Getting Started

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

v7.8.x

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

Published 2014 Revision C
Printed in the United States and Ireland

R280514783

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, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc., 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

Websense is a registered trademark and TRITON is a trademark of Websense, Inc., in the United States and certain international markets. Websense 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.

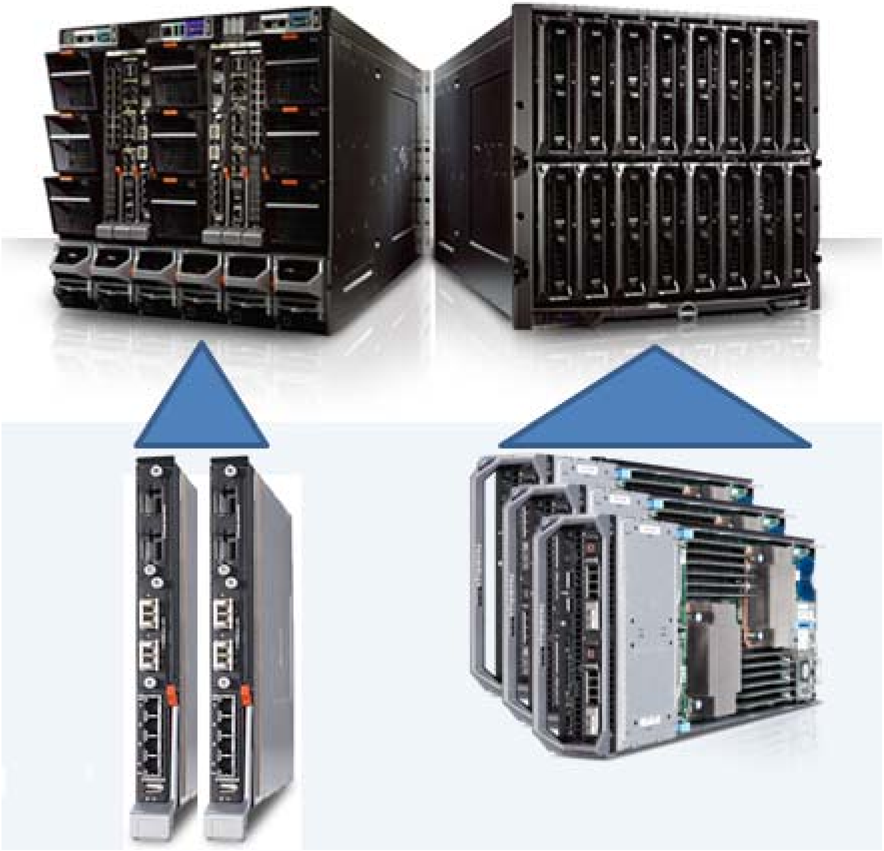
Contents

1 Hardware Setup for the X-Series Modular Chassis

The 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 managing 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.

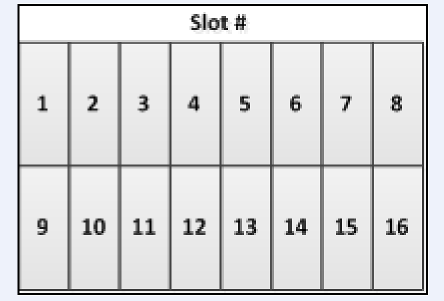
- Unpack and rack the chassis before you insert the security blades. Save the handled cardboard lifter, if a future chassis move is likely.
- Security blades are packaged separately. After installation, blades are imaged with the Websense software you ordered as described later in this guide.
- A few Websense components are Windows-only and must be installed and run off the chassis. The installer for these components is named **WebsenseTRITON783Setup.exe**. This installer is located on the Downloads page at www.websense.com.

X10G Quick Start poster

The Websense **X10G Quick Start Poster**, included in the chassis shipping box and also available on Websense.com here, 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 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.

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.

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`
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)).

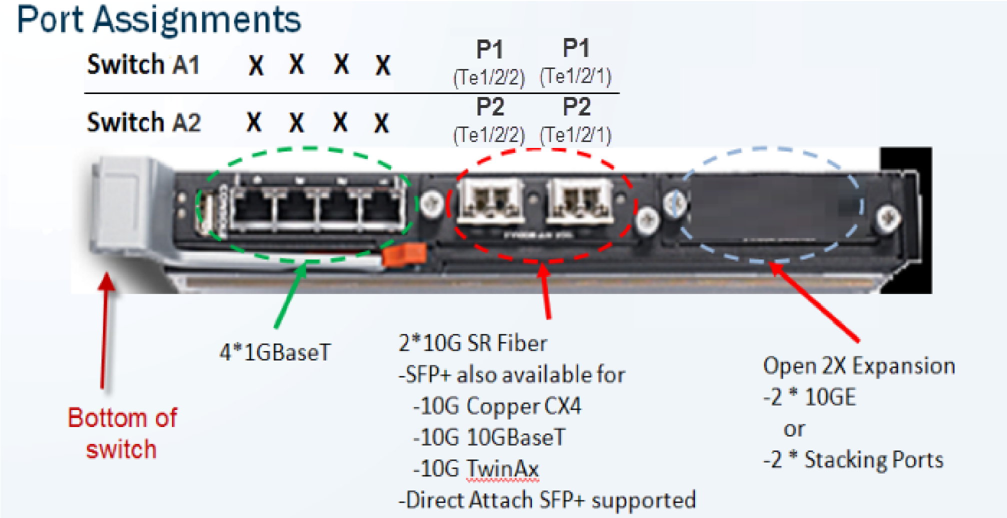
Here is an example for a fully provisioned X10G:

- IP address of CMC might be: `10.8.0.100`
- IP address range (remote access) for 16 blade iDRACs: `10.8.0.101 - 10.008.0.116`
- 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

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

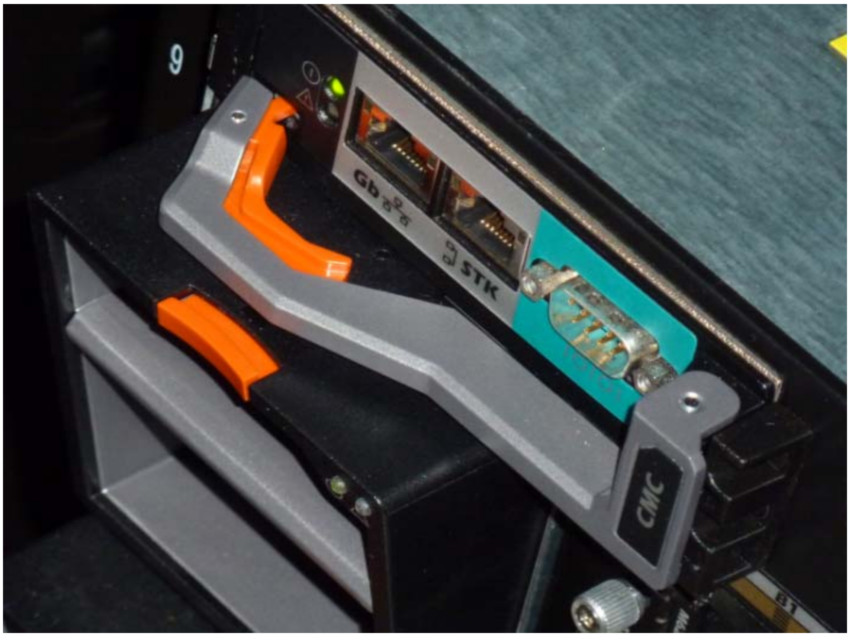
1. Note that the 2 on-chassis switches are oriented vertically at the back of the chassis. The switch on the left side is switch A1. The bottom of the switch is shown at the left in the diagram below. Use an SFP+ cable to connect the P1 interface on chassis switch A1 (left switch) to your network, or 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, 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. The 1GBaseT ports are not supported at this time. For more information, see *Switch configuration essentials*, page 27.

2. Connect a Category 5 network cable (do not use a crossover cable) from the left-most 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. 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.

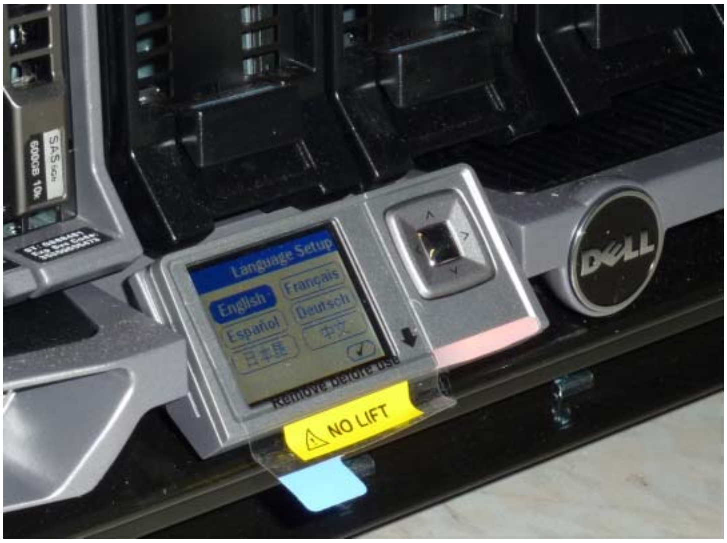
Set up the CMC IP Address

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

LCD Prompt	Recommended response
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.

   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 (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.

Note that the software modules running on the X10G are at version 7.8.3 and are compatible with off-chassis modules at that version.

Big picture

This section discusses Websense Web Security Gateway / Anywhere deployment essentials for the X10G. See Web Security Deployment Recommendations and Web Security core components in the Websense Technical Library for comprehensive information. Work with your Websense solutions partner to qualify your plan before beginning your deployment.

Two components that require attention are:

1. Policy Broker/Policy Database (*policy source*), discussed below
2. An instance of Microsoft SQL Server 2008 or 2012 *installed and running* off-chassis to support the Websense reporting database (discussed below)

TRITON unified installer

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

The installer for off-chassis components to be hosted on a Windows server is: **WebsenseTRITON783Setup.exe**

The installer for off-chassis components to be hosted on a Linux server is: **WebsenseWeb783Setup_Lnx.tar.gz**

To download the installers:

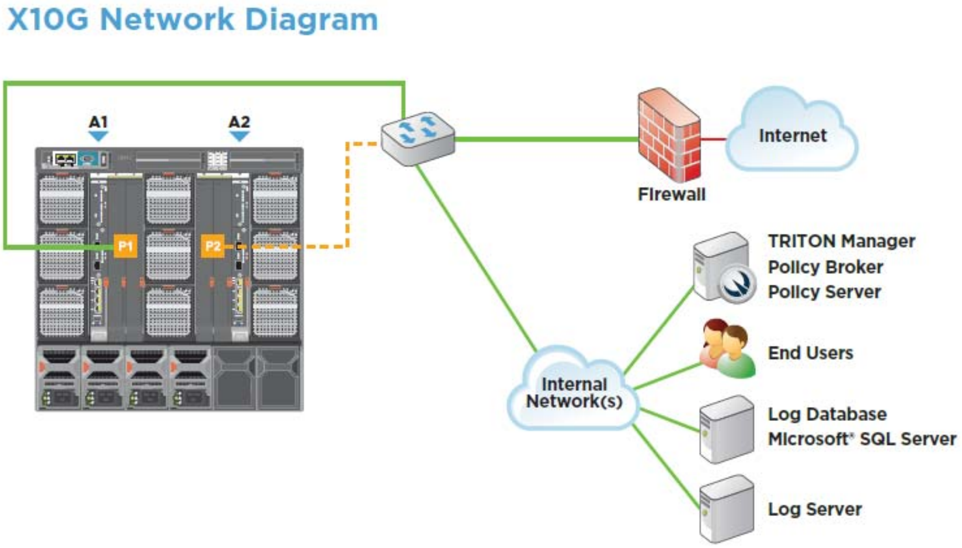
1. Go to mywebsense.com and log in to your account. If you don’t have an account, create one and then contact Websense Technical Support to link your account to your Web Security Gateway / Anywhere subscription key.
2. Click the **Downloads** tab.
3. Under **Download Product Installers**, select your Product and Version 7.8.3. 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.

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 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. The policy source server must be installed, configured, and running before other blades are configured (run the *firstboot* script). In this configuration, policy source replication is not supported.



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. Choose your policy source machine before running the firstboot script on any blade servers.

   If your policy source will be located off-chassis, you will need to install Websense 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 boot 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 Websense TRITON installer version 7.8.3 for installing off-chassis components.
5. Run firstboot and then complete the configuration for all other blades that will run Websense 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 Unified Security Center installation option and mark the Web Security check box.
8. Use the Custom installation option to install the Web Security Log Server off the chassis.

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 security 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 other security components) it runs two Websense components that do not run on any other server or blade: Websense **Policy Database** and **Policy Broker**. (If policy source is located off-chassis, you can configure replicated policy source servers. See Managing Policy Broker Replication.) 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 Websense web security components need up-to-date policy information obtained from the single *policy source* machine.

Following is a brief description of the key Websense 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. Also review the release notes for the version of the Websense security solution you will be using.

Security components

The table below describes Websense Web Security core components.

Installation is simplified by the security blade firstboot procedure, in combination with planning and installation of off-chassis components, as described in *Policy source*, page 11.

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 identification and filtering mode* (selected during firstboot) or *Filtering only mode* (selected during firstboot).

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

Component	Description
Policy Database	Stores Websense software settings and policy information. Installed automatically with Policy Broker. Runs on *policy source* machine only. Typically installed on Windows server off-chassis.
Policy Broker	Manages requests from Websense 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 blade. Primary copy runs on *policy source* machine. • 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 handling Internet requests. Configure Policy Server settings in the 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 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 Websense Master Database. Configure security policies and Filtering Service behavior in the Web Security console.
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 90 categories and subcategories • Contains more than 100 non-HTTP protocol definitions for use in managing protocols After all modules are set up, download the Websense Master Database to activate Internet management, and schedule automatic updates. If the Master Database is more than 2 weeks old, no traffic management occurs.
Web Security manager	Runs off-chassis on a Windows server. Serves as the configuration, management, and reporting interface for Websense software. Use the Web Security console to define and customize Internet access policies, configure Websense software components, report on Internet activity, and more. The Web Security console is made up of the following services: • Websense Web Security • Websense Web Reporting Tools • Websense Explorer Report Scheduler • Websense Information Service for Explorer • Websense Reporter Scheduler • Websense 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.

Component	Description
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. • 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 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.

Understanding the Policy Database

Websense Policy Database stores both policy data (including clients, filters, security components, and delegated administration settings) and global settings configured in the 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 X10G 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 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 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 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

Blades that install Websense Web Security Gateway / Anywhere version 7.8.x have the following core components:

- Policy Server
- Filtering Service
- User Service
- Usage Monitor
- Control Service
- Directory Agent (for sites using hybrid web security)
- Content Gateway (web proxy)

Software that runs off-chassis

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

Use the TRITON installer v7.8.3 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 (on its own 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

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: Web Security, Data Security, and 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.

You must install TRITON Unified Security Center on a Windows Server 2012 or 2008 R2 (64-bit) machine. TRITON Unified Security Center must be able to reach each blade's P1 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)

Web Security console

The Web Security console is used to perform general configuration tasks, set up security policies, assign policies to users and groups, run reports, and other management tasks.

Web Security services include:

- Websense Web Security
- Websense Web Reporting Tools

- Investigative Reports Scheduler
- Reports Information Service
- Websense RTM Client
- Websense RTM Database
- Websense RTM Server

Database management software

Websense Web Security products (and optional 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 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 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.

3 Setting Up Websense X10G Security Blades

Important

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 10 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, plan your deployment, and 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.
3. Install off-chassis components, as described in *Software that runs off-chassis*, page 16.

Blade installation and configuration summary:

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

1. Power on each blade.
2. *Run firstboot*, page 20.
3. Perform *Additional Security Blade configuration*, page 22.

Off-chassis components require installation and configuration. See *Software that runs off-chassis*, page 16 and the Deployment and Installation Center in the Websense Technical Library for more information.

Run firstboot

Security blades are delivered ready to run the **firstboot** script, which completes the software installation (Web Security Gateway or Web Security Gateway Anywhere) and establishes basic Security Blade configuration.

The firstboot script prompts you to:

- 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 *Choosing a policy source machine*, page 12.
- 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 policy mode of the blade without first re-imaging it. See *Restoring to Factory Image*, page 33 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: bladeserver1.example.com)	
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 also handle traffic to and from the Content Gateway proxy. See *Network interface P2*, page 23. 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)	
Primary DNS server for P1 and all active network interfaces on the Security Blade (IP address)	

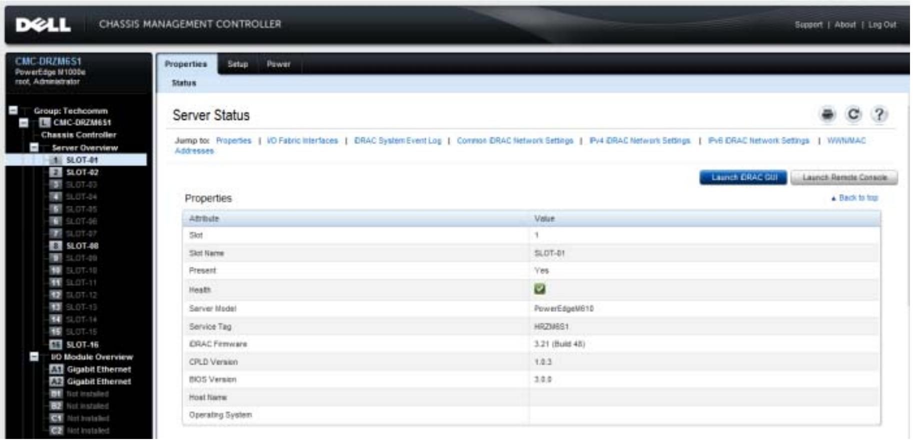
Unified password (8 to 15 characters, at least 1 letter and 1 number) This password is used for this blade, and for the following: ◆ Security Blade command-line interface (CLI) ◆ Content Gateway manager Some sites use the same password for all blades. This choice is yours.	
Send usage statistics?	Usage statistics from Security Blade modules can optionally be sent to Websense servers, to help improve the accuracy of 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. If the policy source machine will be a blade server, configure it first.



Server Status

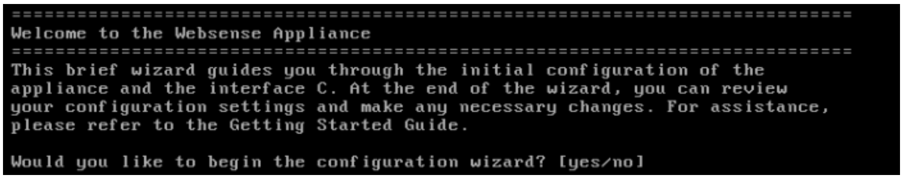
Properties

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 Websense Appliance
===========================================================================
This brief wizard guides you through the initial configuration of the
appliance and the interface C. 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 v7.8.x CLI guide.

To complete Security Blade configuration:

- Optionally, *Enable SSH access to the command-line interface*, page 23
- Optionally, enable *Network interface P2*, page 23
- Optionally, configure *Static routes*, page 25
- Confirm *Switch configuration essentials*, page 27

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, configure Websense Web Security Gateway / Anywhere software. See Web Security 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 then 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 Internet traffic that is routed to the Content Gateway proxy.

Secondary network interface P2 (eth1) is disabled by default, but can be enabled for use by Content Gateway.

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:

To configure P2:

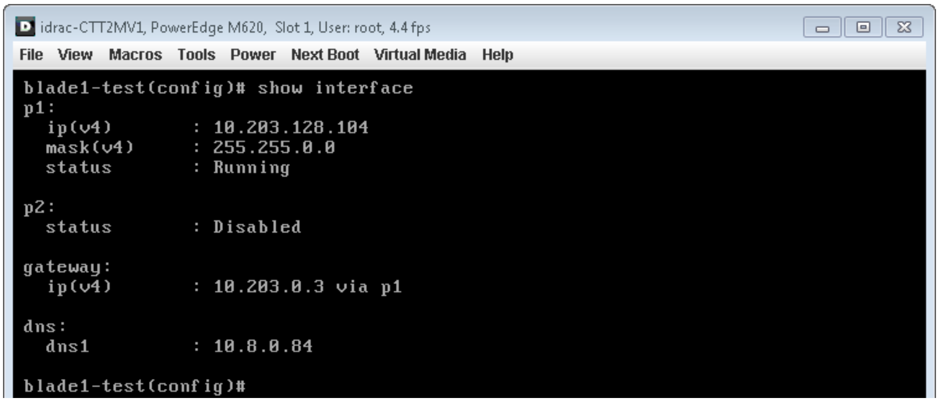
1. Access the Security Blade using its iDRAC.

   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 (or the config password, if you established a separate password).
5. Check the status of the P1 and P2 network interfaces:

   ```
   show interface
   ```


idrac-CTT2MV1, PowerEdge M620, Slot 1, User: root, 4.4 fps
File View Macros Tools Power Next Boot Virtual Media Help

```
blade1-test(config)# show interface
p1:
  ip(v4)        : 10.203.128.104
  mask(v4)      : 255.255.0.0
  status        : Running

p2:
  status        : Disabled

gateway:
  ip(v4)        : 10.203.0.3 via p1

dns:
  dns1          : 10.8.0.84

blade1-test(config)#
```

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. Keep this in mind when you configure Content Gateway.

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

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 25.

Static routes

You can define static routes if needed. Route configuration is described in detail in the X-Series v7.8.x CLI guide.

Route configuration is performed in the CLI. IPv4 and IPv6 address routing is supported. For basic information, in the CLI enter **help set route**, **help set route6**, **help load route**, and **help load route6**.

Load route/route6 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 allows you to define one static route at a time.

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

```
set route --dest <ip_address> --interface <p1 | p2>
          --mask <netmask> --gateway <ip_address>
```

✓ **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**.

The usage is (IPv4):

```
delete route --dest <ip_address> --interface <p1 | p2>
             --mask <netmask> --gateway <ip_address>
```

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

Switch configuration essentials

Switches A1 and A2 arrive with the following default configuration:

Switch A1

P1 Te1/2/1	**Enabled** 10 gigabit 1518 maximum frame size (configurable) Full duplex Auto negotiation disabled Flow control disabled
P1 Te1/2/2	**Disabled** 10 gigabit 1518 maximum frame size (configurable) Full duplex Auto negotiation disabled Flow control disabled
Other ports are not supported.	

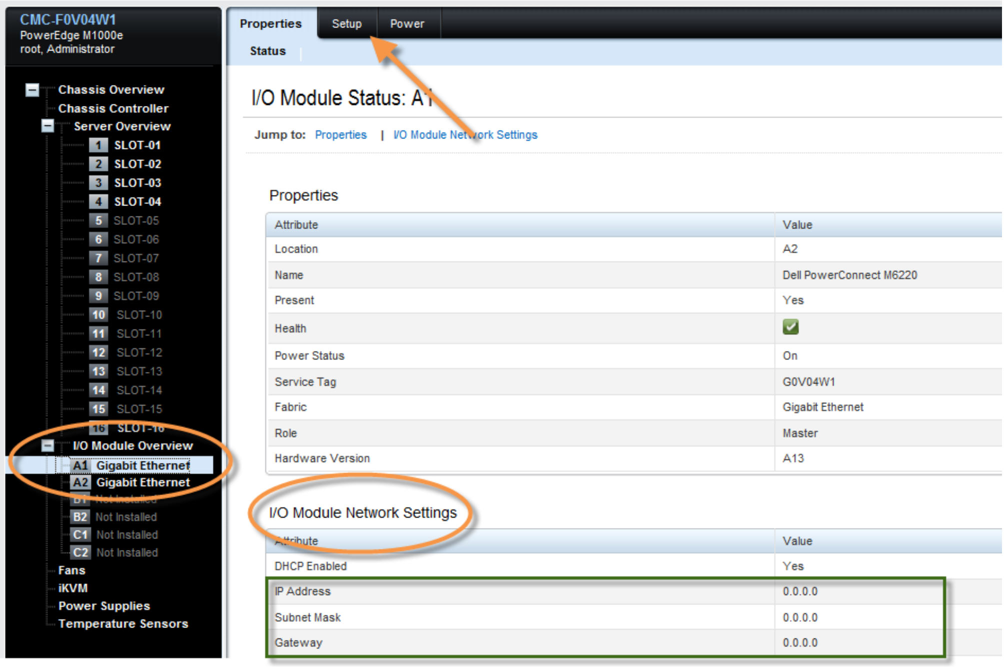
Switch A2

P2 Te1/2/1	**Enabled** 10 gigabit 1518 maximum frame size (configurable) Full duplex Auto negotiation disabled Flow control disabled
P2 Te1/2/2	**Disabled** 10 gigabit 1518 maximum frame size (configurable) Full duplex Auto negotiation disabled Flow control disabled
Other ports are not supported.	

Assign switch I/O modules an IP address

Switches A1 and A2 are accessed through the CMC. Before they can be accessed, each must be assigned an IP address. To assign an IP address:

1. Log on to the CMC and go to **Chassis Overview > I/O Module Overview > A1 Gigabit Ethernet** (or A2).



I/O Module Status: A1

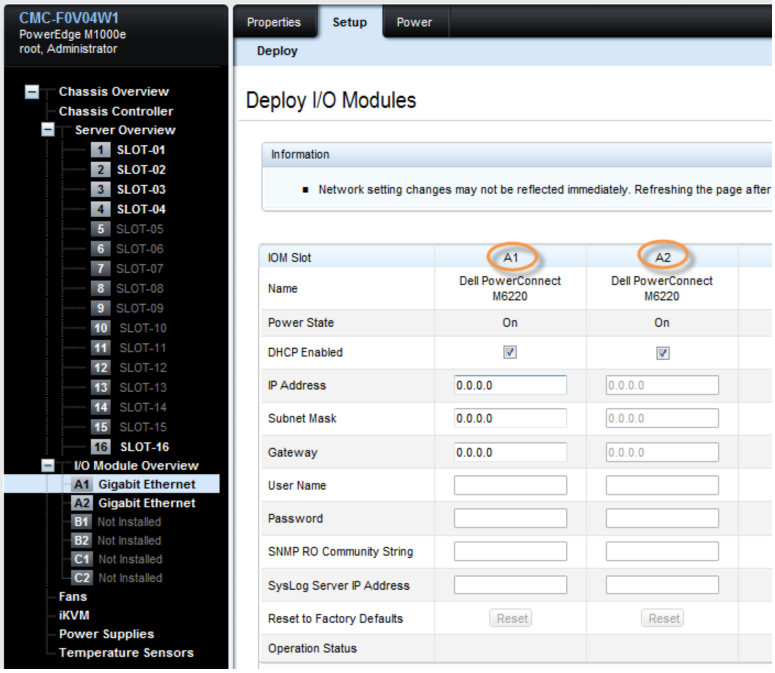
Properties

Attribute	Value
Location	A2
Name	Dell PowerConnect M6220
Present	Yes
Health	✓
Power Status	On
Service Tag	G0V04W1
Fabric	Gigabit Ethernet
Role	Master
Hardware Version	A13

I/O Module Network Settings

Attribute	Value
DHCP Enabled	Yes
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0

2. Click the **Setup** tab.



Deploy I/O Modules

Information

- Network setting changes may not be reflected immediately. Refreshing the page after

IOM Slot	A1	A2
Name	Dell PowerConnect M6220	Dell PowerConnect M6220
Power State	On	On
DHCP Enabled	☑	☑
IP Address	0.0.0.0	0.0.0.0
Subnet Mask	0.0.0.0	0.0.0.0
Gateway	0.0.0.0	0.0.0.0
User Name		
Password		
SNMP RO Community String		
SysLog Server IP Address		
Reset to Factory Defaults	Reset	Reset
Operation Status		

3. For each of A1 and A2, uncheck **DHCP Enabled**, and enter an IP address, subnet mask, and gateway. The IP addresses must be unique.
4. Establish a User Name and Password that meets your organization's security standards. The factory default credentials are:
   User Name = root Password = calvin
5. Click **Apply**. It takes a minute or 2 for the settings to be applied.

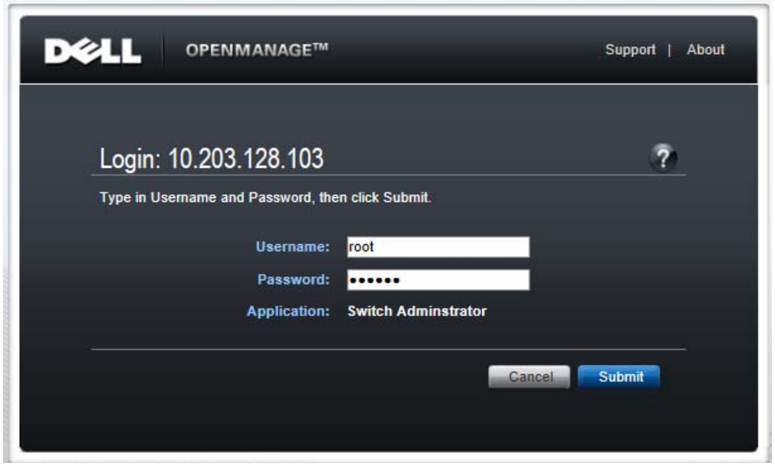
To access a switch, go to **Chassis Overview > I/O Module Overview** and click the **Launch IOM GUI** button corresponding to the switch you want to access.

Enabling and disabling ports

To enable or disable a port:

1. Log on to the CMC, go to **I/O Module Overview**, and click the **Launch IOM GUI** button for switch A1 or A2.

   If the button isn't available, it's because an IP address has not been configured. See *Assign switch I/O modules an IP address*.
2. A logon window displays. Log on.



Login: 10.203.128.103

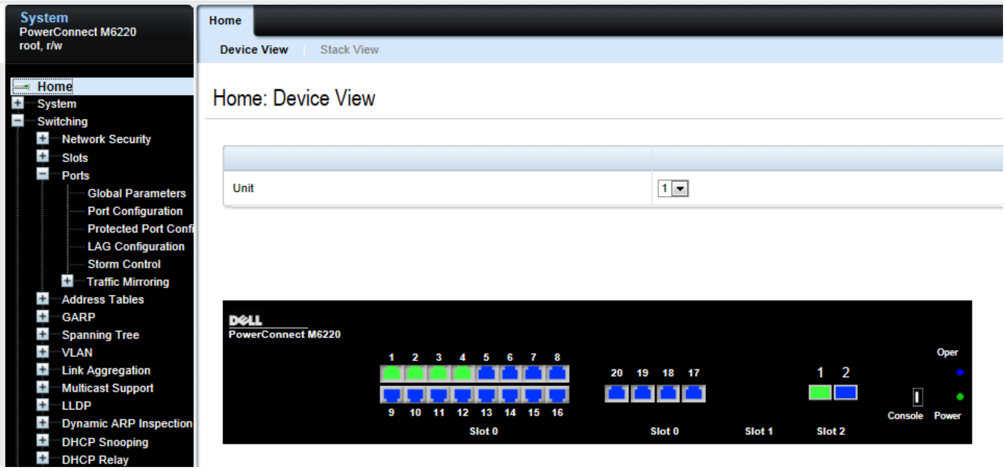
Type in Username and Password, then click Submit.

Username: root

Password: ••••••

Application: Switch Adminstrator

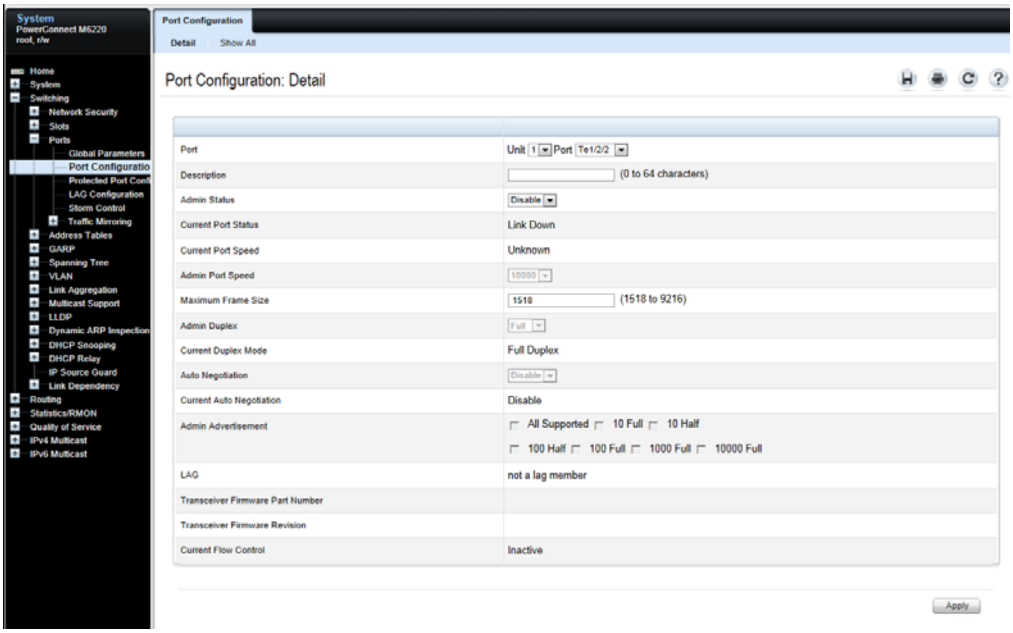
The home screen shows the status of all ports on the switch. A green port is up (enabled), a blue port is down (disabled).



Home: Device View

Unit	1

3. To enable or disable a port, click on the green or blue area of the port. This opens the **Port Configuration: Detail** page.



Port Configuration: Detail

Port	Unit 1 Port Te1/2/2
Description	(0 to 64 characters)
Admin Status	Disable
Current Port Status	Link Down
Current Port Speed	Unknown
Admin Port Speed	10000
Maximum Frame Size	1518 (1518 to 9216)
Admin Duplex	Full
Current Duplex Mode	Full Duplex
Auto Negotiation	Disable
Current Auto Negotiation	Disable
Admin Advertisement	□ All Supported □ 10 Full □ 10 Half □ 100 Half □ 100 Full □ 1000 Full □ 10000 Full
LAG	not a lag member
Transceiver Firmware Part Number	
Transceiver Firmware Revision	
Current Flow Control	Inactive

a. Confirm that the **Port** selection is correct. Change to another port if desired.

b. Add a description if desired.

c. Select **Enable** or **Disable** from the **Admin Status** drop down. This determines if the port is enabled or disabled.

d. Examine and adjust other settings as needed and click **Apply**.

IMPORTANT: The UI may initially indicate that the settings reverted to the previous values. Wait 2 or 3 minutes for the configuration action to complete and then refresh the page. The configuration action takes longer to complete than expected.

High availability

Both switches A1 and A2 have two 10 gigabit ports (Te1/2/1 and Te1/2/2). When both are enabled and connected to an upstream switch, they can be configured for high availability, either active standby or link aggregation.

Active standby (by layer 2 negotiation)

In active standby, the primary port (Te1/2/1) handles all traffic until it suffers a failure, at which time the secondary port assumes all traffic until the primary port is restored. The ports are monitored by a periodic STP calculation.

To configure active standby on the A1 or A2 switch:

1. Ensure that both Te1/2/1 and Te1/2/2 are enabled.
2. Perform these commands in console mode:

   ```
   interface Te1/2/1

   duplex full

   switchport access vlan 1

   exit

   interface Te1/2/2

   duplex full

   switchport access vlan 1

   exit
   ```

3. On the upstream switch:

   a. Enable the 10 gigabit ports.

   b. Configure each according to your VLAN allocation:

      ```
      switchport access vlan <n>
      ```

Load balancing by link aggregation

In link aggregation, both ports are active and share the load. If one port fails, the remaining port assumes all of the load.

Requirement: The upstream connections must be on the same switch or to switches in the same stack.

To configure link aggregation on the A1 or A2 switch:

1. Ensure that both Te1/2/1 and Te1/2/2 are enabled.

2. Perform these commands in console mode:

```
interface Te1/2/1

duplex full

channel-group 1 mode active

switchport access vlan 1

exit

!

interface Te1/2/2

duplex full

channel-group 1 mode active

switchport access vlan 1

exit

!

interface port-channel 1

switchport access vlan 1

exit
```

3. On the upstream switch:
   a. Enable the 10 gigabit ports.
   b. Configure link aggregation. See your switch documentation.
   c. Configure each according to your VLAN allocation:

      ```
      switchport access vlan <n>
      ```

   Some older switches require that the VLAN info be configured on both the physical ports and the link-aggregation port.

   Some newer switches require VLAN configuration on link-aggregation port only.

   Refer to your switch documentation.

Important

“switchport access vlan 1” is the default configuration in Dell M6220 switches. It does **not** appear in the startup or running configuration scripts.

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 that 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.

To reset the blade to the factory image:

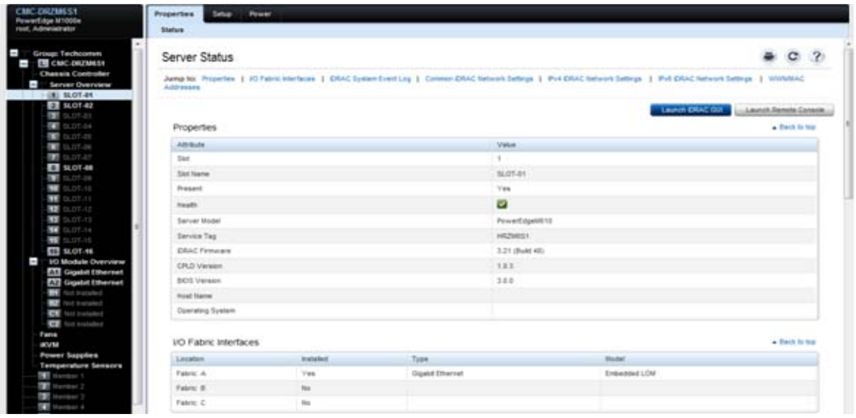
1. Stop all Websense components that are running off the chassis. For example, stop Web Security Policy Broker, Log Server, Sync Service, Linking Service, transparent ID agents, and TRITON Unified Security Center. This is essential.
2. If possible, back up any information on the blade that you want preserved.
    a. Access the Security Blade CLI with SSH, if enabled, or through the Security Blade iDRAC.
    b. In the CLI, use the **create backup** command to create a full backup. Enter **help create backup now** for help.

       Save the backup file to another machine.
3. Plug a portable DVD drive into the blade’s USB port (front of blade) and insert the recovery disk into the drive.
4. Reboot the blade:
    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 reimaged.



Server Status

Properties

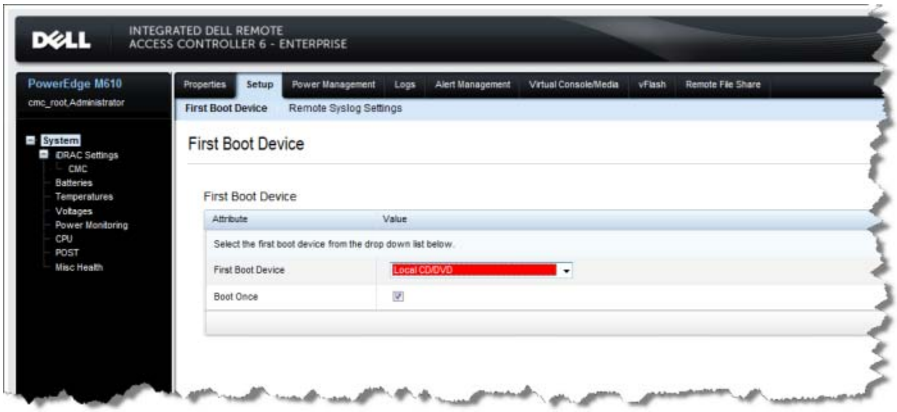
Attribute	Value
Slot	1
Slot Name	SLOT-01
Present	Yes
Health	✓
Server Model	PowerEdgeM610
Service Tag	HRZM6S1
iDRAC Firmware	3.21 (Build 40)
CPLD Version	1.0.3
BIOS Version	3.0.0
Host Name	
Operating System	

I/O Fabric Interfaces

Location	Installed	Type	Model
Fabric A	Yes	Gigabit Ethernet	Embedded LOM
Fabric B	No		
Fabric C	No		

5. Select “Launch iDRAC GUI” at the right.

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

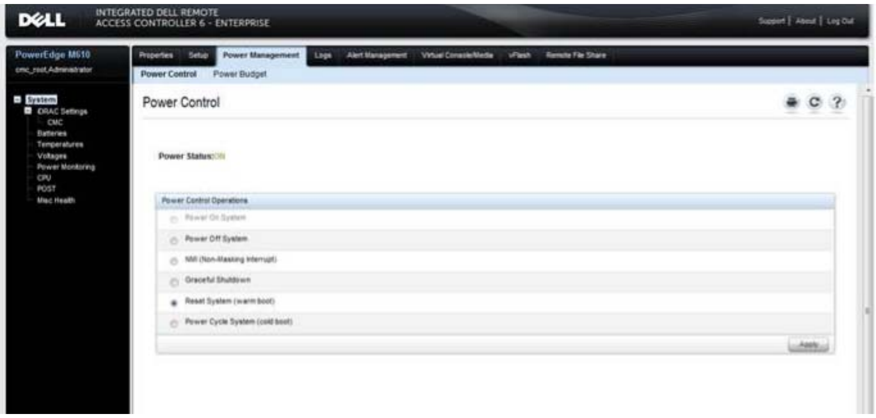


First Boot Device

First Boot Device

Attribute	Value
Select the first boot device from the drop down list below.	
First Boot Device	Local CD/DVD
Boot Once	☑

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



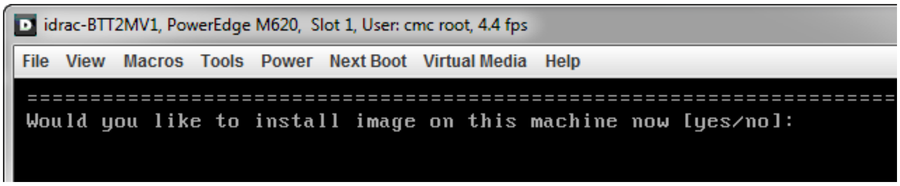
Power Control

Power Status:ON

Power Control Operations

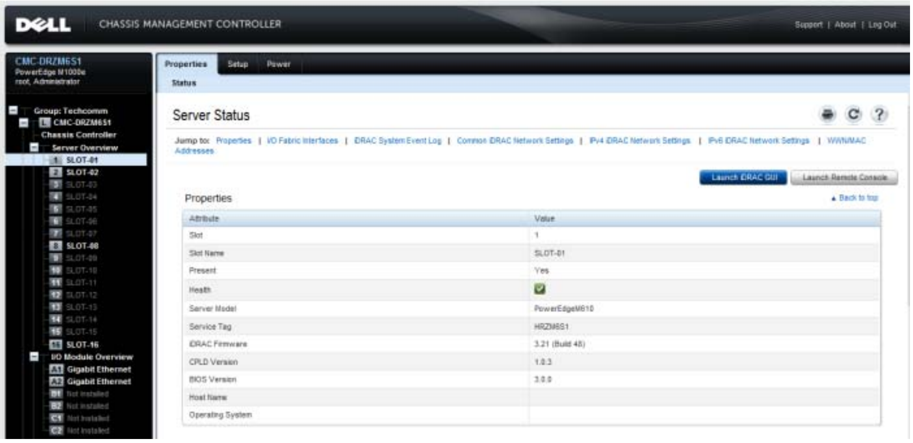
- ○ Power On System
- ○ Power Off System
- ○ NMI (Non-Masking Interrupt)
- ○ Graceful Shutdown
- ● Reset System (warm boot)
- ○ Power Cycle System (cold boot)

8. The blade proceeds to reboot and pauses during the load from DVD, prompting for confirmation that you want to reimage the blade. If you want to reimage the blade, respond **yes**.


idrac-BTT2MV1, PowerEdge M620, Slot 1, User: cmc root, 4.4 fps
File
View
Macros
Tools
Power
Next Boot
Virtual Media
Help

```
===================================================================
Would you like to install image on this machine now [yes/no]:
```

9. After the reboot has completed, run the firstboot script to establish the initial configuration. 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>
   c. Replace <CMC IP address> with the address assigned to the CMC during initial configuration of the chassis.
   d. Log on to the CMC console.
   e. Select SLOT-*N* from the list on the left, where “N” is the slot of the blade being configured.



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	

   f. Select “Launch Remote Console” on the upper right. A new command-line window opens.
   g. When asked whether you want to continue, enter **yes**.
   h. Press any key to view the subscription agreement.
   i. Enter **yes** to accept the subscription agreement, and then enter **yes** to begin firstboot.
   j. Follow the on-screen instructions. See *Run firstboot*, page 20 for details.

   When the process is complete you are logged on to the Security Blade CLI in ‘view’ context. To continue to restore your backed-up configuration, do not exit the CLI.

10. Restore the backed-up configuration via the Security Blade CLI.
   a. In the CLI, enter ‘config’ mode. Use the password you set during firstboot.

   b. Use the **restore backup** command to restore the full backup you made prior to reimaging the blade. Enter **help restore backup** for online help.

11. Ensure that the Security Blade time and date are synchronized with other servers.
12. Restart the Websense components that run off the Security Blade.
13. 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 Web Security console and its embedded Help system.

4 X10G Switch Access and Recovery

X10G Switch access and recovery

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

X10G version 7.8.x switch firmware is version 5.1.2.3.

By default, switches A1 and A2 are configured identically. Ports A1.P1-Te1/2/1 and A2.P2-Te1/2/1 are enabled by default. Ports A1.P1-Te1/2/2 and A2.P2-Te1/2/2 are disabled by default. For information about enabling them and configuring them for high availability or VLAN, see *Switch configuration essentials*, page 27.

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.

Installing a new switch

If you must replace a switch:

1. Contact Websense Technical Support for assistance.
2. Review *Switch configuration essentials*, page 27.
3. When replacing the switch make certain that it is fully seated in the chassis, and that the switch lever is latched.
4. Ask the Technical Support specialist to demonstrate that the new switch is functioning properly, per your switch configuration requirements.

Accessing a switch

To access switch A1 or A2:

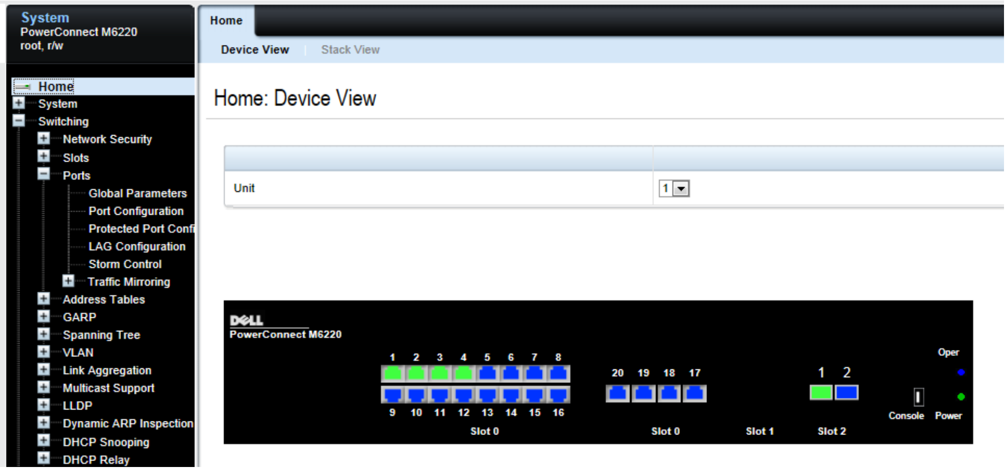
1. Log on to the CMC, go to **I/O Module Overview**, and click the **Launch IOM GUI** button for switch A1 or switch A2.

   If the button isn't available, it's because an IP address has not been configured. See *Assign switch I/O modules an IP address*, page 28.

2. A logon window displays. Log on. The Dell default credentials are: Username 'root', password 'calvin'. Change these to comply with your organization's security policies.

   The switch home screen shows the status of all ports on the switch. A green port is up (enabled), a blue port is down (disabled).

3. Click on a port to go to its configuration page.



Proceed with your desired configuration changes.

For additional Websense guides for the X10G Chassis and Security Blades, please visit the X10G support page.