

READ FIRST!

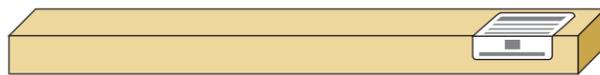
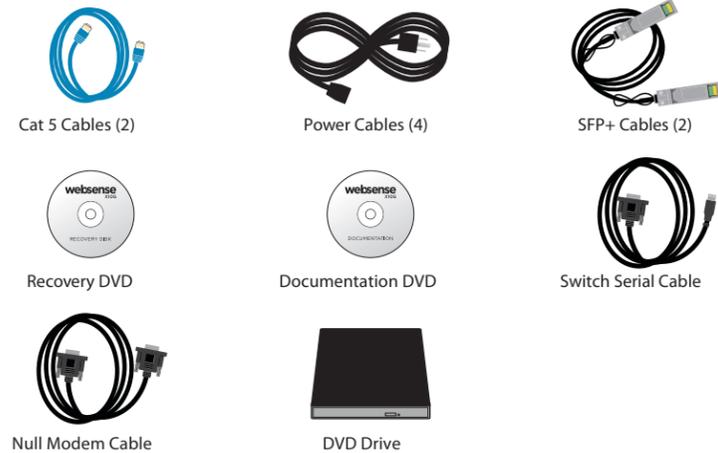
Websense® X10G™ Quick Start Poster This poster describes setup steps for the X10G chassis and blade system.

⚠ Before you begin

Plan your deployment before setting up the X10G. See the checklist and form included in the deployment kit emailed with the subscription key(s).

You can also access these at: <http://support.websense.com/x10g>

1 Verify Contents



Sliding Ready Rail Kit



Blades are in separate cartons

Contact Websense Technical Support if any items are missing.

2 Rack and Install

See the Rack Installation Instructions in the Sliding Ready Rail Kit.
Note: 4 persons required for racking chassis.

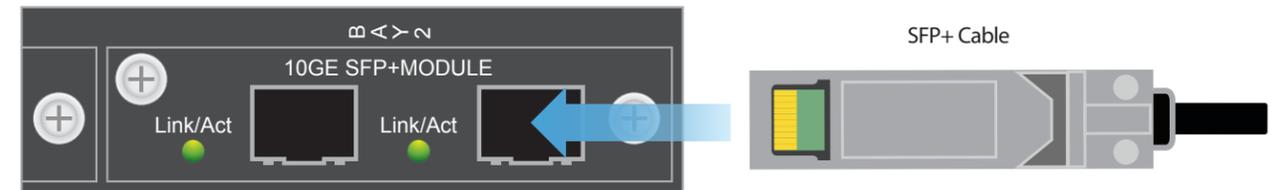
After the chassis has been racked, slide blades into the slots of the chassis starting in slot 1 (top left slot). If using Network Agent, slide one blade into slot 16.
Note: Blades slide smoothly when hanging from the top rail. Do not force.

3 Connect to Network

If you have an optical transceiver kit, follow the installation instructions in the kit and connect appropriate fiber optic cables. Otherwise, connect the SFP+ cable provided for P1 on switch A1. Then, connect all other desired appliance interfaces for each switch:

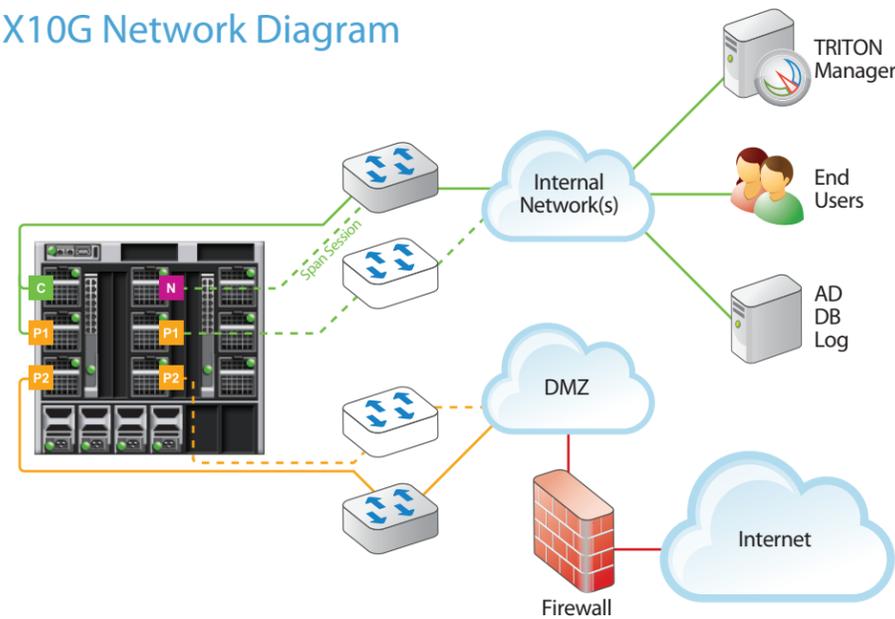
	Switch A1	Switch A2
Required Ports:	C P1	
Optional Ports:	P2	P1** P2** N*

*Required if using Network Agent (available only in slot 16)
**Required only for interface bonding



Interface	Connection Requirements	Function
C	<ul style="list-style-type: none"> Access to DNS server and Internet. Accessible by client computers and computers administering appliance. Use Cat 5 cables. 	<ul style="list-style-type: none"> Provides communication for security blade modules, block pages, Network Agent reset packets, and handles database downloads from the Internet. Receives connections from Websense® TRITON™ Unified Security Center.
P1	<ul style="list-style-type: none"> Access to DNS server and Internet. Connected to a different VLAN than P2. 	<ul style="list-style-type: none"> Enables Websense Content Gateway (proxy) to receive Internet requests and communicate with Web servers.
P2	<ul style="list-style-type: none"> Access to DNS server and Internet. Connected to a different VLAN than P1. 	<ul style="list-style-type: none"> Enables Websense Content Gateway (proxy) to receive Internet requests and communicate with Web servers.
N	<ul style="list-style-type: none"> Span, monitor, or mirror port on an external network switch. Has access to all client traffic. Use Cat 5 cables. 	<ul style="list-style-type: none"> Allows Network Agent to monitor all Internet requests. *Note: Can be enabled on the blade in slot 16 only.

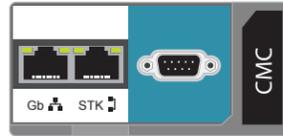
X10G Network Diagram



4 See back for steps to complete your setup

4 Connect Input Device

1. Connect 4 power cables to the 4 power supply units at the lower back of the chassis.
2. Connect a Cat 5 cable from the leftmost Chassis Management Controller (CMC) network port to a switch on the network for the CMC and iDRAC management IP addresses.



5 Power On Appliance

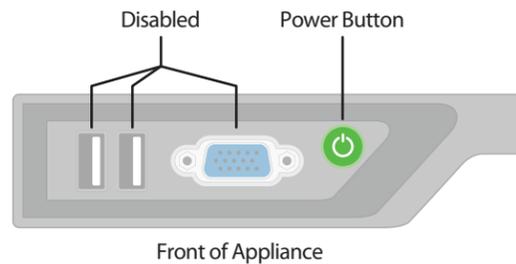
Power on the chassis at the front (lower left corner below slot), and check the following indicators:

Front:

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

Rear:

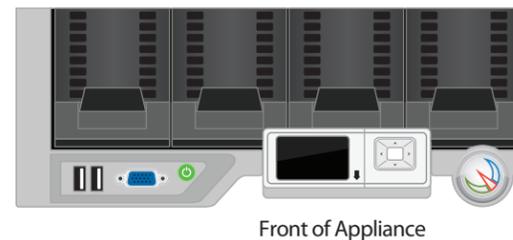
- Power supply LEDs are green.
- LEDs for both switches, the CMC, and all fans are green.
- LED behind power button is solid green.
- System status indicator (LED on front of LCD screen) is blinking orange.



6 Set CMC IP Address

Use chassis LCD to configure CMC.

1. Pull out LCD screen on front of chassis.
2. Select your language preference.
3. Configure the CMC? **YES**
4. Specify the network speed. **Auto (1g)**
5. Specify the protocol type. **IPv4**
6. IP addressing mode: **Static**
7. Enter the static IP address of the Chassis Management Controller.
8. Enter the subnet mask for this IP address.
9. Enter the default gateway for this IP address.
10. Confirm your IP address settings.
11. Specify if you want to register DNS. **NO**
12. Configure iDRACs? **NO**
13. Apply all enclosure settings? **YES**



Support and Resources

Websense® X-Series™ Getting Started Guide
www.websense.com/library/

Online Support and Contact Information
www.websense.com/support

7 Use Web Access to CMC

Retrieve your Pre-deployment Checklist and Reference Worksheet with your IP addresses listed.

1. From your client PC, point an Internet Explorer browser to the IP address of the Dell CMC.
2. Log on with username: root password: calvin
3. Select "Server Overview" > "Setup" tab.
4. Ensure "QuickDeploy..." checkbox is enabled.
5. Set "Starting iDRAC IPv4 Address (Slot 1)" of your assigned IP range for iDRACs.
6. Click "Save QuickDeploy Settings" button.
7. Click "Auto-Populate Using QuickDeploy Settings" button.
Note: Contiguous IP addresses are assigned consecutively to all 16 individual slots for iDRACs.
8. Click "Apply iDRAC Network Settings" button.
9. Select "Chassis Overview" in the left navigation > "User Authentication" tab.
10. Select User ID 1.
11. Change password. Click "Apply."

8 Access Firstboot Configuration

1. From CMC interface, select SLOT-1 and launch Remote Console.
2. Begin firstboot configuration wizard.
*Note: Refer to Reference Worksheet for IP address information.
3. Repeat for each security blade.

9 Configuration Overview

Below is an overview of remaining configuration steps for each blade. Please refer to the Getting Started Guide for more details.

Pre-Configuration

1. Download TRITON installer v7.7.1 from www.websense.com.
2. Configure and launch Microsoft SQL Server 2005/2008 off-chassis.
3. Set up Policy Source machine. See Getting Started Guide.
4. Install TRITON management console and Log Server off-chassis.

Initial Configuration

Security Blade Logon Portal: Access Logon Portal via browser to perform remaining tasks.

Security Blade Manager

- Configure NTP servers/system time.
- On blades not running Network Agent: configure P1/P2
- On the blade in slot 16, if running Network Agent: configure N
- Point to Policy Source machine.

TRITON - Web Security console (off-chassis): Enter subscription key, update Master URL Database, configure Network Agent, and customize policies. Requires Windows Server 2008 with TRITON Unified Security Center, Web Security Log Server and optional components.

Websense Content Manager: Configure authentication and select protocols.