.P2.

b. Click **Save** in the **Websense Content Gateway Interfaces** area when you are done.

Important

If you use the A1.P2 interface, the A1.P1 interface is bound to the virtual eth0 interface, and the A1.P2 interface is bound to the virtual eth1 interface. Keep this in mind when you configure Content Gateway.

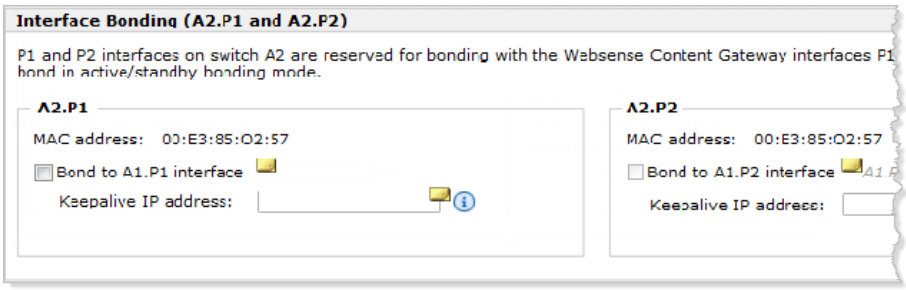
For example, suppose you are using a transparent proxy deployment, and the A1.P1 interface is connected to a WCCP router. In this case, you must configure Content Gateway to use the virtual eth0 interface for WCCP communications (in Content Gateway Manager, see the General tab of the Configure > Networking > WCCP page).

When only A1.P1 is used, it handles both inbound and outbound traffic for the proxy module (Content Gateway).

Alternatively, you could use both A1.P1 and A1.P2 such that A1.P1 handles inbound traffic and A1.P2 handles outbound traffic. To enable this configuration, be sure to set appropriate routing rules for A1.P1 and A1.P2 on the **Configuration > Routing** page. For example, you might set outbound traffic to go through A1.P2.

Additionally, you can use A1.P1 as a communication channel for multiple Content Gateway servers in a cluster. In this scenario, A1.P1 should not be used for outbound traffic. For additional information on clusters, see the Content Gateway Manager Help.

9. Configure Interface Bonding if desired for failover (see *Switch configuration essentials*):

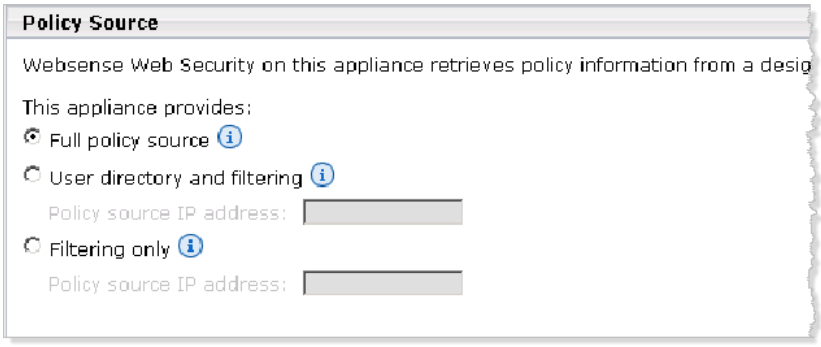


10. Configure routes if desired:
    a. In the left navigation pane, click **Configuration > Routing**.
    b. Under Static Routes, use the **Add/Import** button to specify customized, static routes.
    c. Under Module Routes, use the **Add** button to specify non-management Web Security traffic through the C interface.
    d. For either static or module routes, use the **Delete** button to remove existing routes, if necessary.

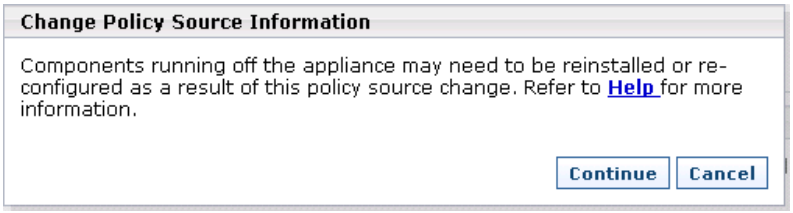
> **Note**
> An existing route cannot be edited. If you want to edit a route, delete it and then use the **Add/Import** (static) or **Add** (module) button to specify the route with the changes you want.

See the Security Blade Manager Help for more information about static and module routes.

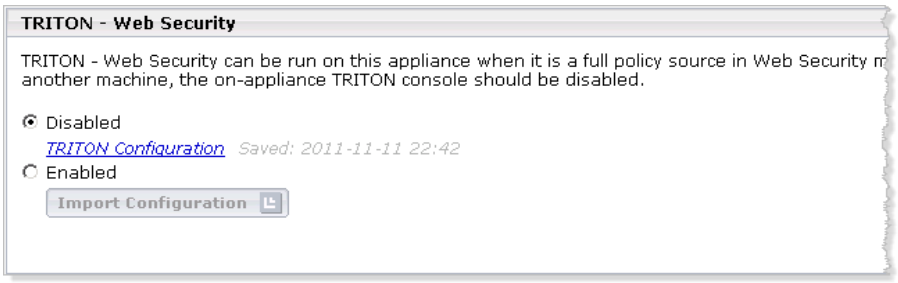
11. Select the policy mode of this security blade:
    a. In the left navigation pane, click **Configuration > Web Security Components**. Specify the role of this security blade with respect to Websense Web Security policy information. You will have three choices.



    Note, Websense blades ship with Full policy source enabled, but only one blade in a chassis (or one server off-chassis) should be the Full policy source. The rest should be used for user directory and filtering, or filtering only.
    b. Choose **Full policy source** if the blade being configured is the full policy source for the chassis.
    c. Choose **User directory and filtering** or **Filtering only** if the security blade currently being configured is *not* the location of the Policy Database. Enter the **IP address** of the machine hosting Policy Database (the policy source).
    d. Click **Save**.
    e. Click **Continue** on the following dialog box, assuming you are doing an initial setup (no servers were previously set to communicate with this blade for policy information).



f. **Disable** the demo copy of TRITON-Web Security on the blade and **Save**.



12. Click **Log Off**, at the top right, when you are ready to log off Security Blade Manager.
13. Set up the next blade, or begin installing off-chassis components.

Web Security Gateway optimized for Network Agent (Slot 16)

For the blade running Network Agent, after firstboot you will use the Security Blade Manager to configure interface N (Network Agent).

Gather the following information before running the Security Blade Manager.

Primary NTP server *Optional* Be sure that interface C can access the NTP server. If interface C does not have Internet access, you can install an NTP server locally on a subnet that can be accessed by interface C.	Domain:
Secondary NTP server *Optional*	Domain:
Tertiary NTP server *Optional*	Domain:
IP address for network interface N	IP address:
Subnet mask for network interface N	Subnet mask:
Primary DNS server for network interface N	IP address:
Secondary DNS server for network interface N *Optional*	IP address:
Tertiary DNS server for network interface N *Optional*	IP address:

Full policy source IP address	This blade provides (choose one): • User directory and filtering (you must specify the IP address of a security blade or other machine running Policy Broker, which can be a *full policy source blade*) • Filtering only (you must specify IP address of a security blade or other machine running Policy Server, which can be a *full policy source* or *user directory and filtering* machine)
TRITON Unified Security Center location (management console for Web Security Gateway). See the Websense Technical Library for details.	Choose: runs on separate server

After collecting the information needed, access the Security Blade Manager through a supported browser and follow the steps below. See the Security Blade Manager Help for detailed instructions.

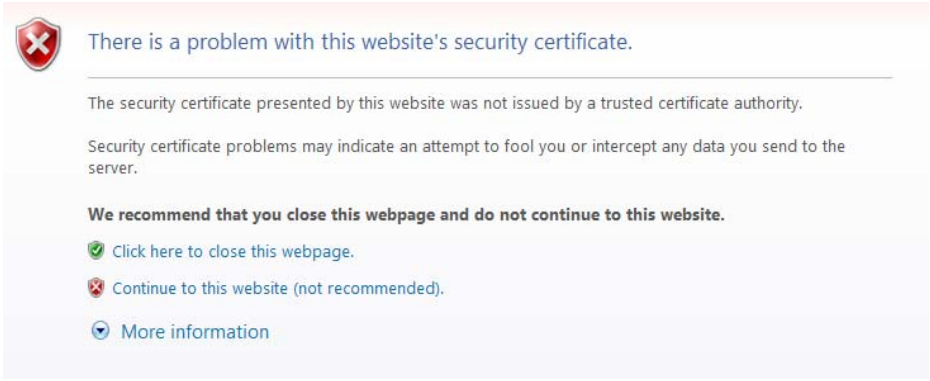
1. Open a supported browser, and enter the following URL in the address bar:

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

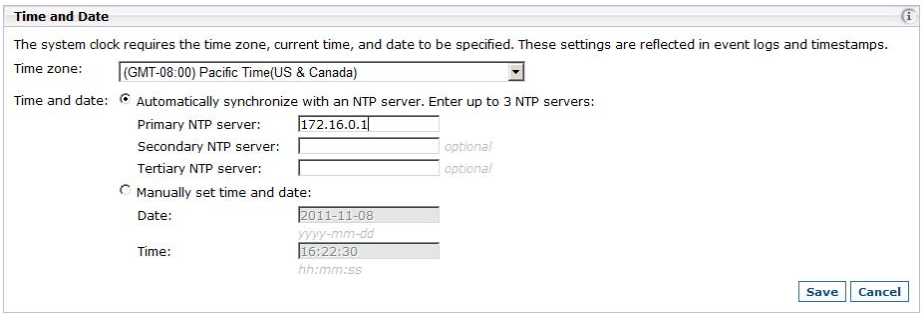
   Replace <IP address> with the address assigned to network interface C during firstboot.

2. Select Security Blade Manager.

3. Select Continue to this website



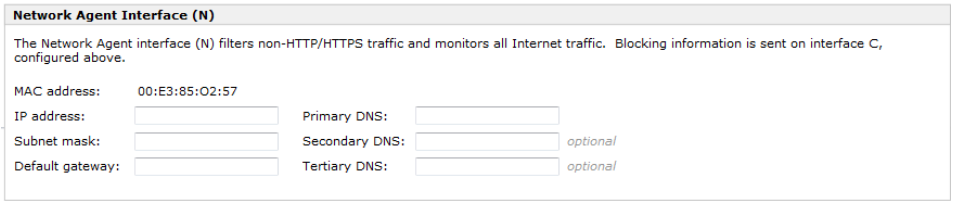
4. Log on with the user name **admin** and the password set during firstboot.
5. In the left navigation pane, click **Configuration > System**.
6. Under **Time and Date**:



   a. Set the time zone.
   b. Set the time and date:
      - **Automatically synchronize with an NTP server**: select this option to use a Network Time Protocol server. Specify up to three NTP servers. Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.
      - **Manually set time and date**: select this option to enter a system time and date yourself.
   c. Click **Save** in the Time and Date area.
7. In the left navigation pane, click **Configuration > Network Interfaces**.
8. Under **Network Agent Interface (N)**, configure the N interface. Note: this option is available only for blades configured to run Network Agent during firstboot.

   The N interface is used by the Network Agent module. It must be connected to a span (or mirror) port on a switch, allowing it to monitor the Internet requests going through the switch. (Note: be sure to configure the switch so the span port is

monitoring all the ports carrying the traffic of interest, See your switch manufacturer's documentation for configuration instructions).



> **Note**
> The security blade does not send block pages to end users who are blocked from non-HTTP and non-HTTPS protocols. The end users simply do not receive the blocked content.

a. Click **Save** in the **Network Agent Interface (N)** area.

9. Configure routes if necessary:
   a. In the left navigation pane, click **Configuration** > **Routing**.
   b. Under Static Routes, use the **Add/Import** button to specify customized, static routes.
   c. Under Module Routes, use the **Add** button to specify non-management Web Security traffic through the C interface.
   d. For either static or module routes, use the **Delete** button to remove existing routes, if necessary.

> **Note**
> An existing route cannot be edited. If you want to edit a route, delete it and then use the **Add/Import** (static) or **Add** (module) button to specify the route with the changes you want.

   See the Security Blade Manager Help for more information about static and module routes.
10. Select the policy mode of this security blade:
    a. In the left navigation pane, click **Configuration** > **Web Security Components**.
    b. Choose **User directory and filtering** or **Filtering only**. Enter the **IP address** of the machine hosting Policy Database (the policy source).
11. Click **Save**.
12. Click **Log Off**, at the top right, when you are ready to log off Security Blade Manager.
13. Set up the next blade, or begin installation of off-chassis components.

Switch configuration essentials

Switch A1 arrives from the Websense factory with a default configuration that supports the C interface for all blades on the chassis. It also supports the A1.P1 and A1.P2 interfaces on the blades in slots 1 through 15. These interfaces are used for proxy traffic.

Switch A2 arrives preconfigured to support the N interface (Network Agent) on the blade in slot 16.

No Network Agent

If you do not want to run Network Agent on the blade in slot 16:

1. Use the CMC Web interface to select SLOT-16 and run `firstboot` on the blade in slot 16. Change the blade's mode to **wcg**.
2. Unplug the network cables on switch A2.
3. Log on to the Security Blade Manager for the blade in slot 1. Run the CLI command "`switch A2 configure wcg`" to configure the A2 switch so that the N interface is disabled.
4. Wait for the switch to finish rebooting, then run "`switch A2 verify`" to verify that the configuration is as expected.
5. Plug in the network cables on switch A2.

Restoring to Factory Image

The X10G comes with a recovery DVD that can be used to restore each security blade to its Websense factory image. You can use this DVD (after saving a Full configuration backup) to re-image the security blade and then recover your custom blade and module settings.

Important

Use the original recovery DVD that came with your security blade. If you have misplaced it, you can download an image from MyWebsense. It is important you use an image that is associated with the manufacture date of your security blade. The MyWebsense Downloads page will indicate the security blade manufacture date appropriate for each image.

Note that all Websense components running off the chassis must be stopped before you reset the blade to factory image.

1. Stop all Websense components that are running off the chassis. For example, stop Web Security Log Server, Sync Service, Linking Service, transparent ID agents, and TRITON Unified Security Center.
2. If possible, back up any information on the blade that you want preserved.
   a. Using a Web browser, log on to the Security Blade Manager:

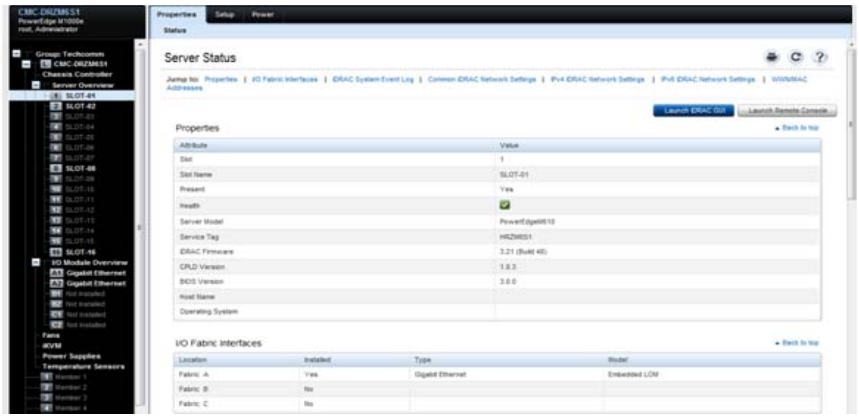
      `http://<C interface IP address>`

   b. Go to **Administration** > **Backup Utility**, and create a Full Configuration backup. See online Help for assistance. Save this backup file to another machine.
3. Plug the DVD drive into the blade's USB port (front of blade) and insert the recovery disk into the DVD drive.
4. To start the reboot:
   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>

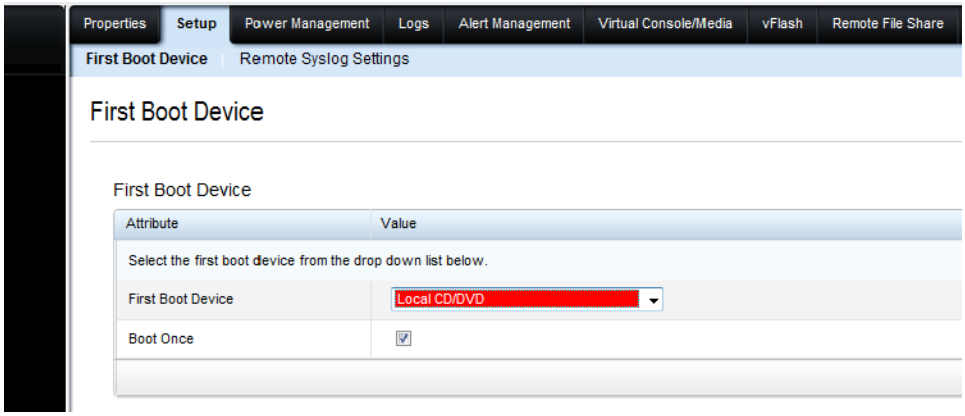
      Replace <CMC IP address> with the address assigned to the CMC during initial configuration of the chassis.

   b. Log on to the CMC console and select SLOT-N from the list on the left, where "N" is the slot of the blade being configured.

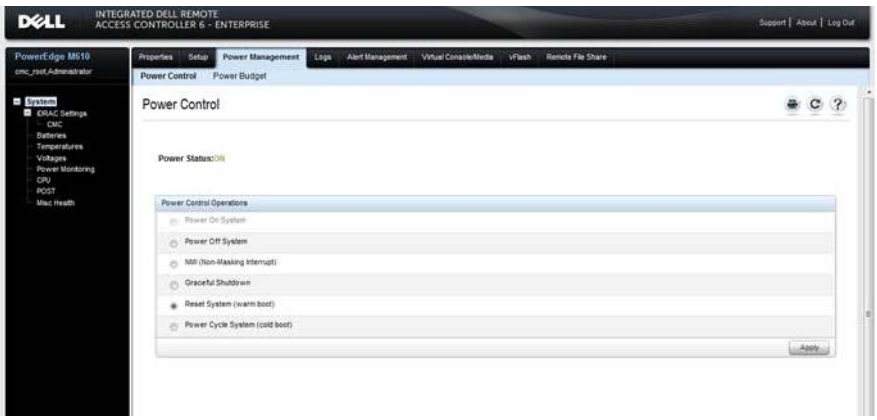


5. Select "Launch iDRAC GUI" at the right.

6. Under the **Setup** tab, set the First Boot Device to be **Local CD/DVD**. Click **Apply**.



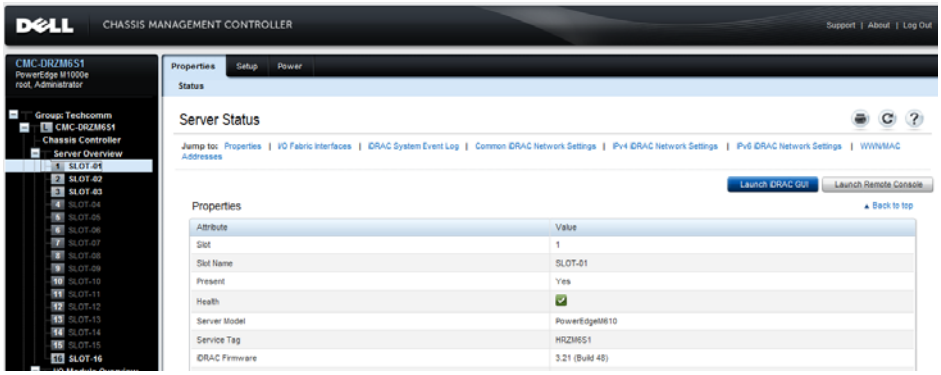
7. Under the **Power Management** tab, select **Reset System** (warm boot). Click **Apply**.



8. The reboot from DVD may take 20 minutes. After the reboot has completed, run the firstboot script on the reset blade. To do this:
    a. Enter the IP address of the CMC into a browser that has connectivity to the network the chassis is on.
    b. http://<CMC IP address>

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

d. Select SLOT-N from the list on the left, where “N” is the slot of the blade being configured.



e. Select “Launch Remote Console” on the upper right. A new command-line window opens.

f. When asked whether you want to continue, enter **yes**.

g. Press any key to view the subscription agreement.

h. Enter **yes** to accept the subscription agreement, and then enter **yes** to begin firstboot.

i. Follow the on-screen instructions. See *Run firstboot*, page 23 for details.

9. Restore the backed-up configuration via the Security Blade Manager.
   a. Using a Web browser, log on to the Security Blade Manager
      `http://<C interface IP address>`
   b. Go to **Administration** > **Backup Utility**.
   c. Choose **Restore**.
10. Select **Full Blade Configuration** restore mode and click **Run Restore Wizard**.
11. In the Restore Wizard:
    a. File Location: Select **Another location (browse for file)**. Then click **Next**.
    b. Select File: **Browse** to the backup file (*.bak file) to select it. Then click **Next**.
    c. Confirm: Verify backup file details and then click **Restore Now**.

       The security blade will be rebooted automatically after the restore is complete. Security blade and software module settings are restored.
12. Ensure that the security blade time and date are synchronized with other servers.
13. Restart the Websense components that run off the security blade.
14. On occasion, a manual download of the Websense Web Security Master Database should be initiated after a recovery. Do this in the TRITON Unified Security Center (Web Security module) if you receive a warning message about the Master Database.

Default Policies

Websense Web Security Gateway 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 Websense solution, the Default policy applies to everyone on the network. To customize the policy, use the TRITON - Web Security console and its embedded Help system.

4 Troubleshooting Tips for X10G Appliances

Tips for responding to X10G alerts and other warning messages are provided in this chapter. Additional tips are provided online in the Websense Solution Center, Customer Forums, and Technical Library.

X10G Switch configuration and recovery

X-Series switches A1 and A2 on the chassis connect the X10G security blades to your network. Continual communication from each security blade to the appropriate switches is essential to running the Websense security solution.

Switch A1 and A2 are configured differently. Thus, they are not interchangeable (without an assisted reset). If a switch cannot be recovered through the steps described below, please contact your Websense professional for assistance with a factory reset and pre-initialization.

- Switch A1 is used by *all blades* to communicate with the off-chassis TRITON console. It is also used by all blades running Content Gateway (proxy) to receive and send proxy traffic.
- Switch A2 is configured by default in **na** mode. Switch A2 is used by the Network Agent blade (if there is one configured in Slot 16), to communicate with the N interface that monitors all network traffic for bandwidth use, and filters non-HTTP and non-HTTPS traffic, such as streaming media.

Commands available from Security Blade Manager (blades 1 through 15) in a command-line interface (CLI) are:

CLI command	Description
switch A1 configure	Returns switch A1 to Websense factory settings
switch A2 configure na	Resets switch A2 to Websense factory settings and enables Network Agent interface N on switch A2.
switch A2 configure wcg	Resets switch A2 to Websense factory settings and disables network interface N. The Network Agent module is not enabled on the chassis.
switch A1 (A2) verify	Shows the current status of the switch, the service tag number, and other information.

Switch recovery techniques

Status messages from the switches, and the switch alerts that can appear on the console, are described below. Detailed recovery steps are provided for each situation.

Status messages

Non-standard configuration

This status indicates that the switch was configured by your Websense partner or Websense Technical Support professional in a special way, to accommodate your network.

- Typically, no action is required. The switch can operate in a non-standard configuration when properly provisioned.
- If you wish to return the switch to its standard configuration, use the CLI command: `switch A1 (A2) configure`.
- If this does not resolve the issue, check the switch firmware version. Switch firmware version must be version 4.1.1.9.
- If the issue persists, perform *Booting the switch to Dell settings* and then *Configuring the switch mode*.
- For additional assistance, please contact your Websense Support professional.

Alert messages

Connection to switch A1 (or A2) failed

1. Make certain that the switch hardware is fully seated in the chassis, and that the switch lever is latched. The switch indicator LED may be on, even if the switch is not fully seated. This is because the pins connecting the switch hardware into the chassis are of varying lengths, so that they connect in this sequence as you insert the switch: grounding pin; power pin; data lines.
2. Try to reach the switch via this CLI command: switch A1 (A2) verify.

3. It is possible that the switch is in the process of rebooting (to clear an error condition). Try again to verify the switch configuration in 5 minutes.
4. If you still cannot connect from the blade to the switch, or if you must replace a switch with a new switch that was not configured by a Websense team, then these recovery steps are required (can be accomplished with line console, telnet, or Web UI). Your Websense professional can guide you through these steps.
    a. Unplug the network cables.
    b. Perform *Booting the switch to Dell settings*.
    c. Perform *Configuring the switch mode*.
    d. Plug in the network cables.

Switch A1 (A2) logon was not successful

1. You may not have used the current switch password. Verify the current password at your site and enter it again.
2. To change the password when you do not know the old one, request assistance from your Websense professional:
    a. Unplug the network cables.
    b. Perform *Booting the switch to Dell settings*.
    c. Perform *Configuring the switch mode*.
    d. Plug in the network cables.

Installing a new switch

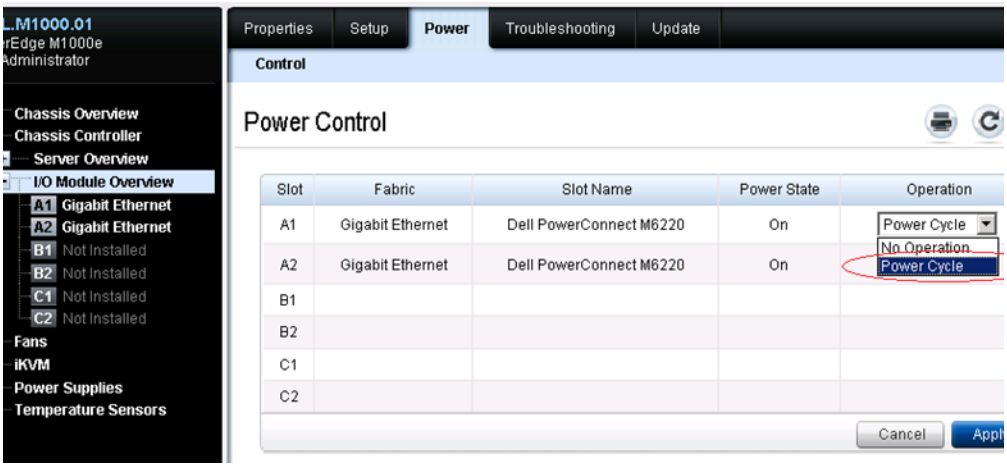
If you must replace a switch with a new one that has not been set up by a Websense team, insert the switch and latch it. Do not cable it. Then follow these steps:

a. Perform *Booting the switch to Dell settings*.
b. Perform *Configuring the switch mode*.
c. Plug in the network cables.

Booting the switch to Dell settings

Connect to the line console with a serial cable.

1. Log on to the CMC and choose **I/O Module Overview** at the left. Select the appropriate switch and then initiate a **Power Cycle**, as shown below:



2. Wait for the Boot Menu to appear on the console, and then choose:
   `2 - Start Boot Menu`
3. From the list of options that appears, choose:
   `10 - Restore configuration to factory defaults (delete config files)`
4. Wait for the console prompt to appear: **`console>`**
5. Copy and paste the following configuration commands into the console for switch A2 (all commands also apply to switch A1, but IP address [line 6] for switch A1 is **169.254.253.1**):

```
enable
configure
vlan 4003
exit
interface vlan 4003
ip address 169.254.253.2 255.255.255.0
exit
interface range gigabitethernet 1/0/1-16
switchport mode general
switchport general allowed vlan add 4003 tagged
exit
enable password websense
username root password websense
exit
write
y
exit
```

6. Remember to configure the switch mode. (See *Configuring the switch mode*.)

Configuring the switch mode

1. Unplug the network cables from the switch, if not already done.
2. On any blade except blade 16, to configure switch A1: Run the CLI command "`switch A1 configure`" in Security Blade Manager. This configures switch A1 for use with all X10G blade servers.
3. On any blade except blade 16, to configure switch A2: Choose a mode for Switch A2 in the Security Blade Manager:
   - Run the CLI command "`switch A2 configure wcg`" to configure switch A2 to support failover for proxy interfaces on blade 16. (This disables the N interface, used if Network Agent runs on blade in Slot 16.)
   - Run "`switch A2 configure na`" to configure switch A2 with the N interface for Network Agent supported (default setting).
4. Wait for the switch to finish rebooting, then run "`switch A1 (A2) verify`" to verify that the configuration is as expected.
5. Plug in the network cables for appropriate interfaces C/N/P1/P2 on the switch.

How to know if a blade in Slot 16 runs Network Agent

In the Security Blade Manager console for the blade in slot 16, under **Configuration > Network Interfaces,** if you see the Network Agent Interface (N) option displayed, then the blade was configured during firstboot to use Network Agent.