Websense® Security Blade Manager

Websense X-Series™ Modular Chassis Family

Model: Websense X10G™

v7.7.1

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

Published 2012
Printed in the United States and Ireland

Trademarks

Contents

1 X-Series Overview

The Websense® X-Series™ modular chassis family includes the Websense X10G™ blade chassis and Websense X10G security blades, also referred to as appliances. The X10G chassis holds up to 16 security blades and runs Websense Web Security Gateway (Anywhere). Each blade analyzes and filters Web traffic in real time.

The mode in which each blade runs is determined during the execution of the firstboot script. Two choices are available in this release:

- Web Security Gateway with no Network Agent
- Web Security Gateway optimized for Network Agent

Network Agent, if used, always resides on the blade in slot 16.

See the *Getting Started Guide for Websense X-Series* for more information on the initial configuration process.

The Websense Web Security Gateway (Anywhere) solution:

- Instantly categorizes new sites and dynamic content, proactively discovering security risks, and blocking malware.
- Provides advanced analytics—including rules, signatures, heuristics, and application behaviors—to detect and block proxy avoidance, hacking sites, adult content, botnets, keyloggers, phishing attacks, spyware, and many other types of unsafe content.
- Closes a common security gap: decrypting and scanning SSL traffic before it enters the network.

These real-time capabilities on the X10G security blade integrate with industry-leading Websense Web Security software to provide Web filtering with over 90 default URL categories and control of more than 150 network protocols and applications.

- Software on the security blade can be linked with Websense Data Security solutions, to give data security software access to both Master Database URL categorization and user information collected by Websense Web filtering services.
- Software on the security blade can also be synchronized with Websense hybrid Web filtering, an on-demand, cloud-based service, to apply your organization's policies to off-site users, or to branch offices, remote campuses, and so on.

The TRITON - Unified Security Center, used to manage the Web Security software, is typically installed on a Windows Server machine off the security blade. You download

this software installation archive from the Websense Web site at www.mywebsense.com.

Note that Websense Email Security Gateway is available on the Websense V-Series™ appliance but is not currently available on X10G security blades.

X10G chassis security best practices

- Lock the chassis inside an IT closet or data center and enable a BIOS password. Physical access to the blade chassis and security blades can be a security risk for your network.
- Ensure that administrator credentials are restricted to a select few persons. This helps prevent unauthorized access to the system.
- Enable troubleshooting ports and permit remote access only when requested to do so by Websense Technical Support. Return these settings to the disabled state immediately after the Websense specialist logs off.

X10G security blade management consoles

Help | X-Series Appliance | Version 7.7.1

The Websense Security Blade Manager is the name of the management console for the X10G security blades. This is a graphical interface for configuring each security blade, checking the status of the software modules, updating passwords, troubleshooting, and applying patches to the blades.

Note that the Security Blade Manager differs from the Chassis Management Controller, which provides remote management capabilities and power control functions for hardware and software on the blade chassis.

Security Blade Manager provides status information about each module running on a security blade and enables you to establish assignments and routes for each blade's network interfaces.

Perform configuring tasks for the software module on each security blade (such as setting up users and defining and applying filtering policies) through the module's management console, as shown below.

Software module	Description	Console name
Websense Web Security	Uses policies to filter Internet requests from clients.	TRITON™ - Web Security*

Software module	Description	Console name
Network Agent (optional)	Internet traffic sniffer. Enforces filtering for non-HTTPS and non-HTTP protocols.	TRITON - Web Security
Websense Content Gateway	As the Web proxy component of Web Security Gateway, includes proxy software and advanced analytics.	Content Gateway Manager

*Part of the Websense TRITON Unified Security Center.

To launch Content Gateway Manager directly, go to:

```
https://<IP-address-of-interface-C>:8081/
```

To launch the TRITON Unified Security Center directly, go to:

```
https://<IP-address-of-TRITON-machine>:9443/triton/
```

When you log on to the TRITON console, you are taken to the Web module (TRITON - Web Security) by default.

To launch a combined Logon Portal that offers access to the Security Blade Manager and Content Gateway Manager, go to:

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

Security Blade Manager and the TRITON Unified Security Center support the following browsers:

- Microsoft Internet Explorer 8 and 9
  - Turn off Enhanced Security Configuration
  - With IE8, Compatibility View is not supported
- Mozilla Firefox 4.x and later
- Google Chrome 13 and later

Managing appliances in TRITON Unified Security Center

Help | X-Series Appliance | Version 7.7.1

The TRITON Unified Security Center (TRITON console) provides a facility for managing Websense appliances in your network. Appliances that are part of your TRITON installation are registered automatically on the TRITON console **Appliances** > **Manage Appliances** page. Information for each appliance includes:

- C interface IP address
- Host name
- Security Mode (Web Security)
- Policy source (Full, Limited, or Filtering Only)
- Software version (for example 7.7.1)

- Hardware platform (for example X10G security blade)
- Appliance description

See TRITON Unified Security Center online Help for complete details.

Accessing Security Blade Manager and other consoles

Help | X-Series Appliance | Version 7.7.1

How you access Security Blade Manager depends on how access has been configured in the TRITON console. There are 3 modes:

- If no special configuration has been performed, you can access Security Blade Manager via a link on the **Manage Appliances** page in the TRITON console, or directly via the appliance's C interface IP address and port number (described below). You are prompted for credentials.
- If single sign-on is configured for you in the TRITON console, you can access Security Blade Manager via the Single Sign-On button on the **Manage Appliances** page. You are not prompted for credentials. Alternatively, you can go direct to the C interface IP address and port number; you will be prompted for credentials.
- If two-factor authentication (certificate authentication) has been configured on TRITON console, you must also be configured with single sign-on privileges to access Security Blade Manager. To get to the manager, log on to the TRITON console using your two-factor authentication and then use the Single Sign-On button on the **Manage Appliances** page. Direct access via the C interface IP address is disabled when two-factor authentication is configured. See *Configuring two-factor authentication*.

For information about configuring single sign-on, see *Configuring an existing appliance for single sign-on* in TRITON console online Help.

Direct access

As stated above, if two-factor authentication is not configured, consoles can be accessed directly or through the TRITON console.

Logging on to Security Blade Manager

You can log onto the Security Blade Manager by pointing a browser to the Logon Portal (described above), or by going directly to:

```
https://<IP-address-of-interface-C>:9447/appmng/
```

You can also log on to the Security Blade Manager of any X10G security blade registered with your TRITON Unified Security Center via a link on the **Manage Appliances** page in the TRITON console.

The user name is **admin**.

The password was set on your security blade when the script **firstboot** was run.

To change the console password, see *X10G security blade account management*, page 67.

Configuring two-factor authentication

Help | X-Series Appliance | Version 7.7.1

Two-factor authentication:

- Is configured for and applies to TRITON console log on.
- Requires administrators to perform certificate authentication to log on.
- Can be made to apply to Security Blade Manager and Content Gateway Manager by forcing administrators to log on to TRITON console before accessing other consoles.
- Requires single sign-on to be configured for administrators allowed access to Security Blade Manager and Content Gateway Manager.
- Requires that the password logon capability be **disabled** using an appliance command line interface command. This prevents administrators not configured for single sign-on from accessing the Security Blade Manager and Content Gateway Manager.

Configuration is described in detail in *Configuring Certificate Authentication* in TRITON console online Help.

X10G logs and reporting

Websense X10G security blades keep detailed logs of activity on the system. These logs are designed to assist you and Websense Technical Support when there is unexpected behavior or a problem. For more information about X10G security blade logs, see *X10G security blade logs*, page 47.

Modules on the X10G security blades by default generate detailed reporting records (usually called “log records”) of module usage and actions. This requires installing a Windows-only reporting component (**Log Server** for Web) on another machine.

To add the Log Server component to your deployment:

- Download the TRITON software installer, available from www.mywebsense.com.
- Install Log Server on a Windows 2008 R2 server with access to:
  - The Microsoft SQL Server instance that hosts the Log Database
  - The security blade, so that it can retrieve filtering data from Web components to create log records

Management reports based on filtering log records can be generated using the reporting tools included in the Web Security module of the TRITON Unified Security Center.

Important

Except in demonstrations in which only TRITON - Web Security is installed on an X10G security blade and the network includes a small number of users, the TRITON Unified Security Center should be installed on a separate Windows Server 2008 R2 64-bit machine.

Web security reports

- The **Threats** tab of the **Status > Dashboard** page appears first when you log on to TRITON - Web Security. It shows information about suspicious activity that may be related to advanced malware threats in your network.
- The **Risks** tab shows information about blocked and permitted requests for URLs that fall into the Security Risk class.
- The **Usage** tab shows information about traffic patterns in your network, including bandwidth information and filtering summaries.
- The **System** tab shows alert messages, status information, and graphical charts that show the current state of your Web security software, focusing on Internet filtering activity in your network.
- **Presentation reports** provide customizable graphical and tabular reports of client Internet activity or message filtering activity.
- Web mode **investigative reports** are interactive reports that allow you to drill-down into your data to find the information of most interest to your organization.
- Web mode **Real-Time Monitor** allows you to see what traffic is being filtered by the Filtering Service associated with a Policy Server, and what action is applied to each request.

Databases used with the X10G security blade

Websense software filters Internet activity based on your active policies **and** information stored in filtering databases that must be updated at regular intervals.

- The Websense Web Security **Master Database** contains URL category information and protocol definitions. It is managed by Filtering Service. Administrators can control how often the database is updated, and whether or not partial, real-time updates are applied between full updates, in TRITON - Web Security. (See The Websense Master Database for details.)

  A limited, initial version of the filtering database is pre-installed on the security blade, so that filtering can begin as soon as you enter a subscription key. Download the full Master Database as soon as possible to enable comprehensive

Internet filtering capabilities. See the *Getting Started Websense X-Series* after you complete initial setup of the security blade.

- Websense Content Gateway scanning and categorization options rely on a set of databases installed with Websense software. The software checks for updates to these databases at a regular interval. Updates to these databases occur independently of all Master Database updates.

  Every time you restart a security blade or the Content Gateway module, a download of these small databases is initiated. If that download fails, a new download is attempted every 15 minutes until a successful download occurs.

Navigating in the X10G security blade

Security Blade Manager opens showing the **Status > General** page in the content pane. The slot number, Appliance Controller host name, Security mode, and a Log Off button are displayed in the banner at the top of the page.

- To see another page, select an entry in the left navigation pane.
- To get a detailed explanation of the options on any page, go to **Help > Explain This Page**.

Security Blade Manager offers access to the following pages:.

Status

- *General system status*, page 8
- *X10G security blade CPU and memory status*, page 10
- *X10G security blade disk use by module*, page 10
- *X10G security blade network bandwidth*, page 11

Configuration

- *System configuration*, page 13
- *X10G security blade network interface configuration*, page 16
- *X10G security blade routing configuration*, page 23
- *X10G security blade alerting*, page 26
- *Configuring Web Security components on the X10G security blade*, page 29

Administration

- *X10G security blade patch management*, page 34
- *Using the backup utility on an X10G security blade*, page 41
- *X10G security blade logs*, page 47
- *X10G security blade toolbox*, page 48
- *X10G security blade account management*, page 67

Clustering multiple Web Security Gateway X10G security blades

Content Gateway is the Web proxy component of Web Security Gateway. An important feature of Content Gateway is its ability to link together multiple instances of Content Gateway to form a *managed cluster*. This allows Web Security Gateway blades to quickly scale to increase capacity and system performance while system administration remains simple and can be performed from a single cluster node. Management clustering is fully described in the Content Gateway online Help system.

To configure clustering, open Content Gateway Manager, click **Get Help!**, and select the **Clusters** topic from the **Contents** tab. If you are using **SSL Manager**, be sure to read the section on SSL clustering. Also be sure to read the section titled **Adding nodes to a cluster**. Fully familiarize yourself with the feature before enabling it. There are several essential requirements, including that all nodes must be on the same version of Content Gateway, and that clustering must be enabled on each node separately (although, once enabled, all can be administered on any node).

General system status

The **Status > General** page appears first when you log on to Security Blade Manager. It presents the current status of each software module on the security blade.

Use this page to:

- Check for system alerts, including information about new patches.
- Gauge resources used by each module, including:
  - How many CPUs are dedicated to the Appliance Controller module.
  - How much memory (RAM) is allocated to the Appliance Controller module.
  - Which security blade interfaces are used by the module (for example, C or A1.P1).
  - Which services (daemons), if any, are included in the module.
- Stop and start software services, or restart an entire software module.

- Restart or shut down the security blade itself.

Important

For security purposes, a Security Blade Manager session ends after 30 minutes of inactivity. You can choose to monitor the status pages even after the 30-minute timeout is reached.

To do this, mark the box labeled **Monitor status without timing out** in the Appliance Controller section on this page.

Information on all Status pages then continues to update normally until you close the browser or navigate away from the Status pages. Be sure to **Save** all changes; these are lost if not saved before 30 minutes of inactivity.

Each X10G security blade configured with Web Security Gateway includes:

- The **Appliance Controller** software operates behind the scenes. It manages security blade configuration, downloads and applies patches, accesses the backup utility, requests module restarts, initiates shutdowns, and handles other security blade management tasks.
- **Websense Content Gateway** contains the Websense proxy software and Web content scanning and analysis for Web Security Gateway. Several services (daemons) comprise this software.
- **Websense Web Security** is the software that handles Web filtering. Several services (daemons) comprise this software.

In addition, the X10G security blade may include:

- **Network Agent** is the optional Web solution component that monitors Internet traffic and filters protocols other than HTTP and HTTPS.

You may see some or all of the following links and buttons, depending on your configuration:

Button or Link	Description
View Patch	Appears when an alert indicates that a new patch is available. Click the button to go to the **Administration > Patch Management** page where you can view a list of available patches and access the patch management facility.
Restart Appliance	Causes a security blade to be rebooted. All modules are stopped. Modules are then restarted. Modules that are flagged as Disabled are not restarted.
Shutdown Appliance	Causes a security blade and all software modules to be shut down in an orderly fashion.
Restart Module	Causes a module on a security blade (all of its services) to be stopped and then restarted.

Button or Link	Description
Launch (Content Gateway Manager)	Launches Content Gateway Manager. See *X10G security blade management consoles*, page 2.
Stop Services Start Services	Causes all services for a module on a security blade to be stopped. Or, if services are stopped, Start Services causes all services to be started.
Launch (TRITON - Web Security)	Launches TRITON - Web Security. See *X10G security blade management consoles*, page 2.
Restart Module (Network Agent) (optional)	Causes the Network Agent service on a security blade to be stopped and then restarted.
Stop Services Start Services (Network Agent) (optional)	Causes the Network Agent service on a security blade to be stopped. Or, if services are stopped, Start Services causes all services to be started.

X10G security blade CPU and memory status

The **Status > CPU and Memory** page provides information about CPU and memory usage for the software module running on a security blade, for the previous 60 seconds.

- **CPU Usage** displays:
  - An aggregate of all CPU usage during the previous 60 seconds, based on occupied resources and total available resources for a module
  - The percentage of each available CPU used by a module during the previous 60 seconds
- **Memory Usage** displays the:
  - Percentage of available memory used by a module during the previous 60 seconds
  - Actual memory used by a module during the previous 60 seconds, in megabytes
  - Total memory available to a module during the previous 60 seconds, in megabytes

X10G security blade disk use by module

The **Status > Disk Usage** page provides a summary of the previous 60 seconds of disk activity, as well as information about overall disk space availability, for the module on a security blade.

- **Disk Activity** shows average input/output operations per second (IOPS) and charts the previous 60 seconds of activity.
- **Usage Statistics** shows disk space used and available within a module.

The sections for the Appliance Controller, Websense Web Security, Websense Content Gateway, and the optional Network Agent module show one summary of information for all components within a module. This is represented as **system** disk activity or usage.

The section for the Content Gateway module may also show information for cache and Websense PreciseID™ disk activity and usage.

- The cache consists of a high-speed object database called the **object store**. The object store indexes objects according to URLs and associated headers, enabling Content Gateway to store, retrieve, and serve Web pages, and also parts of Web pages, providing optimum bandwidth savings. If the cache disk fails, Content Gateway goes into proxy-only mode (no caching).
- When Content Gateway integrates with Websense Data Security, PreciseID™ fingerprinting is used to detect sensitive information despite manipulation, reformatting, or other modification.

X10G security blade network bandwidth

The **Status > Network Bandwidth** page provides information about throughput on the security blade network interfaces listed here.

- **Appliance Controller Interface** (C)
- **Websense Content Gateway Interface** (A1.P1 or A1.P2, if enabled)
- **Network Agent Interface** (N) (optional). Note that blocking information is sent on interface C.

For information about configuring the interfaces, see *X10G security blade network interface configuration*, page 16. The bandwidth display includes them only if they are enabled.

For each interface, the following information is displayed for the previous 60 seconds:

Inbound/Outbound

- Current megabits per second, inbound and outbound, on the interface
- Maximum bandwidth capacity in megabits per second

Bandwidth Statistics

- Total megabits of data received and sent
- Total number of packets received and sent
- Packets dropped, inbound and outbound
- Total errors, inbound and outbound
- Rate in megabits per second, inbound and outbound

X10G security blade system watchdog

X10G security blades implement a system watchdog daemon to monitor critical system processes and conditions. Should one of the monitored processes or conditions fail or fault, the watchdog service performs a reset or restart.

Monitored processes and states include:

- Appliance kernel -- is the kernel active.
- Domain Agent -- is the Domain Agent running. This is an essential process that is responsible for communicating between the user interface and a security blade's back-end processes.
- Journal Commit I/O -- detect a "journal commit I/O" error.
- File table -- detect a file table overflow condition.

Watchdog actions are recorded in the system log file, which can be viewed in the Security Blade Manager on the **Administration > Logs** page.

2 Configuration

Use the Configuration section of the Security Blade Manager to:

- Set a security blade's time and date, host name, and description (see *System configuration*, page 13).
- Define the network interfaces for a security blade (see *X10G security blade network interface configuration*, page 16). This will include C, A1.P1, A1.P2, and N.
- Optionally specify static routes for all security blade interfaces and between modules, if applicable (see *X10G security blade routing configuration*, page 23).
- Set up SNMP alerting (see *X10G security blade alerting*, page 26).
- Identify which computer is hosting filtering configuration and policies for the network (*Configuring Web Security components on the X10G security blade*, page 29).

System configuration

Use the **Configuration > System** page to:

- Review basic security blade information, including the current blade hostname, security configuration, version number, hardware platform, system date and time, and uptime.
- See which software module is installed on the security blade and get its version number.
- Set the system **time and date**.

Important

If any Websense services are running, stop all Websense services before changing the time. Then, reset the time **and** make certain that the time is consistent across all servers running Websense services. Finally, restart Websense services.

If you do not stop the services first, client updates and policy changes entered after the time reset are not saved.

- Use the **Time zone** list to select the time zone to be used on this system.

  GMT (Greenwich Mean Time), the default, is also known as UTC (Universal Time, Coordinated). Other time zones are calculated by adding or subtracting from GMT. GMT is sometimes chosen to provide a common time stamp for geographically distributed systems.
- Use the **Time and date** radio buttons to indicate how you want to set the date.

  Time is set and displayed using 24-hour notation.
  - To synchronize with an Internet Network Time Protocol (NTP) server (www.ntp.org.), select the **Automatically synchronize** option and enter the address of a primary NTP server. The secondary and tertiary fields are optional.

    Important

    If you synchronize the system clock with an NTP server, NTP protocol packets and their response packets must be allowed on any firewall or NAT device between a security blade and the NTP server. Ensure that you have outbound connectivity to the NTP servers. Add a firewall rule that allows outbound traffic to UDP port 123 for the NTP server.

    If interface C on a security blade is not connected to the Internet, then you must provide a way for interface C to reach an NTP server. One solution is to install an NTP server on the local network where interface C can reach it.
  - To set the time yourself, select the **Manually set** option and change the value in the Date and Time fields. Use the format indicated below the entry field.
- Click **Save** to apply and save the changes.

◆ Set the appliance **hostname**, or system name (1 - 60 characters long).
- The first character must be a letter.
- Other characters can be letters, numbers, dashes, or periods.

- The name cannot end with a period.

Important

If this is a Web Security Gateway appliance and Content Gateway will be configured to perform Integrated Windows Authentication (IWA), the hostname cannot exceed 11 characters, excluding the domain name.

In addition, hostname should not be changed after the domain is joined. If it is changed, IWA will immediately stop working and will not work again until the domain is unjoined and then re-joined with the new hostname.

For more information, see the section titled *Integrated Windows Authentication* in Content Gateway Manager Help.

- Create or edit a unique **appliance description** to help you identify and manage the system.

  The description is displayed in the security blade list in the TRITON Unified Security Center when the blade is added there.

In each section that allows changes, **OK** saves and applies the new values. **Cancel** discards changes and restores entry field values to their current settings.

X-Series 7.7.1 support for IPv6

Help | X-Series Appliance | Version 7.7.1

Version 7.7.0 of TRITON Enterprise, including 7.7.1 X-Series appliances, provides incremental support for IPv6.

X-Series support is provided in combination with Web Security and Web Security Gateway (Anywhere).

Important

To use IPv6 with Web Security Gateway (Anywhere) you must configure the Content Gateway proxy as an **explicit proxy**. IPv6 is **not** supported in transparent proxy deployments.

For Web Security, IPv6 support includes:

- Dual IP stack implementation on interfaces C and N
- IPv6 traffic to the Internet or clients on interfaces C and N, including Block pages sent on C
- IPv6 static routes

- SNMP traps and counters for IPv6 data
- Network diagnostic tools in the Command Line Utility and Command Line Interface

For Web Security Gateway (Anywhere), support includes all of the above, plus:

- Dual IP stack implementation on interfaces A1.P1 and A1.P2
- Traffic to the Internet or clients on interfaces A1.P1 and A1.P2, and their bonded interface (A2.P1/A2.P2), if configured

Limits and restrictions:

- IPv6-only internal networks are not supported
- IPv4 must be used to communicate among Websense appliances (such as security blades) and with TRITON components

See TRITON – Web Security Help and Content Gateway Manager Help for detail pertinent to those components.

IPv6 configuration summary

Help | X-Series Appliance | Version 7.7.1

IPv6 support is disabled by default.

IPv6 is enabled in the Security Blade Manager at the top of the **Configuration > Network Interfaces > IPv6** page. When it is enabled, all IPv6 support is enabled for all affected capabilities on the security blade.

In any field that accepts an IPv6 address, the address can be entered in any format that conforms with the standard. Note that IPv4-mapped IPv6 addresses are not supported. For example:

- Leading zeros within a 16-bit value may be omitted
- One group of consecutive zeros may be replaced with a double colon
- IPv4-mapped IPv6 addresses are not supported. For example, the address ::ffff:192.168.1.128 is not supported.

Disabling IPv6 support requires a full restart of the security blade.

When IPv6 is disabled, IPv6 values remain in the configuration files, but are not editable.

X10G security blade network interface configuration

Use the **Configuration > Network Interfaces IPv4** and **IPv6** pages to specify the IP address, subnet mask, default gateway, and DNS addresses for each network interface on the appliance.

- *X10G Appliance Controller Interface (C)*, page 17

- *Websense Content Gateway Interfaces (A1.P1 and A1.P2)*, page 19
- *Network Agent Interface (N)*, page 20

Click **OK** to save and apply new values in each section.

X10G Appliance Controller Interface (C)

The Appliance Controller interface (C):

- Communicates with all Websense management interfaces
- Communicates with the Websense Data Security server
- Provides inter-blade communication
- Transports (optionally) non-HTTP and non-HTTPS protocol enforcement
- Handles Websense Master Database downloads via the Internet (unless your site uses A1.P1 for database downloads).

Initial configuration of the C interface is completed when the security blade is first powered on and you access the blade via the iDRAC; a script called **firstboot** prompts you for the values needed to configure interface C.

Important

Changing the C interface IP address significantly impacts the deployment and may require reinstallation of some components. See *Changing the C interface IP address*, page 21.

To enable the C interface IP address entry field, place the mouse pointer over the iHelp icon and click “Enable IP field” in the pop-up.

Guidelines for configuring network interface C

IP address (C interface)	Required. This interface typically requires continual access to the Internet, though some sites use A1.P1 for all communication with the Internet. If you change the IP address of the C interface, the update process may take about 5-6 minutes. After the IP address is changed, you are redirected to a logon page. Enter your user name and password. The **Status > General** page will show that the services are starting up. Wait for all services to start.
Subnet mask (C)	Required.
Default gateway (C)	Optional. IP address of the router that allows traffic to be routed outside of the subnet.

Primary DNS (C)	Required. IP address of the domain name server.
Secondary DNS (C)	Optional. Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS (C)	Optional. Serves as a backup in case the primary and secondary DNSes are unavailable.

Websense Content Gateway Interfaces (A1.P1 and A1.P2)

Content Gateway Interfaces (A1.P1 and A1.P2) handle traffic directed to and from the Content Gateway proxy module.

- Both the A1.P1 and A1.P2 proxy interfaces can be used to accept users' Internet requests (inbound traffic) and communicate with Web servers (outbound traffic). In other words, both interfaces can be configured to handle traffic into and out of the proxy module.
- A typical configuration is to use A1.P1 for both inbound and outbound traffic; A1.P2 is not used.
- Another option is to configure A1.P1 to accept users' Internet requests (inbound only). In this case, A1.P2 is configured to communicate with Web servers (outbound).

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).

Guidelines for configuring network interfaces A1.P1 and A1.P2

General guideline	If you use both A1.P1 and A1.P2 and you locate them in 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 (A1.P1 or A1.P2 interface)	Required.
Subnet mask	Required.

Default gateway	Required. 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.
Primary DNS	Required. IP address of the domain name server.
Secondary DNS	Optional. Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS	Optional. Serves as a backup in case the primary and secondary DNSes are unavailable.

Network Agent Interface (N)

Help | X-Series Appliance | Version 7.7.1

In this configuration, Network Agent is a software component used to monitor all Internet traffic, report on bandwidth usage, and send blocking information for protocols other than HTTP and HTTPS. Blocking information is sent on interface C.

Note that Network Agent, if used, always resides on the security blade in slot 16 (or off the chassis).

Network Agent continually monitors overall network usage, including bytes transferred over the network. The agent sends usage summaries to other Websense software at predefined intervals.

Network Agent is typically configured to see both inbound and outbound traffic in your network. The agent distinguishes between:

- Requests sent from internal machines to internal machines (hits to an intranet server, for example)
- Requests sent from internal machines to external machines such as Web servers (user Internet requests, for example)

X10G security blade interface bonding

Interface bonding provides Active/Standby mode: A1.P1 (or A1.P2) on switch A1 is active, and A2.P1 (or A2.P2) on switch A2 is in standby mode. Only if the primary interface fails would its bonded interface (A2.P1or A2.P2) become active.

For more information on switch configuration and recovery, please see *Switch recovery techniques*, page 72.

Changing the C interface IP address

Sometimes it is necessary to change the C interface IP address. What is affected and what must be done depends on the configuration of your security blades and the details of your deployment. **The number of activities that must be performed and the service disruption can be significant. If possible, retain the current C interface IP address.**

In most cases, off-chassis components that depend on or directly service a security blade should be uninstalled prior to changing the C interface IP address and reinstalled after the IP address change is completed. These components include:

- Off-chassis TRITON Unified Security Center
- Filtering Service
- Network Agent
- Real Time Monitor
- DC Agent
- Logon Agent
- Directory Agent
- Radius Agent
- Remote Filtering Service
- Sync Service
- Linking Service

Important

It is strongly recommended that you back up your security blade(s) and affected off-chassis components before making any changes.

Follow the steps in the scenario below that matches your deployment:

Scenario 1: Multiple security blades in a cluster, Web Security Gateway with off-chassis TRITON Unified Security Center and off-chassis Log Server

Summary of steps:

Covered under this scenario:

1. Changing the C interface of the Full policy source security blade
2. Changing the C interface of User directory and Filtering security blades
3. Changing the C interface of Filtering only security blades

Summary steps for changing the C interface of the Full policy source security blade:

1. If Web DLP is configured, unregister Content Gateway with the Data Security Management Server.
2. On the Log Server host, stop the Log Server service.
3. On the TRITON Unified Security Center host, uninstall TRITON Unified Security Center and associated components (see the component list, above). Make a list of uninstalled components.
4. Document the Policy Source settings of all security blades in the cluster and then on the User directory and filtering and Filtering only blades, change the policy source setting to Full policy source.
5. On the original Full policy source security blade, change the C interface IP address.
6. On each of the secondary security blades, change the policy source setting from Full policy source to the original setting, pointing the blade to the new Full policy source C interface IP address.
7. Reinstall TRITON Unified Security Center and associated components.
8. On the Log Server host, change the IP address of the Policy Server entry in websense.ini to the new C interface IP address and restart Log Server.
9. If Web DLP is used, reregister with Data Security Management Server.

Summary steps for changing the C interface of the User directory and Filtering security blade:

1. Uninstall off-chassis components that are registered to the User directory and Filtering security blade whose C interface IP address will change.
2. Temporarily make Filtering only security blades that depend on the User directory and Filtering security blade whose C interface IP address will change, Full policy source security blades.
3. Change the C interface IP address of the User directory and Filtering security blade.
4. Return the policy source setting of the Filtering only security blades to Filtering only, pointing them to the new User directory and Filtering C interface IP address.
5. Reinstall off-chassis components that are registered to the User directory and Filtering security blade.

Summary steps for changing the C interface of the Filtering only security blade:

1. Uninstall off-chassis components that are registered to the Filtering only blade whose C interface IP address will change.
2. Change the C interface IP address.
3. Reinstall off-chassis components that are registered to the Filtering only security blade.

For detailed step-by-step instructions, go to the Websense Technical Library and search for the article titled Changing the C interface IP address: step-by-step.

Scenario 2: Multiple security blades in a cluster, Web Security Gateway with off-chassis Policy Broker and off-chassis TRITON

Unified Security Center

> **Note**
> No security blade is set to Full policy source.

If you have multiple security blades in a cluster, it is considered best practice to follow Scenario 2 when changing the C interface IP address.

Summary of steps:

1. If Web DLP is configured, unregister Content Gateway with the Data Security Management Server.
2. Uninstall off-chassis components that are registered to the security blade(s) whose C interface IP address will change.
3. Document the Policy Source settings of all security blades in the cluster and then change the policy source setting of each to Full policy source.
4. Change the C interface IP address (or addresses, if more than one blade must change).
5. Return the policy source settings of the security blades to their original mode, pointing them to the new C interface IP address of a changed security blade if appropriate (if the blade is a Filtering only blade and the C interface change was to the User directory and Filtering security blade it pointed to).
6. Reinstall off-chassis components that are registered to security blades in the cluster.
7. If Web DLP is used, reregister with Data Security Management Server.

For detailed step-by-step instructions, go to the Websense Technical Library and search for the article titled Changing the C interface IP address: step-by-step.

X10G security blade routing configuration

Help | X-Series Appliance | Version 7.7.1

Use the **Configuration > Routing** page to specify:

- Static routes from subnets and client computers through any active blade interface, except C. If IPv6 is enabled, static IPv6 routes can also be added and imported.
- Module routes from security blade modules through blade interface C to subnets. IPv6 module routes are **not** supported.

Configuring static routes

- Static routes can be specified for any active interface on the security blade, except N, which is dedicated to Network Agent and cannot be routed.

- The same route cannot be added for 2 different interfaces on the same module. If attempted, the blade displays an error.
- Static routes that are defined for an interface that is later made inactive remain in the routing table, and are displayed in gray to indicate that the routes are inactive.
- Static routes that become invalid because the IP address of the interface changes are disabled and displayed in red.
- Static routes can be added and deleted, but not modified. To modify a route, delete it and add a new route specifying the new values.
- The static route table has a maximum limit of 5,000 entries.

Adding static routes

Static routes can be added one at a time, or many at time using an import file.

When a static route is added, data entered in each field is validated by the blade, and an error message is displayed if there is an inconsistency in the route.

To add static routes:

1. Go to the **Configuration > Routing** page, select the IPv4 or IPv6 tab, and click **Add/Import** under **Static Routes**.
2. **To manually add a single route**, select the **Add individual route** radio button, enter values for all fields, and then click **Add Route**.

Destination Network	Required. Specify the subnet IP address for which traffic will be routed.
Subnet Mask	Required. The subnet mask for the network where the clients reside (such as 255.255.0.0)
Gateway	Required. IP address providing access from the proxy subnet to the client subnet. This address must be on the same subnet as the blade.
Interface	Required. The blade interface to be used for the static route. Only active interfaces are offered in the drop-down list.

3. **To add multiple routes using an import list file**:
   a. Prepare the import file. See **Import file specifications**, below.
   b. Select the **Import route file** radio button.
   c. Specify the full path and file name, or **Browse** to locate the file. Click **Import Route** to import the routes specified in the file.

      The security blade reads the file, validates each route, and reports errors for lines that are invalid.

      Duplicate route entries are ignored; duplicate entries are not created.

If the number of routes in the file, combined with the number of existing routes, exceeds the 5,000 route table limit, the import fails. No routes are added and an error message displays.

Import file specifications:

1. The file must be a plain text file. (Most routers export route tables to a plain text file.)
2. The file can contain comment lines. Comment lines begin with "#".
3. A line that defines a route must include the following 4 fields in the order shown. Each field must be separated by a space.

   For IPv4:

   ```
   destination netmask default-gateway interface
   ```

   Destination is a subnet address or host IP address.

   Netmask determines the proper value of *destination*.

   Default-gateway is the next hop.

   Interface is the appliance interface through which traffic is routed. The specified interface must be enabled. If it is disabled, the appliance reports an error and does not add the route.

   For IPv6:

   ```
   destination prefix-length default-gateway interface
   ```

   Destination is a subnet address or host IP address.

   Prefix-length determines the proper value of *destination*.

   Default-gateway is the next hop.

   Interface is the appliance interface through which traffic is routed. The specified interface must be enabled. If it is disabled, the appliance reports an error and does not add the route.

Deleting static routes

1. In the Static Routes table, select the routes to be deleted:
   - To select 1 route, click the box to the left of entry you want to delete.
   - To select multiple entries, click the box to the left of each entry you want to delete.
   - To delete all routes, click the box to the left of the label **Destination Network**.
2. Click **Delete**.

Exporting the route table

To export the route table to a text file, click **Export Table**. Use the Browse dialog to specify a location and name for the file.

All routes in the table, whether enabled or disabled, are exported.

The file is formatted as described above for import files.

Configuring module routes

In some deployments, it is necessary or desirable to route some Web traffic through the security blade C interface (typically Web traffic is routed through separate, dedicated interfaces (A1.P1 or A1.P2), and C is reserved for management traffic). However, some sites might want to route authentication (or other) traffic through the C interface. This is accomplished by defining module routes on the **Configuration > Routing** page if this is supported by your subscription.

The module route table has a maximum limit of 5,000 entries.

Adding a module route

1. In the Module Route section of the **Configuration > Routing** page, click **Add**.
2. Specify a value for each field and click **Add Route**.

Module	Required. Select a module from the drop down list. The list displays only modules installed on the security blade. The Network Agent module may be installed, but will not appear in the list.
Destination subnet	Required. Specify the subnet IP address for which traffic will be routed.
Subnet mask	Required. The subnet mask for the destination subnet.

Note

It is the responsibility of the administrator to verify that the endpoint is available on the subnet.

Deleting a module route

1. In the Module Routes section, select the routes to be deleted.
   - To select 1 route, click the box to the left of entry you want to delete.
   - To select multiple entries, click the box to the left of each entry you want to delete.
   - To delete all routes, click the box to the left of the label **Module**.
2. Click **Delete**.

X10G security blade alerting

Help | X-Series Appliance | Version 7.7.1

Use the **Configuration > Alerting** page to enable and configure SNMP alerting.

There are 2 methods of SNMP alerting that you can enable on the **Setup** tab:

- Allow your SNMP manager to poll the security blade for standard SNMP counters (see *Enable SNMP polling (monitoring)*, page 27).
- Configure the blade to send SNMP traps for selected events to your SNMP manager (see *Enable SNMP traps*, page 27).

  After enabling the SNMP trap server on the blade, use the **Alerts** tab to configure which events cause a trap to be sent. See *Enable specific alerts for an X10G security blade*, page 28.

Enable SNMP polling (monitoring)

1. Under Monitoring Server, click **On**.
2. Select the **SNMP version** (v1, v2c, or v3) used in your network.
   - With SNMP v1 and v2c, a suffix (-wcg, -wws, or -na) is appended to the community name to indicate the originating module for the counter.
   - With SNMP v3, you can specify the context name (WCG, WWS, or NA) to poll counters for each module.
3. If you selected v1 or v2c, provide the **Community name** for the security blade, and then click **Save**.

   You have completed your SNMP monitoring configuration.
4. If you selected v3, select the **Security level** (None, Authentication only, or Authentication and Encryption) used in your network, and the **User name** to associate with SNMP communication.
5. If you selected a security level that includes authentication, also enter and confirm the **Password** for the selected user name, then select the **Authentication protocol** (MD5 or SHA).
6. If you selected authentication and encryption, select the **Encryption protocol** (DES or AES), and then enter and confirm the **Encryption key** used for encryption.
7. Click **OK** to implement your changes.

Enable SNMP traps

Before enabling the security blade to send SNMP traps, download the **appliance MIB file** using the link in the Trap Server section of the **Configuration > Alerting** page. The MIB file must be installed in your SNMP manager before it can interpret traps sent by the security blade.

When you are ready for the blade to start sending SNMP traps:

1. Under Trap Server, click **On**, and then select the SNMP version (v1, v2c, or v3) used in your network.
2. For SNMP v1 or v2c, provide the following information:
   - The **Community name** to associate with traps sent by the security blade
   - The IP address and port used by your SNMP manager.

3. To verify your configuration, click **Send Test Trap**. If the test trap succeeds, click **Save** to implement your changes. See *Enable specific alerts for an X10G security blade*, page 28 to configure which events cause a trap to be sent.

   If there is a problem sending the test trap, verify the community name, IP address, and port, and make sure that the network allows communication between the security blade C interface and the SNMP manager.
4. For SNMP v3, enter the **Engine ID** and **IP address** of your SNMP manager, as well as the **Port** used for SNMP communication.
5. Select the **Security level** (None, Authentication only, or Authentication and Encryption) used in your network, and the **User name** to associate with SNMP communication.
6. If you selected a security level that includes authentication, also enter and confirm the **Password** for the selected user name, then select the **Authentication protocol** (MD5 or SHA).
7. If you selected authentication and encryption, select the **Encryption protocol** (DES or AES), and then enter the **Encryption key** used for encryption.
8. To verify your configuration, click **Send Test Trap**. If the test trap succeeds, click **Save** to implement your changes. See *Enable specific alerts for an X10G security blade*, page 28 to configure which events cause a trap to be sent.

   If there is a problem sending the test trap, verify the community name or Engine ID, IP address, and port, and make sure that the network allows communication between the security blade and the SNMP manager.

Enable specific alerts for an X10G security blade

Help | X-Series Appliance | Version 7.7.1

The security blade can send traps for each of its modules: Appliance Controller, Content Gateway, Web Security, and Network Agent. The Alerts tab of the **Configuration > Alerting** page lists the alerts associated with only the modules that you have enabled.

A table for each module lists:

- The hardware or software **Event** that triggers the alert (for example, a RAID disk failure, or a Websense service stopping).
- The **Threshold**, if applicable, that defines the alert condition (for example, CPU usage exceeding 90%, or free disk space reaching less than 10% of the total disk size).
- The **Type** of alert (system resource or operational event).
- Whether or not an SNMP trap is sent when the event occurs or the threshold is reached.

To enable all alerts for a module, select the check box next to **SNMP** in the table header. All check boxes in the column are selected.

Otherwise, mark the check box next to an event name to enable SNMP alerts for that event. To disable alerts for an event, clear the associated check box.

Time-based thresholds: Most of the events that have a configurable threshold also have a configurable time-based threshold, specified in minutes. When the time-based threshold is set and **both thresholds** are exceeded, an alert is sent. To enable time-based thresholds, select the **Enable time-based thresholds** check box at the top of the page. The time-based threshold is enabled on every event for which it is configurable.

Event-cleared alerts: In addition to generating event condition alerts, you can configure alerts to be sent when conditions return below the threshold. These are called **event-cleared alerts**. To enable event-cleared alerts, select the **Generate event-cleared alerts** check box at the top of the page.

The following events do not generate event-cleared alerts:

- Hostname change
- IP address change
- Scheduled backup failure
- SNMP authentication failure

When you have finished configuring alerts, click **OK** to implement the changes.

Configuring Web Security components on the X10G security blade

Help | X-Series Appliance | Version 7.7.1

Use the **Configuration > Web Security Components** page to specify which Web Security components are active on the blade, and where the blade gets Web Security global configuration and filtering policy information. Also define the TRITON - Web Security location.

1. Under **Policy Source**, select which Web solution configuration is used on this security blade: **Full policy source** (default; see *What is a policy source on the X10G security blade*, page 30), **User directory and filtering**, or **Filtering only** (see *What if a security blade is not the policy source?*, page 31). If this is a Full policy source appliance, it acts as both the Policy Broker and a Policy Server. There can be only 1 Full policy source appliance in your network.
2. If this is a User directory and filtering appliance, it also acts as a Policy Server. Enter the IP address of the Policy Broker appliance or server.
3. If this is a Filtering only appliance, enter the IP address of a Policy Server. It does not have to be the IP address of the Policy Broker machine.
4. Click **OK** to save and apply your changes.

What is a policy source on the X10G security blade

Help | X-Series Appliance | Version 7.7.1

Every Websense Web solution deployment must include a single **policy source**. This is a security blade or other server that hosts 2 components, Websense Policy Broker and Websense Policy Database, in addition to other Web solution components. All other Websense security blades or other servers point to this machine and receive regular updates from it. This blade (or other server) is called the **policy source**.

- When a security blade for a Web solution is configured as a policy source, all available Web solution components run on that blade, including some or all of the following:
  - Filtering Service
  - Policy Database
  - Policy Broker
  - Policy Server
  - User Service
  - Directory Agent (required for hybrid service)
  - State Server (optional; disabled by default)
  - Multiplexer (disabled by default; unavailable when the appliance is Filtering only)
  - Usage Monitor
  - Control Service
  - Websense Content Gateway module
  - Network Agent (optional on blade in slot 16 only)

  Windows-only services, like Log Server, and optional services, like transparent identification agents, still run on other machines.
- When a policy source blade runs a Web security solution, the TRITON services should be disabled and located on a Windows 2008 R2 server.
- A non-blade policy source is a server off the chassis that is hosting **Policy Broker**. The Policy Database is automatically created and run on the Policy Broker machine. This machine typically also includes a Policy Server instance, and may include additional Websense software components.

The Policy Database holds all filtering policies (including client definitions, filters, and filter components) for all security blades and all domains in the network. It also holds global configuration information that applies to the entire deployment.

If you are configuring a blade that is not the full policy source machine, then it must point to the policy source.

What if a security blade is not the policy source?

Help | X-Series Appliance | Version 7.7.1

A Websense X10G security blade that is not serving as the policy source can be designated to run either **user directory and filtering** or **filtering only**.

- A **user directory and filtering** security blade is a secondary blade, a lightweight version of the policy source machine. It runs:
  - Policy Server
  - User Service
  - Usage Monitor
  - Filtering Service
  - Control Service
  - Directory Agent
  - Websense Content Gateway module
  - Network Agent (optional on blade in slot 16 only)

  Having User Service and Policy Server together on a security blade means that you are able to obtain local network user names. Latency between User Service and Policy Server is eliminated, because both run on the same blade.

  Whenever you make a policy change in the TRITON management console, that change is immediately updated on the policy source blade. The change is pushed out to user directory and filtering blades within 30 seconds.

  These security blades can continue filtering for as long as 14 days if their connection with the policy source machine is interrupted. So even if a network connection is poor or is lost, filtering continues as expected.

  A **User directory and filtering** blade is configured to point to the Full policy source for updates.
- A **filtering-only** blade does not run Policy Server. It runs only:
  - Filtering Service
  - Control Service
  - Websense Content Gateway module
  - Network Agent (optional on blade in slot 16 only))

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

  These blades require a continual connection to the centralized policy server, not only to stay current, but also to continue filtering. If the connection to the policy server machine becomes unavailable for any reason, filtering on a filtering only blade can continue for up to 3 hours.

  If the policy server machine is on a remote network, with a WAN connection, it can be difficult to obtain user name/IP address maps for the local users.

User directory with X10G security blades

Help | X-Series Appliance | Version 7.7.1

If your organization relies on user identification or authentication, each security blade that is running Websense User Service must be configured to talk to a user directory. Multiple blades can talk to the same user directory, or to different user directories.

Preparing for hybrid user identification

With Web Security Gateway Anywhere (Web Security Gateway with the hybrid deployment option and enterprise-class data loss prevention) running, some users in your organization may be filtered by the hybrid (SaaS) cloud service. In this situation, an interoperability component on the security blade called **Directory Agent** is required to enable user-, group-, and domain- (OU) based filtering.

Directory Agent must be able to communicate with:

- A supported LDAP-based directory service:
  - Windows Active Directory® (Mixed Mode)
  - Windows Active Directory (Native Mode®)
  - Oracle (Sun Java™) System Directory
  - Novell eDirectory
- Websense **Sync Service**

After deployment, use TRITON - Web Security to configure User Service and Directory Agent.

- User Service configuration is performed on the **Settings > General > Directory Service**s page.
- Directory Agent configuration is performed on the **Settings > Hybrid Configuration > Shared User Data** page.
  - You can have multiple Directory Agent instances.
  - Each Directory Agent must use a unique, non-overlapping root context.
  - Each Directory Agent instance must be associated with a different Policy Server.
  - All Directory Agent instances must connect to a single Sync Service. (A deployment can have only one Sync Service instance.)
  - You must configure the Sync Service connection manually for all supplemental Directory Agent instances (these are the Directory Agents running on secondary blades). Communication is configured automatically for the Directory Agent instance that connects to the same Policy Server as Sync Service. See the TRITON - Web Security Help for details.

You can configure Directory Agent to use a different root context than User Service, and to process its directory data differently than User Service. Also, with Windows Active Directory, if User Service is configured to communicate with multiple global catalog servers, Directory Agent can communicate with all of them.

3 Administration

Help | X-Series Appliance | Version 7.7.1

Websense, Inc., maintains a customer portal at mywebsense.com where you can download product updates, get patches, access customer forums, read product news, and access other technical support resources for your Websense software and security blades.

As a best practice, create your MyWebsense account when you first set up an X-Series chassis family security blade, so that you can:

- Immediately apply any patches made available since your security blade was assembled.
- Get access whenever you need support or updates.

X10G security blade administration options

Help | X-Series Appliance | Version 7.7.1

The Administration pages enable you to:

- Install software patches (see *X10G security blade patch management*, page 34).
- Install software hotfixes (see *Hotfix management*, page 36).
- Prepare and restore backups of your blade's configuration (see *Using the backup utility on an X10G security blade*, page 41).
- Access system logs for all active modules (see *X10G security blade logs*, page 47)
- Customize block pages, enable remote access to the blade command-line interface, and launch the command-line utility (see *X10G security blade toolbox*, page 48).
- Change the Security Blade Manager or Content Gateway Manager **admin** password (see *X10G security blade account management*, page 67).
- Change the Help Language Preference (see *Help System Language*, page 69).

X10G security blade patch management

Help | X-Series Appliance | Version 7.7.1

X10G security blades are kept up to date with a simple, easy-to-use patch management facility.

Go to the **Administration > Patches/Hotfixes** page to check for, download, and install patches.

- Security blades automatically check for new patches once a day. The time of the check is randomized, cannot be configured, and is different for every blade.
- To manually check for patches at any time, use the **Check for Patches** button.
- When a new patch is available, the patch version number, description, and status are displayed in the **Available patches** table and an alert is displayed on the **Status > General** page.
- After a patch is downloaded it can be copied to another location on your network where it can be easily and efficiently uploaded to multiple blades.
- If the security blade management interface (C) does not directly connect to the Internet, you can configure a proxy server through which the blade checks for patches.
- The Patch History table provides an immediate history of patches that have been applied to the blade.

See:

Patch update options for X10G security blades, page 35

Best practices for security blade patches

- A new security blade at your site should immediately be patched to the latest version.
- Keep all X10G security blades on your network at the same version.
- Install software patches as soon as they become available.

Patch process

Patch discovery is performed automatically every 24 hours at random time, or manually with the **Check for Patches** button.

Patch download and installation is always initiated manually by the security blade administrator.

- Use the **Administration > Patches / Hotfixes** page to download and install each patch on the blade, during a low-activity period on your network.
- Install patches in consecutive sequence.

- On the **Patches** page, the "Appliance current version" number is the current blade version (reflects the latest patch installed).
- Be sure that all Websense modules running off the blade, such as Log Server, are upgraded to the appropriate level each time you patch the security blade. See the patch release notes for details.
- Multiple X10G security blades may be installed in your network. However, they must all be running the same version of Websense software modules. Websense, Inc., does not support running different versions of the software on different blades on one network. Filtering results are not expected to be consistent in that scenario.

Patch update options for X10G security blades

Help | X-Series Appliance | Version 7.7.1

- Available patches are listed in the **Available patches** table.
- For each available patch, a version number, description, and status is given. There is also a link to the patch release notes.

Important

It is very important to read the release notes. In addition to a summary of changes contained in the patch, there is information about impacts to other modules and an estimate of the time it will take to apply the patch.

The following options are available:

Download	Click **Download** to start downloading an available patch. In the Status field, a progress bar displays the progress of the download. Another patch can be selected, and the download initiated, while the first download is underway. Such requests form a sequential download queue. When the patch download is complete: • The **Download** button is replaced by **Install** and **Delete** buttons. (See descriptions of these buttons below.) • A **Save to network location** link is included after the patch description. Click the link to copy the patch file to another location on your network. This is helpful since you have multiple security blades and do not want to download the patch from Websense separately for every blade. Instead, on each blade, simply use the **Upload Patch Manually** function to upload the patch from the network location. It is recommended that patches be downloaded and applied in numeric sequence. In many cases, this is a requirement.
Pause	When a download is underway, a **Pause** button displays. Click **Pause** to temporarily halt the download.

Cancel	When a download is underway, a **Cancel** button displays. Click **Cancel** to end the download process.
Resume	When a patch download has been paused, a **Resume** button displays. Click **Resume** to continue a paused download.
Install	When a patch has been downloaded and verified (a checksum is performed as part of the download process), and is ready for installation, the **Install** button is enabled. **IMPORTANT: Before installing a patch, it is important that you read the patch release notes.** Click **Install** to install the patch. A series of pages prompt you for confirmation and provide status. You are notified if a restart is required after installation. After the restart, the patch is removed from the patch queue and logged in the Patch History table. The new security blade version number is reflected in the **Appliance version** field. If an earlier patch has not been installed but is required, you receive a message in the **Status** column indicating which earlier patch is required, and the **Install** button for the dependent patch is disabled. Install the earlier patch first. If a patch installation fails, any installed files from that patch are immediately uninstalled and a message displays indicating that the patch installation failed. You can try installing it again. If that fails, delete the patch, then download it again and re-attempt the installation.
Delete	Click **Delete** if you want to delete a patch.
Check for Patches	Click the **Check for Patches** button to manually check for new patches.
Upload Patch Manually	Click **Upload Patch Manually** to upload a patch from another location on your network. This can be a convenient and efficient method of distributing a patch among multiple security blades in a cluster or where multiple blades have access to a local network. For instructions on copying a patch file from a blade to another location in the network, see the entry for **Download**, above.

Hotfix management

Help | X-Series Appliance | Version 7.7.1

Related topics:

- *Hotfix application process*, page 37
- *Hotfix installation*, page 38
- *Hotfix history*, page 39

When necessary, Websense, Inc. releases a targeted *hotfix* to address a specific issue in a security blade module. In most cases, you receive notification of hotfixes in a Websense Technical Alert email. Sometimes, in response to a specific problem that you have reported, a Technical Support Agent recommends a specific hotfix.

The Security Blade Manager **Hotfixes** page is your facility for finding, installing, uninstalling, and maintaining a history of hotfix application.

Go to the **Administration > Patches / Hotfixes > Hotfixes** page to manage hotfixes.

- In the majority of cases, you are notified of hotfixes through:
  - A Websense Technical Alert email, or
  - A Websense Technical Support Agent. The Agent will provide the name of a specific hotfix to address the problem you reported.
- A hotfix may address an issue on any module running on your appliance.
- A hotfix should not be recommended to you for a module that you have not configured or are not running on your appliance.
- As a best practice, unless otherwise instructed by a Websense Technical Support Agent, do not install a hotfix for an issue that you have not encountered.
- Hotfix names are constructed: *XXX*-#.#.#-###:

  For example: WCG-7.7.4-001
- The Hotfix facility will not install a hotfix that is not valid for the module versions on your appliance.
- A hotfix may have dependencies on one or more other hotfixes, in which case the hotfix facility will not allow the installation of the hotfix until after its dependents are installed.

Hotfix application process

Following is a summary. For complete details, see *Hotfix installation*, page 38.

1. In the **Hotfix Installation** area, enter the name of the hotfix and click **Find**. If the hotfix is not found, review the notification from Websense and check that the name is entered correctly. If the name repeatedly returns not found, contact Websense Technical Support.
2. When a hotfix is found, a pop-up displays that includes a description of the hotfix and other pertinent information. If the description is what you expect, click **Download** to download the hotfix to the appliance. Otherwise, click **Cancel**.
3. After the hotfix is downloaded, a description and status display in the **Downloaded hotfixes** table. Confirm that the hotfix has no dependencies and is ready for installation. If the hotfix is dependent on another hotfix, you must download and install that hotfix first.
4. Click **Install** to install the hotfix.

If you have several security blades and do not want to download the hotfix from Websense.com multiple times, you can use the **Save to network location** link to copy

the downloaded hotfix to a convenient location on your network, and then, on each blade, use the **Upload Hotfix Manually** button to upload the file to the blade.

For procedural information, see:

Hotfix installation, page 38

Hotfix history, page 39

Hotfix installation

Help | X-Series Appliance | Version 7.7.1

Related topics:

- *Hotfix management*, page 36
- *Hotfix application process*, page 37
- *Hotfix history*, page 39

Use the Hotfix Installation area to:

- Search for and download a hotfix
- Install a hotfix
- Delete a hotfix that has not yet been installed
- Copy a hotfix to a network location
- Upload a hotfix from a network location

The following options are available:

Hotfix ID entry field	Specify the exact name of the hotfix to be searched for in the Websense.com hotfix repository. Inclusion of leading or trailing zeros is required. The format is: *XXX*-#.#.#-### For example: WCG-7.7.0-001
Find button	After the hotfix name has been entered, click **Find** to direct the Security Blade Manager to go to Websense.com to search for the hotfix. If the hotfix is found, a **Hotfix Details** pop-up dialog box displays with a description of the hotfix, and a **Download** and **Cancel** button.
Downloaded hotfixes table	This tables maintains a complete list of hotfixes downloaded to the blade but not yet installed. A record of installed hotfixes is maintained in the Hotfix History section.
Hotfix ID	The hotfix ID.

Description	A high-level description of the hotfix that usually includes: • The name • A short description of the problem that the hotfix addresses • The module the hotfix applies to • Relative severity (high, moderate, low) • The release date • A link to the official **Release notes** (hosted on Websense.com) • A **Save to network location** link that opens a dialog that allows you to save the hotfix to a location on your network.
Status	States whether the hotfix is ready for installation or has a dependency on another hotfix that must be installed first.
Action	Includes the **Install** button to initiate installation, and a **Delete** button to remove the hotfix from the blade prior to installation. To uninstall and remove a hotfix, see the uninstall function that is accessed from the Hotfix History area.
Upload Hotfix Manually	Use this button to upload a hotfix from the blade to a location on your network.

Hotfix history

Help | X-Series Appliance | Version 7.7.1

Related topics:

- *Hotfix management*, page 36
- *Hotfix application process*, page 37
- *Hotfix installation*, page 38

Use the Hotfix History section to:

- View the current blade version
- View a record of installed hotfixes
- Uninstall hotfixes
- View a record of uninstalled hotfixes

The following options are available:

View drop down list	From the drop down list, select **Installed hotfixes** to populate the table with a list of hotfixes that have been installed, and that were attempted to be installed but failed. Select **Uninstalled hotfixes** to populate the table with a list of hotfixes that have been uninstalled, or were attempted to be uninstalled but failed.
When **Installed hotfixes** is selected from the **View** drop down list	
Radio button adjacent to the **Hotfix ID**	Select the radio button to activate the **Uninstall** button. If the hotfix has dependencies that prevent it from being uninstalled, a message is displayed below the table.
Hotfix ID	The hotfix ID.
Name	The name of the hotfix and a link to the Release Notes.
Module	The name of the effected appliance module.
Date Installed	The day and year that the hotfix was installed.
Status	Indication of whether the installation succeeded or failed. If the installation failed, a link is provided to the installation log file.
Uninstall button	Use this button to initiate uninstallation of the selected hotfix.
When **Uninstalled hotfixes** is selected from the **View** drop down list	
Hotfix ID	The name of the hotfix.
Reason	A reason that you provide for uninstalling the hotfix. It is easy to lose track of why a hotfix was uninstalled. Recording a clear description here can save repeated errors and lost time in the future.
Date Uninstalled	The day and year that the hotfix was uninstalled.
Status	Success or failure status of the uninstall action. Occasionally a hotfix may fail to uninstall. One reason may be that uninstallation is dependent on uninstalling another hotfix or set of hotfixes.

Patches and hotfixes proxy settings

Help | X-Series Appliance | Version 7.7.1

If the blade management interface (C) does not directly connect to the Internet, you can configure a proxy server through which the appliance checks for patches and hotfixes.

Use proxy server	Select the check box to enable or disable the option.
Proxy IP address and port	Specify the IP address and port number of the proxy to be used.
User name/ password (optional)	Optionally, authenticate the proxy connection with a user name and password.
Test Connection	Click **Test Connection** to test the connection to the specified proxy.

Using the backup utility on an X10G security blade

Help | X-Series Appliance | Version 7.7.1

Related topics:

- *Scheduling backups on the X10G security blade*, page 43
- *Full X10G security blade configuration backups*, page 44
- *Module configuration backups on the X10G security blade*, page 45
- *Restoring a backup file on the X10G security blade*, page 45

Use the Backup tab of the **Administration > Backup Utility** page to initiate configuration backups, schedule recurring backups, or manage existing backup files.

It is always a best practice to perform a full backup of the security blade and of each module prior to restoring to factory image.

You cannot restore from a backup file taken from Web Security Gateway (no Network Agent) to a blade with Web Security Gateway that is optimized for Network Agent. Also, Network Agent can only be enabled on a blade in slot 16 of the chassis.

To restore a security blade or module configuration from an existing backup file, click the Restore tab, and then see *Restoring a backup file on the X10G security blade*, page 45.

Two types of backup are available on the X10G security blade:

- A **Full Appliance Configuration** backup saves all security blade settings, as well as configuration and policy information for all active modules. Websense, Inc., recommends running a full backup on every security blade in your network on a regular basis.

Note that the full backup file may be smaller than the module backup files, because it is compressed.

- A **module configuration** backup of the Web solution saves all configuration information for this module. This includes any client and policy data stored on the selected blade.

> **Note**
>
> Module configuration backup does not include a Content Gateway option.
>
> Content Gateway only backups (snapshot) can be performed in Content Gateway Manager. Snapshots must be performed manually; there is no scheduling facility.

Backup types and backup status information are shown in the Perform Backup list. To start or schedule a backup, first select the backup type, and then click either **Run Backup Now** or **Configure Backup Schedule** (for information about scheduling backups, see *Scheduling backups on the X10G security blade*, page 43.

You must initially set up the backup function; it is not automatic. Once you schedule backups, however, those backups will continue to run at regular intervals without requiring further intervention. To stop a scheduled backup from recurring, click **Cancel Scheduled Backup**.

The Local Backup Files list shows all backup files stored on the current security blade. Select a backup type from the **View backups for** list to change the type of backup file shown.

Each entry in the list includes the following information:

- The date and time of the backup
- The name of the backup file

For full security blade configuration backup files, the following information is also included:

- The patch version of the blade on which the backup was run. When you restore from a backup, the backup file must be the same version as the security blade you are restoring.
- The host name of the backup source.
- A comment on the policy information in each backup file for the configuration that applies to you.
  - **Full policy source** (Web) is the default comment if the backup was generated on the policy source blade.
  - **User directory and filtering** (Web) is the default comment if the backup was generated on a security blade configured to run Filtering Service and User Service on those components.

- **Filtering only** (Web) is the standard comment if the backup was generated on a filtering only security blade.

Up to 20 blade backup files and 20 backup files for each module can be stored on a security blade. When the twenty-first backup file is created, the oldest file is automatically deleted.

To download a backup file to another machine, click the file name, then browse to path where you want to save the file.

To delete local backup files manually, mark the checkbox next to the backup file name in the Local Backup Files list, and then click **Delete**.

Scheduling backups on the X10G security blade

Help | X-Series Appliance | Version 7.7.1

Related topics:

- *Using the backup utility on an X10G security blade*, page 41
- *Full X10G security blade configuration backups*, page 44
- *Module configuration backups on the X10G security blade*, page 45
- *Restoring a backup file on the X10G security blade*, page 45

Use the **Backup Utility > Configure Backup Schedule** page to specify how frequently and at what time of day the selected backup type is performed, and to select a location for storing backup files.

To schedule backups:

1. Select a **Backup frequency**: daily, weekly, or monthly.
   - For weekly backups, select which day of the week the backup is run.
   - For monthly backups, select which day of the month the backup is run. You cannot schedule backups to run on the 29th, 30th, or 31st day of the month, because not all months have those days.
2. Specify a **Start time** for the backup process. Ideally, select a time when the security blade is unlikely to be under heavy load.

   Enter the time in 24-hour format (where 00:00 indicates midnight, and 12:00 indicates noon).
3. Provide a **Storage location** for the backup files. Only one remote backup location can be configured for each backup type.
   - Select **Appliance** to have the file stored locally. A maximum of 20 backup files can be saved, and the backup file directory cannot be renamed, moved, or deleted.

     Backup files saved to the security blade can be viewed on the Backup Utility page, under Local Backup files.

- Select **Remote machine** to store the backup file on another machine in the network, then indicate whether to use a **Samba file share** or **FTP server** and provide the following connection information:
  a. The **IP address/hostname** of the remote machine, and the connection **Port** to use.
  b. The **Default directory** in which backup files will be created. A different subdirectory will be created automatically for each backup file type.

  Important
  If you want to create backup files for multiple security blades on the same remote machine, be sure to use a separate directory for each blade's backup files.

  This avoids the possibility of conflicts that could lead to files being mistakenly overwritten or deleted.

  c. The **User name** and **Password** to use when connecting to the remote machine. If a network logon is used, also provide the **Domain** in which the account resides.
  d. Click **Test Connection** to make sure the security blade can communicate with the remote machine and write to the specified location.
  e. If you want remote backup files to be automatically deleted after a specified time period, mark the **Delete backup files that are older than** check box, and then select a time period from the list.

4. Click **OK** to save your changes and return to the Backup Utility page. The new backup schedule is displayed in the Perform Backup list.

Full X10G security blade configuration backups

Help | X-Series Appliance | Version 7.7.1

A full appliance configuration backup saves all blade settings, as well as saving configuration and policy data for all active modules. If you have multiple blades, run backups on each one. The backup file includes data for only the blade on which it is created.

Note
If you have Websense software components installed off the security blade—like Log Server or the TRITON Unified Security Center—Websense, Inc., recommends that you run the Backup Utility on those machines at approximately the same time that you back up your blade. When you restore the system, this allows you to restore from a time-compatible set of backups on all machines.

Full blade configuration backup files for Web solution blades include:

- All configuration files for the security blade on which the backup is run, including configuration files for the Security Blade Manager
- A snapshot of all configuration data. For Web Security, this data is captured by the Websense Backup Utility, **wsbackup**. The snapshot includes:
  - Global configuration information, stored in the Policy Database (if Policy Broker is running on the selected blade)
  - Local configuration information, such as Filtering Service settings, stored in the **config.xml** file (if Policy Server is running on the selected security blade).
  - Websense component initialization (.ini) and configuration (.cfg) files.

Module configuration backups on the X10G security blade

Help | X-Series Appliance | Version 7.7.1

Module configuration backups save all configuration information, including policy data, for the selected module.

- Web solution configuration backups performed on the *full policy source* security blade include all information stored in the Policy Database.
- Backup operations for Content Gateway are managed through Content Gateway Manager. Click the Content Gateway Manager link at the top of the Backup Utility page to open the console and initiate backups.

Restoring a backup file on the X10G security blade

Help | X-Series Appliance | Version 7.7.1

Related topics:

- *Using the backup utility on an X10G security blade*, page 41
- *Scheduling backups on the X10G security blade*, page 43
- *Full X10G security blade configuration backups*, page 44
- *Module configuration backups on the X10G security blade*, page 45

When you initiate the restore process, all current settings for the security blade or module are erased. Backup files stored on the blade are not affected. When restoring the full blade configuration, at the end of the restore process, the blade restarts. The blade is not restarted after you restore only a module.

To restore a security blade or module to a saved configuration:

1. Stop all Websense software components running off the blade.

   For example, stop Log Server, Sync Service, Linking Service, transparent identification agents, all components associated with the TRITON Unified Security Center, and the integrated Data Security Management Server.

2. Open Security Blade Manager on the blade whose configuration you want to restore and go to the **Administration > Backup Utility** page
3. Click the **Restore** tab, then select the configuration type that you want to restore from the **Select restore mode** list. Also, note that when you restore a full security blade configuration:
   - The current security blade version must match the version associated with the backup file. (The security blade version is displayed on the **Restore** tab.) Thus, a version 7.7.1 backup can be restored only to a blade that is at version 7.7.1.
   - The current blade policy source mode (full policy source, user directory and filtering, or filtering only) must match the policy source mode in effect when the backup file was created.
   - The hardware model of the current blade must be the same as the model that was backed up.
   - The original blade that was backed up cannot also be running elsewhere in the network. Restoring a full configuration re-creates the original blade and makes use of unique ID numbers from that blade.
4. Click **Run Restore Wizard**. The restore wizard opens.
5. Select a radio button to indicate where the backup file is stored, and then click **Next**.
   - **This remote machine: <***host name or IP address***>**: Retrieve the file from the default location on the specified machine. The default location is the path specified in the backup schedule for the selected backup type.
   - **This appliance**: Use a backup file that was saved locally.
   - **Another location (browse for file)**: Use a file saved on any accessible machine in the network.
6. Select or specify the file to use.
   - If you selected the default local or remote backup file location, you are given a list of available backup files to use. Select an entry in the list, and then click **Next**.
   - If you selected another location, browse to the path on the remote machine where the backup file is located, and then click **Next**.
7. Verify the details on the Confirm page, and then click **Restore Now**. The security blade is restored to the selected configuration.

   If you have initiated a full appliance configuration restore, the blade is restarted during the restore process.
8. Before starting the off-box components, ensure that the system time of all TRITON component hosts is synchronized. On the blade, either set the time manually, or, if an NTP server is configured, click **OK** to trigger an update with the NTP server.
9. Start the Websense components that are running off the security blade.

   Note that if the restore process changed blade IP addresses, you may need to reconfigure or reinstall off-blade components to re-establish communication between on-blade and off-blade components.

X10G security blade logs

Help | X-Series Appliance | Version 7.7.1

Websense Technical Support may request log files to assist you with troubleshooting. This page provides access to these log files for viewing and download.

> **Note**
>
> Network Agent generates a log file only if you have enabled logging in the TRITON - Web Security console.
>
> If you want to examine Network Agent log files in the Security Blade Manager, first log on to the TRITON - Web Security console and navigate to **Settings > Network Agent > Global**. Then scroll down to **Additional Settings** to enable logging of protocol traffic and specify a logging interval.

Select the module for which you want to view logs:

- Appliance Controller
- Websense Content Gateway
- Websense Web Security
- Network Agent

If you are reviewing the Appliance Controller log, next select the date range.

- Use the drop-down list to choose the date range.
- Log files are available in weekly increments for up to 5 weeks.

Then select the view option. Select either:

- View last __ lines

  Indicate how many lines of the log you want to see in a pop-up window:

  - last 50 lines
  - last 100 lines
  - last 500 lines
- Download entire log file

Click **Submit** to begin the process of gathering the requested log file.

If you are downloading the entire log file, use the **File Download** dialog box to navigate to the save location.

X10G security blade toolbox

Help | X-Series Appliance | Version 7.7.1

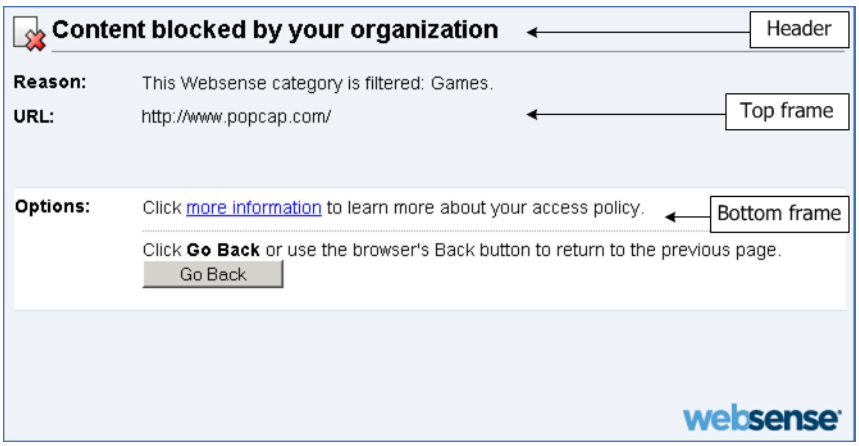
Use the **Administration > Toolbox** page to set up customized block pages, access basic Linux commands, and assist with troubleshooting.

Web solution block pages on the X10G security blade

Help | X-Series Appliance | Version 7.7.1

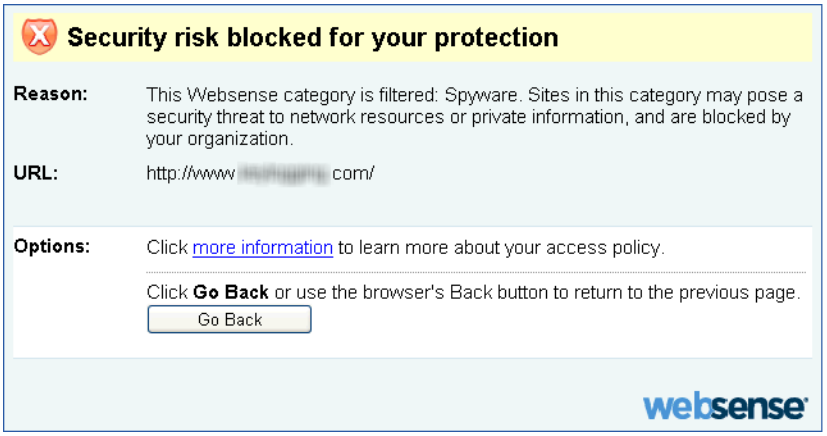
The X10G security blade hosts a set of default block pages. These are displayed to end users each time a Web request is blocked.

Block pages are constructed from HTML and JavaScript files. By default, the block page has 3 main sections:



- The header explains that the site is blocked.
- The top frame contains a block message showing the requested URL and the category of the URL.
- The bottom frame presents any options available to the user (go back to the previous page, continue to the site, use quota time to access the site, use different credentials to try to access the site).

If the site is blocked because it belongs to a category in the Security Risk class, a special version of the block page is displayed.



To verify the behavior and appearance of block pages, use the links at testdatabase.websense.com to attempt to access test sites in categories that your organization blocks.

Use the **Administration > Toolbox** page to determine whether to:

- Use the block pages (both standard and security) provided with your Websense Web solution software (**Default block page**).
- Edit the block page files to suit the needs of your organization (**Custom block page**).

Customizing block pages

When you select **Custom block page**, a copy of the default block page files is created in an editable directory on the security blade. The default block page files are neither moved nor deleted, so that you can revert to them at any time.

After selecting the custom block page option:

1. Select the files you want to change, and then click **Download File(s)**. The available files are:

File Name	Contents
block.html	Contains the text for the top frame of the block message, which explains that access is restricted, lists the requested site, and describes why the site is restricted.
blockFrame.html	Text and button (Go Back option) for sites in blocked categories.
blockStyle.css	Cascading style sheet containing most block page styles
continueFrame.html	Text and buttons for sites in categories to which the **Confirm** action is applied.

File Name	Contents
master.html	Constructs the information frame for the block page, and uses one of the following files to display appropriate options in the bottom frame.
messagefile.txt	Contains text strings used in block pages
moreInfo.html	Content for the page that appears when a user clicks the **More information** link on the block page.
webDLPPolicyViolation.html	Provides block page content when Websense Data Security components block content from being posted to or downloaded from the Web.
quotaFrame.html	Text and buttons for sites in categories to which the **Quota** action is applied.
security.js	JavaScript file used in construction of a security block page

- When you select a single file, its details are displayed, including its default use, last modification date, and size.
- If you select more than one file to download, the files are packaged into a single ZIP file.

2. Make modifications locally.

Important

Do **not** change the default file names.

- To replace the Websense logo with another image, see *Changing the block page logo*, page 51.
- If the information that you want to display in the block message is longer than the space provided, see *Changing the size of the message frame*, page 51.
- If you want to start again from the original, default set of block page files, see *Starting over*, page 52.
- Additional information about customizing block pages can be found in the "Block Pages" section of the TRITON - Web Security Help.

3. Click **Upload File(s)** to place the modified files and any supporting graphics files on the security blade.
   - The edited files can refer to custom graphics files (like logos). If you use custom graphics, be sure to upload these additional graphics files to the editable directory.
   - If you have more than 5 files to upload, select the first 5 files to be uploaded, and then click **Add More Files**. You can upload a maximum of 10 files at a time.
4. Click **Apply Changes**. This restarts Filtering Service.
5. To test the customized block pages, go to testdatabase.websense.com and try to access test sites in categories blocked by your organization's policies.

6. Return to Step 2 if adjustments are needed.

Changing the block page logo

The **master.html** file includes the HTML code used to display a Websense logo on the block page. To display your organization's logo instead:

1. Download the **master.html** file to a temporary directory.
2. Locate an image file for your organization's logo, and copy it to the same location.
3. Open **master.html** in a text editor, such as Notepad or vi (not an HTML editor), and edit the following line to replace the Websense logo with the image name for your organization's logo:

   ```
   <img title="Websense" src="/Images/wslogo_block_page.png"
   ...>
   ```

   - Replace the value of the **title** parameter to reflect name of your organization.
   - Change the path to indicate that your image file is located in the **Custom** folder (not in the Images folder).
   - Replace **wslogo_block_page.png** with the name of the image file containing your organization's logo.

     The result will look something like this:

     ```
     <img title="ABC_Corporation" src="/en/Custom/
     myimage.png" ...>
     ```

     Note that parameter and folder names are case-sensitive.
4. Save and close the file.
5. Upload both the image file (containing your logo) and the edited copy of **master.html** to your X10G security blade, and then click **Apply Changes**.

Changing the size of the message frame

Depending on what information you want to provide in the block message, the default width of the block message and height of the top frame may not be appropriate. To change these size parameters:

1. Download the **master.html** file.
2. Open the file in a text editor, such as Notepad or vi (not an HTML editor).
3. To change the width of the message frame, edit the following line:

   ```
   <div style="border: 1px solid #285EA6;width: 600px...">
   ```

   Change the value of the **width** parameter as required.
4. To cause the top frame of the message to scroll, in order to show additional information, edit the following line:

   ```
   <iframe src="$*WS_BLOCKMESSAGE_PAGE*$*WS_SESSIONID*$" ...
      scrolling="no" style="width:100%; height: 6em;">
   ```

   Change the value of the **scrolling** parameter to **auto** to display a scroll bar when message text exceeds the height of the frame.

   You can also change the value of the **height** parameter to change the frame height.
5. Save and close the file.

6. Upload the file to your X10G security blade, and then click **Apply Changes**.

Starting over

If you need to start over with a default block page file at any time, click the **default files** link under the Upload and Download buttons. This allows you to download a copy of the default block page files to your local machine.

Edit the files you want to change, and then upload the edited files to the security blade.

X10G security blade command line

Help | X-Series Appliance | Version 7.7.1

On the blade **Toolbox** page, the **Appliance command line** section provides:

- The ability to turn on and off SSH remote access to the blade **command line interface** (the same shell that can be used to run the **firstboot** script). SSH access allows administrators to log on to the blade command line shell from machines on the network that have a route to the security blade.
- Access to a **command line utility** that is embedded within Security Blade Manager. The command line utility provides convenient access to common troubleshooting commands.

SSH Remote Access

Use the **Remote Access** option to enable and disable SSH access to the security blade command line interface.

To connect to the blade command line shell when SSH access is enabled:

- Use a terminal emulator that supports SSH.
- SSH to the IP address of the C interface.
- Use your Security Blade Manager administrator logon credentials when prompted.
- Run the “help” command to see the available commands.

The following is a list of relevant command-line commands:

firstboot

help

history

ip address

ip dns

ip gateway

local-access

module disable

module enable

module restart
module start
module stop
patch delete
patch list
policy-source
quit
reload
remote-access disable
remote-access enable
reset password
show cpu
show disk-io
show disk-space
show interface c
show memory
show module
show module service
show patch
show patch history
show platform
show policy-source
show remote-access
show remote-access history
show security-mode
show ssh
shutdown
ssh disable
ssh enable
switch A1 configure
switch A1 (or A2) verify
switch A2 configure na (or wcg)

Note that switch commands are available only on the security blades in slots 1 through 15. For more information on switch configuration and recovery, see *Switch recovery techniques*, page 72.

Command line utility

Use the **Command Line Utility** to run troubleshooting, debugging, and utility commands. Results are displayed in the **Console output** section of the page. You can download the output file for the command last executed.

Click **Launch Utility** to open the command utility.

The **Module** drop down list includes an entry for each module installed on the security blade depending on your security mode but could include one or more of the following modules. Select the module that you want to work with:

- Appliance Controller
- Websense Content Gateway
- Websense Web Security
- Network Agent (if using blade 16)

Select the command you want to run from the **Command** drop-down list, enter appropriate parameters as described below, and then use the **Run** and **Stop** buttons as appropriate:

Command	Description	Parameters
arp	Displays the kernel ARP table for the selected module.	None.
cache-user-names	Pertains only to the Websense Web Security module. Use it to turn on, turn off, or query the status the caching of user names resolved from IP addresses by Content Gateway. Cached entries are valid for 10 minutes.	[Action]: Enter **enable** to turn on user name caching. Enter **disable** to turn off user name caching. Enter **status** to display the status of user name caching.
content-line -r	Pertains only to the Websense Content Gateway module. Use it to display the current value of a configuration variable in Content Gateway's records.config file.	[Variable Name]: Enter the name of the configuration variable for which you want to retrieve a value. **Example**: `proxy.config.vmap.enabled` This variable returns "0" or "1". "0" indicates that the virtual IP manager is disabled; "1" indicates that it is enabled. For a complete list of valid configuration variables, click the link **Websense Content Gateway variables** and navigate to the records.config topic. [You may be asked for credentials if you have not logged on to the proxy console earlier in the session.]

Command	Description	Parameters
content-line -s	Pertains only to the Websense Content Gateway module. Use it to set the value of a configuration variable in Content Gateway's records.config file. With this command, you can make changes to Content Gateway variables without restarting the proxy. To activate the changes, run `content_line -x` (see below).	[Variable Name]: Enter the name of the variable you want to modify. [Value]: Enter the value you want to supply the variable. **Example**: Enter the variable name **proxy.config.arm.enabled** and the value "1" or "0". This enables or disables the ARM, which his used for transparent proxy caching, IP spoofing, and ARM security. For a complete list of valid configuration variables, click the link **records.config**. [You may be asked for credentials if you have not logged on to the proxy console earlier in the session.]
content-line -x	Pertains only to the Websense Content Gateway module. Use it to read and apply the values of all configuration variables in Content Gateway's records.config file. If you have used `content_line -s` to change the setting of any variables in the file records.config, you can activate your changes immediately (without restarting the proxy) by running this command.	None.
copy-MasterCA	Pertains only to the Websense Web Security module. Copies the most recent Master CA certificate created in TRITON Certificate Authentication to the Websense Web Security module.	None.
directory-agent-service	Pertains to Websense Web Security module only. Enable or disable the Directory Agent service with this command. This service is disabled by default.	[Action]: Enter **enable** to enable the Directory Agent service. Enter **disable** to disable the Directory Agent service.

Command	Description	Parameters
ethtool	Displays the current ethernet card settings of the specified network interface (NIC) device. This includes: • Supported ports • Supported link modes • Auto-negotiation support • Advertised link modes • Advertised auto-negotiation • Speed • Duplex • Port • PHYAD • Transceiver • Auto-negotiation setting • Wake-on support • Wake-on status • Link detection Use **ethtool** to verify local network connectivity.	None.
ethtool -k	Displays offload parameters, including checksum, for the selected network interface (NIC) device. This can be used to investigate a variety of problems. For example, if your NIC settings are right, but you are having duplex issues, you know you need to change your duplex settings. **-k** Change the checksumming parameters of the specified ethernet device.	None.
ifconfig	Use to troubleshoot network interface issues. Helps you identify IP issues and check subnets and network interfaces. Displays status information about the specified NIC, including but not limited to: • IP and broadcast address • subnet mask • number of packets received and transmitted • number of bytes received and transmitted	[Interface]: Enter the NIC for which you want settings. Click the information icon for valid NIC values. Enter **all** to display all interface status. Example: eth0 or eth1

Command	Description	Parameters
multiplexer	Enables and disables the Multiplexer service that supports SIEM integrations. See TRITON – Web Security Help. Multiplexer service will not run on a Filtering only appliance. Instead it transparently uses the Multiplexer service running on the Policy source machine.	[Action]: Enter **enable** to enable the Multiplexer service. Enter **disable** to disable the Multiplexer service.
nc -uvz	Attempts to read and write data across a network using user datagram protocol (UDP) to the specified server. Use it for functional tests of components and verification of connectivity. Use it to check data going across a UDP network. If you are having problems loading a Web page, or are getting a block, this command can help determine the problem. If you see a reset coming from the proxy, you can determine which DOM/module it is coming from. **-u** Run netcat in UDP mode **-v** Run netcat in verbose mode. **-z** Run netcat in zero I/O mode (used for scanning).	[Destination]: Enter the IP address of the server with which you want to communicate. [Port]: Enter the port number of that server.
nc -vz	The netcat (nc) utility. Attempts to read and write data across a network using transmission control protocol (TCP) to the specified server. Use it for functional tests of components and verification of connectivity. **-v** Run netcat in verbose mode. **-z** Run netcat in zero I/O mode (used for scanning)	[Destination]: Enter the IP address of the server with which you want to communicate. [Port]: Enter the port number of that server.

Command	Description	Parameters
netstat -neatup	Displays a list of open sockets on the selected module, appended with the process column. **-n** Displays active TCP connections. However, addresses and port numbers are expressed numerically, and no attempt is made to determine names. **-e** Displays ethernet statistics, such as the number of bytes and packets sent and received. **-a** Displays all active TCP connections and the TCP and UDP ports on which the computer is listening. **-t** Indicates which open ports are using TCP. **-u** Indicates which open ports are using UDP. **-p** Limits display of statistics or state of all sockets to those applicable to protocol.	None.
netstat -ng	Displays multicast group membership information about the selected module. **-n** Displays active TCP connections. However, addresses and port numbers are expressed numerically, and no attempt is made to determine names. **-g** Shows the multicast group memberships for all interfaces.	None.

Command	Description	Parameters
netstat - nItup	Use one of the netstat commands if you are having network connection and routing issues. **netstat -nItup** displays the following: • the amount of traffic in your network. • all active TCP connections and the TCP and UDP ports on which the computer is listening. Addresses and port numbers are expressed numerically, and no attempt is made to determine names. • Ethernet statistics, such as the number of bytes and packets sent and received. **-n** Displays active TCP connections and the ports they use when they connect. (This is useful if, for example, Filtering Service is not filtering. You can look at the connection the module is using here. If it is not the IP and port of the Filtering Service machine, you have found the source of the problem.) **-I** Shows the state of a particular interface, such as eth0 or eth1. **-t** Indicates which open ports are using TCP. **-u** Indicates which open ports are using UDP. **-p** Limits display of statistics or state of all sockets to those applicable to protocol.	None.

Command	Description	Parameters
netstat -s	Displays summary statistics for each protocol on the selected module. By default, statistics are shown for the IP, ICMP, TCP, UDP, and TCPEXT protocols. This includes such things as: • IP - the number of packets received, forwarded, and discarded for each protocol. • ICPM - the number of messages received, failed, sent. • TCP - the number of active and passive connection openings and failed connection attempts. • UDP - the number of packets received and set. • TCPEXT - statistics about SYN cookies, ACKs, packets received and queued, retransmits, and DSACKs. This is just a sampling. Many more statistics are shown.	None.
nslookup	Use this for DNS resolution problems. For example, if a particular Web site is not loading, perform an nslookup on it to view its IP address. **nslookup** lets you query DNS servers to find DNS details, including IP addresses of a particular computer, MX records for a domain, and the DNS servers of a domain.	[Host]: Enter the hostname (for example myintranet.com) or IP address of the host for which you want DNS information. [DNS server]: Enter the hostname or IP address of the DNS server for the security blade.
ping	Checks that a hostname or IP address exists, can accept requests from the selected module, and that DNS is resolving. Use this to test connectivity to another host— for example, the Data Security Management Server or TRITON - Web Security machine—and determine response time.	[Destination]: Enter the hostname (for example myintranet.com) or IP address of the host you want to test.
ping -I	Checks that a network interface can communicate with a hostname or IP address and that DNS is resolving. Use this to test connectivity to another host—for example, the Data Security Management Server or TRITON - Web Security machine—from one of the security blade NICs.	[Interface]: Enter the name of the NIC you want to test. Click the information icon for valid NIC values. **Example**: eth0 [Destination]: Enter the hostname or IP address of the host you want to test.
ping6	Tests IPv6 connectivity with the specified hostname or IP address.	[Destination]: Enter the hostname (for example myintranet.com) or IPv6 address of the host you want to test.

Command	Description	Parameters
ping6 -I	Tests IPv6 connectivity from the specified appliance interface to the specified hostname or IP address.	[Interface]: Enter the name of the NIC you want to test. Click the information icon for valid NIC values. **Example**: eth0 [Destination]: Enter the hostname or IPv6 address of the host you want to test.
policy-broker-token	Pertains only to the Websense Web Security module. Use this command to retrieve the Policy Broker token for this security blade. This may be needed to configure support for Remote Filtering. See the Websense Technical Library for more information.	None.
print-bypass	This command applies only to the Websense Content Gateway module. When Content Gateway is in transparent proxy caching mode, use this command to see which source and destination IPs the proxy is bypassing. If sites are not loading correctly, this helps you identify if a site is loading from your cache or going directly to the site for download. All entries in the source and destination bypass tables for the proxy are printed to the output console. For more information on source and destination bypass, see the **Configuration Files > bypass.config** section of the Content Gateway Manager Help system.	None.
route -A inet6 -n	Displays the contents of the IPv6 routing tables in numeric format.	None.
route -n	Display the current contents of the selected module's kernel IP routing table in numeric format. This is useful in complex network environments—for example, those with proxy chaining—to show if the environment is set up properly.	None.
show-triton-admin-email	Pertains only to the Websense Web Security module. Displays the email address to which alerts, password resets, and other TRITON administrator messages are sent.	None.
show-triton-smtp-settings	Pertains only to the Websense Web Security module. Displays the SMTP server information and sender email settings used when notifications are sent from TRITON.	None

Command	Description	Parameters
state-server	Applies to Websense Web Security module when the appliance is configured as a Full policy source or User directory and filtering system. In multiple Filtering Service deployments, Websense State Server is required for proper application of time-based filtering actions (Quota, Confirm, Password Override, and Account Override). See **Policy Server, Filtering Service, and State Server** in TRITON - Web Security Help.	[Action]: Enter **enable** to enable the state server service. Enter **disable** to disable the state server service.
sysctl-tcp-timestamps	Pertains only to the Websense Content Gateway module. View or change the setting for TCP time stamps. Edit this setting if you are experiencing performance problems with specific Web sites that do not properly support TCP time stamps. The operating system sets this kernel setting during installation. If the setting was changed and you are experiencing site latency with other sites—those that work best with TCP time stamps— return the setting to its default value and consider routing traffic to the problematic sites around the proxy. Be sure to choose a setting that works well for the sites that are most important to you. The setting affects the use of time stamps by the kernel for all TCP connections.	[Value]: Enter “0” to disable the current time stamp setting, and restore it to its default. Enter “1” to re-enable a custom setting. Enter “view” to view the current setting.

Command	Description	Parameters
sysctl-tcp-window-scaling	Pertains only to the Websense Content Gateway module. View or change the setting for TCP window scaling. Edit this setting if you are experiencing performance problems with specific Web sites that do not properly support TCP windows scaling. The operating system sets this kernel setting during installation. If the setting was changed and you are experiencing site latency with other sites—those that work best with TCP windows scaling— return the setting to its default value and consider routing traffic to the problematic sites around the proxy. Be sure to choose a setting that works well for the sites that are most important to you. The setting affects the use of windows scaling by the kernel for all TCP connections.	[Value]: Enter "0" to disable the current window scaling setting, and restore it to its default. Enter "1" to re-enable a custom setting. Enter "view" to view the current setting.

tcpdump	Use for any Web traffic issues to get packet captures—for example, if a site will not load or if you are having authentication problems.
	tcpdump intercepts and displays packets being transmitted or received by the specified network interface. Use the Expression field to select which packets are displayed.
	The output from **tcpdump** can help you determine whether all routing is occurring properly, to and from the interface. The output is verbose; it displays the data of each package in both hex and ASCII; and it includes a link-level header on each line.
	Note that if you do not stop the tcpdump command manually, 10,000 packets are captured, the maximum allowed.
		[Interface]: Enter the name of the NIC you are debugging. Click the information icon for valid NIC values.
		Example: eth0
		[Expression]: Enter a boolean expression that filters the packets to those of interest. Click the information icon for examples.
		Example 1: To capture all TCP traffic to and from the proxy on port 8080, enter this expression:
		`tcp port 8080`
		Example 2: To capture all TCP traffic to the site google.com, enter this expression:
		`tcp and dst host google.com`
		Example 3: To capture all TCP traffic from a specific end-user machine, enter this expression:
		`tcp and src host user.websense.com`
		Note that you can enter a hostname if it is resolvable by a DNS server, but the output uses IP addresses either way.

Command	Description	Parameters
tcpdump -w	Use this to dump traffic (raw packets) from the specified NIC to a file. To download the file, click the link, **Download output file for last command**, after running the command. This link is under the console output window. Websense Technical Support may request this file on occasion.	[Interface]: Enter the name of the security blade NIC you are debugging. Click the information icon for valid NIC values. [Expression]: Enter a boolean expression that filters the packets to those of interest. Click the information icon for examples. Enter **all** to capture all packets. Note that you can enter a host name if it is resolvable by a DNS server, but the output uses IP addresses either way.
top -bn1	Displays all operating system tasks that are currently running on the selected module. Use this to help troubleshoot CPU and memory issues. **-b** Run in batch mode. **-n** Update the display for a number of iterations, then exit. **-1** Do not display idle processes.	None.
traceroute	Use this to determine the route taken by packets across a network to a particular host. If some machines are not getting filtered or blocked, or if traffic is not even getting to the security blade, this shows the devices (or hops) that are between the machines that may be blocking access to the host. Use **tcpdump** to get a packet capture from each device. If you are having latency issues, **traceroute** can also help identify the causes. (Note that **traceroute** is of limited utility if an IP is being spoofed.)	[Destination]: Enter the hostname or IP address of the host destination you are investigating
traceroute6	Displays the route used by packets to reach the specified destination.	[Destination]: Enter the hostname or IPv6 address of the host destination you are investigating
triton-admin-email	Pertains only to the Websense Web Security module, and only when TRITON - Web Security is running on the blade for demonstrations. Use this to set the email address to which alerts, password reset notifications, and other administrator communication is sent.	[Email address]: The email address of the administrator.

Command	Description	Parameters
triton-smtp-settings	Pertains only when TRITON - Web Security is running on the blade for demonstrations. Use it to configure the SMTP server and sender settings. **Note**: Typically these settings are made in the TRITON Unified Security Center on the **Settings > Notifications** page.	[SMTP server IP]: The IP address or host name of the SMTP server through which email alerts should be routed. [Port]: The SMTP port. [From email address]: The email address to use as the sender for email alerts. [Sender name]: The name of the sender of the alerts.
triton-websecurity-services	Use it to start, stop, restart, and query the status of TRITON - Web Security services.	[Action]: Enter **start** to start TRITON - Web Security services. Enter **stop** to stop TRITON - Web Security services. Enter **restart** to restart TRITON - Web Security services. Enter **status** to display the status of TRITON - Web Security services.
user-group-ip-precedence	Applies to the Web Security module only. Use this command to change the precedence of identification attributes applied to: filtering policy, Delegated Administrator (DA) role identification, protocol policy, and quota time available. By default, the precedence attributes are, in descending order: User > Computer > Network > Group > Domain When user-group-ip-precedence is enabled, the precedence order is: User > Group > Domain > Computer > Network	[Action]: Enter **enable** to modify the precedence order to: User > Group > Domain > Computer > Network Enter **disable** (default) to set the precedence order to: User > Computer > Network > Group > Domain Enter **status** to display the current setting. **WARNING:** Changing the state of user-group-ip-precedence causes Filtering Service to stop and restart.
wcg-net-check	This command applies only to the Websense Content Gateway module. Use it to display diagnostics for Websense Content Gateway, such as: • interface status • connection to DNS name servers • connection to Policy Server • gateway packet loss • ping statistics for various modules • Internet connectivity • filtering status This command is useful for investigating latency issues, outages, or filtering problems, among other things.	None.

Command	Description	Parameters
wget	Use to initiate a non-interactive download of files from the Web, so you can diagnose connectivity issues. Use **wget**, for example, if you have configured the proxy, but cannot access the Web. **wget** simulates the proxy going out and retrieving the Web site. This command supports HTTP, HTTPS, and FTP protocols.	[URL]: Enter the URL of the Web site from which you want to download files.
wget-proxy	Use to test connectivity between the specified URL and the proxy (file download not supported). Use **wget**, for example, if you have configured the proxy, but cannot access the Web. **wget** simulates the proxy going out and retrieving the Web site. This command supports HTTP, HTTPS, and FTP protocols.	[URL]: Enter the URL of the Web site to which you want to test connectivity. [Proxy IP]: Enter the proxy IP address. This is the IP address of the A1.P1 interface on most security blade configurations. [Port]: Enter the port on which the proxy expects this traffic. 8080 is configured for HTTP by default. 8070 is configured for HTTPS by default. [User name]: Enter the user name of the client, if required for authentication. [Password]: Enter the password of the client, if required for authentication. Enter 'none' in both fields if user name and password are not applicable.

Technical Support tools for the X10G security blade

Help | X-Series Appliance | Version 7.7.1

When you collaborate with Websense Technical Support or a Websense partner to examine possible causes for network issues, these built-in tools can assist with troubleshooting:

- *Troubleshooting ports*, page 66
- *Security blade configuration summary*, page 67
- *Remote access*, page 67

Troubleshooting ports

With Websense Web solutions, you can open troubleshooting ports temporarily, so that various troubleshooting tests can be run. Use this tool only when directed to do so by Websense Technical Support.

Check **Enable troubleshooting ports**, and then click **Save** to cause the special ports to be enabled.

Important

Be sure to **clear** the check box and click **Save** to disable the ports when Technical Support is done using them. Do not leave these ports open and unattended.

Security blade configuration summary

The configuration summary tool gathers data from the blade and generates an archive file that can be sent to Websense Technical Support for analysis and debugging. The process takes 1 to 2 minutes.

When Websense Technical Support requests this file:

- Click **Generate File**.
- When the file is ready, a message appears at the top of the page: Configuration summary has been successfully collected. Click the link in the message to download the archive file to your desktop.
- You can then open the file or save it.
- Your technician will provide an FTP site for secure file transfer to Websense Technical Support.

Remote access

Enable remote access only at the request of Websense Technical Support.

- When you click **On** and then click **Save**, a passcode is generated and displayed on screen.
- Provide the passcode to your Websense Technical Support technician. This enables SSH, so that the technician can log on to your security blade.
- Each time you allow remote access to the blade and a Websense technician logs on, a record is added to the **Remote access logon history** at the bottom of the **Toolbox** page.
- When the technician is done, be sure to click **Off** and click **Save** to disable the access.

X10G security blade account management

Help | X-Series Appliance | Version 7.7.1

Use the **Administration > Account Management** page to change the password for accessing Security Blade Manager or Content Gateway Manager. In some circumstances, the page also includes a section for resetting TRITON - Web Security passwords.

Changing the Security Blade Manager password

Help | X-Series Appliance | Version 7.7.1

1. Enter the current password.
2. Enter the new password.
3. Confirm the new password.

Save applies and saves new values in the pane.

Cancel discards all changes entered since the last **Save** and restores entry fields in the pane to the last saved values.

Resetting the TRITON - Web Security password

Help | X-Series Appliance | Version 7.7.1

Administrators can change their own TRITON console password at any time from the TRITON Settings > My Account page.

For administrators who have forgotten their TRITON - Web Security password, when TRITON - Web Security runs on the blade for demonstrations, the **Administration > Account Management** page includes a section to facilitate resetting the administrator password.

Click the **logon page** link, and then click **Forgot my password**.

Note

In most deployments, the TRITON Unified Security Center, including TRITON - Web Security, is installed on a separate machine. In such cases:

- The **TRITON - Web Security Password Reset** section is not displayed.
- To reset the password, launch the TRITON console, and then click **Forgot my password** on the logon page.

The password reset process sends a temporary password to the email address associated with your administrator account. The temporary password is valid for only 30 minutes. If more than 30 minutes elapses before you attempt to log on with the temporary password, you must request a new password again.

You are prompted to enter a new password when you log on using the temporary password.

If the email SMTP settings and administrator email address are not configured for TRITON - Web Security, you must use the **triton-smtp-settings** and **triton-admin-email** commands in the Websense Web Security category of the **Toolbox > Command Line Utility** to configure the settings. See *Command line utility*, page 54.

Content Gateway Manager password reset

Help | X-Series Appliance | Version 7.7.1

This option is available when Content Gateway is run on the security blade.

1. Click **Reset Password** to reset your proxy password.
2. The new password appears at the bottom of the screen. Write it down.
3. As soon as you navigate away from the **Account Management** page in the Security Blade Manager, your reset password is no longer displayed.
4. Log on to Content Gateway Manager with the new password.
5. Go to **Configure > My Proxy > UI Setup > Login** to change the new password to the desired string.

Help System Language

Help | X-Series Appliance | Version 7.7.1

From the **Administration > Account Management** page, you can select the language in which the Help system will display. Once you make your selection and click on **OK**, all help system pages will be displayed in the language you have chosen.

4 Troubleshooting

Tips for responding to X10G security blade 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 on the next pages. 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 4.2.2.3.
- If the issue persists, perform *Booting the switch to Dell settings*, page 73, and then *Configuring the switch mode*, page 75.
- 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*, page 73.
   c. Perform *Configuring the switch mode*, page 75.
   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*, page 73.
   c. Perform *Configuring the switch mode*, page 75.
   d. Plug in the network cables.

Installing a new switch

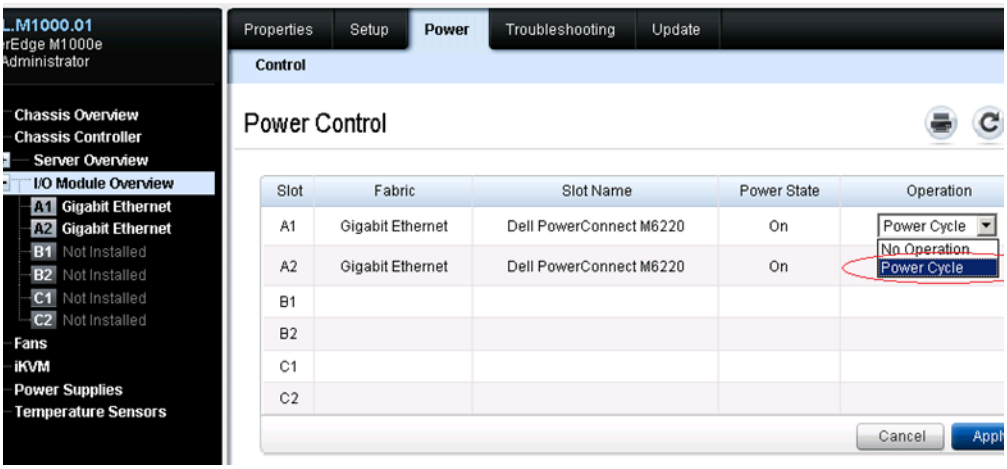
If you must replace a switch with a new one that has not been set up by a Websense team, insert the switch and latch it. Do not cable it. Then follow these steps:

a. Perform *Booting the switch to Dell settings*, page 73.
b. Perform *Configuring the switch mode*, page 75.
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. You need to confirm that you want to delete the configuration:
   `Are you SURE you want to delete the configuration? (y/n): y`
5. Select **1-Start operational code** to reboot the switch.
6. Wait for the console prompt to appear: **`console>`**
7. 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
```

8. Remember to configure the switch mode. (See *Configuring the switch mode*, page 75.)

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 does not run 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.