v7.7.1 Release Notes for X10G Appliance

Topic 44001 / Updated: 14-August-2012

Applies To:	Websense® X10G Appliance v7.7.1

Use these Release Notes to find information about what's new and improved in X10G Appliance version 7.7.1. To upgrade from v7.6.4, back up each blade server and reimage it with the new 7.7.1 image. Then restore your customized files and policies.

- *New in X10G Appliance v7.7.1*, page 2
- *Installation*, page 10
- *Operating tips*, page 11
- *Resolved and known issues*, page 13

The X10G appliance can host the TRITON Web security component of TRITON Enterprise.

Following is a list of the TRITON security modules and their console name.

Software module	Description	Console name
TRITON Unified Security Center	Manages configuration and settings common to all modules. Provides centralized access to consoles.	TRITON Unified Security Center
Websense Web Security	Uses policies to filter Internet requests from clients.	TRITON – Web Security
Network Agent	An Internet traffic sniffer that enforces filtering for protocols other than HTTP and HTTPS.	TRITON – Web Security
Websense Content Gateway	A Web proxy that includes real-time content analysis.	Content Gateway Manager

New in X10G Appliance v7.7.1

Topic 44002 / Updated: 14-August-2012

Applies To:	Websense® X10G Appliance v7.7.1

- *Single sign-on and two-factor authentication*
- *Hotfix management facility*
- *SNMP alerting enhancements*
- *SIEM integration*
- *Support for IPv6*
- *Recovering the admin password*
- *Page-level OK and Cancel operations*
- *Other enhancements*
  - *Security Blade Manager Help available in English only*
  - *Additions to the Command Line Utility*
  - *Additions to the Command Line Interface*

Single sign-on and two-factor authentication

Using the TRITON Unified Security Center, X-Series security blades can be accessed via single sign-on (no-prompt) and two-factor authentication.

Single sign-on

In TRITON Unified Security Center, you can configure administrator accounts for single sign-on (no-prompt) access to the X-Series Security Blade Manager. In this configuration, when the administrator is logged onto TRITON console, she or he can go to the **Appliances** tab, locate the registered security blade he or she wants to access, and click the **Single Sign-On** button to get transparent access to the corresponding Security Blade Manager. See the TRITON console Help system for configuration details. In this configuration, administrators can still access the Security Blade Manager directly via its IP address. The administrator is prompted for credentials.

Two-factor authentication

TRITON console can also be configured as the access point for certificate-based, two-factor authentication.

Two-factor authentication:

- Is configured for and applies to TRITON Unified Security Center logon only.
- 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. See X-Series Security Blade Manager Help.

For more information about configuring two-factor authentication, see “Configuring certificate authentication” in TRITON console Help.

Hotfix management facility

Modeled on the Security Blade Manager patch management facility, the hotfix management facility is an all-inclusive resource for downloading, installing, uninstalling, and maintaining a history of hotfix use on the security blade.

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

In the Security Blade Manager, go to the **Administration** > **Patches / Hotfixes** > **Hotfixes** page to manage hotfixes.

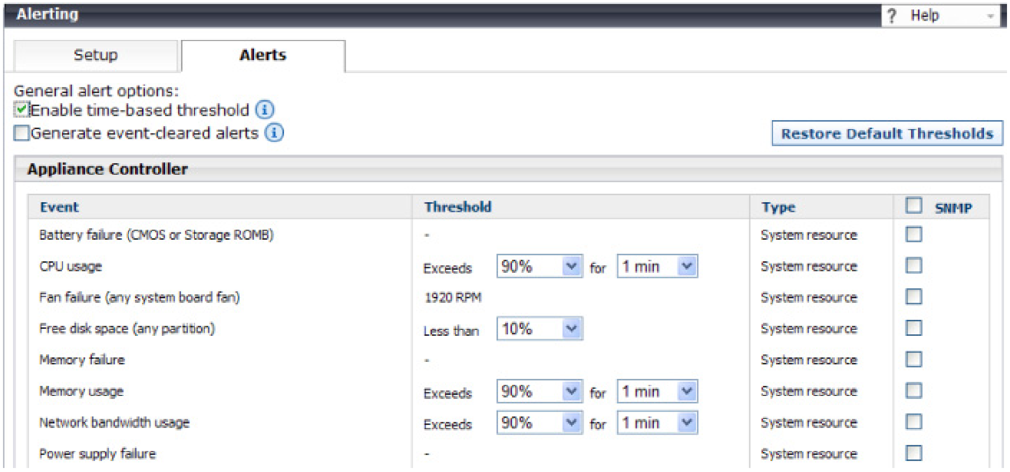
- The Hotfix facility will not install a hotfix that is not valid for the module versions on your security blade.
- A hotfix may have dependencies on or conflicts with other hotfixes, in which case the hotfix facility will not install the hotfix until its dependents are installed or the conflicts are resolved. Specific hotfix dependencies and conflicts are described within the hotfix facility.
- 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 experienced.

See "Hotfix management" in Security Blade Manager Help.

SNMP alerting enhancements

Time-based alert thresholds

Most event alerts that offer a configurable threshold, now also offer a configurable time-based threshold, specified in minutes on the **Configuration** > **Alerting** > **Alerts** page. When the time-based threshold is set and both thresholds are exceeded, an alert is sent. To enabled time-based thresholds, select the **Enable time-based thresholds** check box. The time-based threshold is enabled on every event for which it is configurable.



General alert options:
☑ Enable time-based threshold
☐ Generate event-cleared alerts

Appliance Controller

Event	Threshold	Type	☐ SNMP
Battery failure (CMOS or Storage ROMB)	-	System resource	☐
CPU usage	Exceeds 90% for 1 min	System resource	☐
Fan failure (any system board fan)	1920 RPM	System resource	☐
Free disk space (any partition)	Less than 10%	System resource	☐
Memory failure	-	System resource	☐
Memory usage	Exceeds 90% for 1 min	System resource	☐
Network bandwidth usage	Exceeds 90% for 1 min	System resource	☐
Power supply failure	-	System resource	☐

Event-cleared alerts

In addition to event threshold 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.

The following events do not generate event-cleared alerts:

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

SIEM integration

Log records for traffic managed by Content Gateway and sent to Websense Web Security Filtering Service can also be routed to your Security Information and Event Management (SIEM) solution.

See the section titled, “Integration with third-party SIEM solutions” in the Websense Web Security v7.7 Release Notes.

On X-Series appliances, on the **Full policy source** and each **User directory and filtering** machine, use the **Administration > Toolbox > Command Line Utility** to enable the **multiplexer** service in the Websense Web Security module.

Support for IPv6

Version 7.7 of TRITON Enterprise, including 7.7.1 X-Series appliances, provides incremental support for IPv6.

IPv6 support is included for Websense Web Security, Web Security Gateway, and Web Security Gateway Anywhere.

Important

To use IPv6 with Web Security Gateway (Anywhere), Content Gateway must be deployed as an **explicit proxy**.

IPv6 is **not** supported in transparent proxy deployments.

For Websense Web Security, IPv6 support includes:

- Dual IP stack implementation on interfaces C and N

- IPv6 traffic to the Internet or clients on interface C. For Network Agent (non-HTTP/S traffic), reset packet 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 Websense Web Security Gateway and 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

Limits and restrictions:

- IPv6-only internal networks are not supported
- IPv4 must be used to communicate among X-Series appliances and with TRITON components

See Content Gateway Help for proxy support, limits, and restrictions.

IPv6 configuration summary

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, IPv6 support is enabled for all affected capabilities on the appliance.

In any field that accepts an IPv6 address, the address can be entered in any format that conforms with the standard. For example:

- Leading zeros within a 16-bit value may be omitted
- One group of consecutive zeros may be replaced with a double colon

Disabling IPv6 support requires a full restart of the appliance.

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

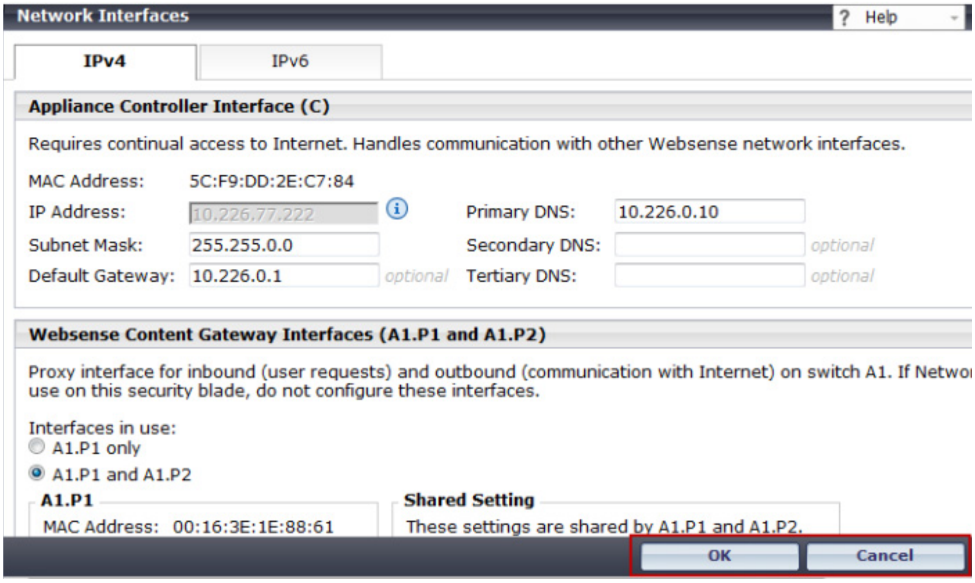
Recovering the admin password

The password recovery (reset) method for the Security Blade Manager “admin” account has been expanded to use a pre-configured email account to which a temporary password is sent when the “Forgot my password” link is clicked on the login page.

If the email account and SMTP service information are not configured, the recovery method falls back to providing a passcode for use when contacting Technical Support.

Page-level OK and Cancel operations

To be consistent with the work flow of other TRITON managers, many Security Blade Manager configuration pages have moved from a unit-level “Save” activity model to a page-level “OK/ Cancel” model.



Network Interfaces

Appliance Controller Interface (C)

Requires continual access to Internet. Handles communication with other Websense network interfaces.

MAC Address: 5C:F9:DD:2E:C7:84

IP Address: 10.226.77.222

Subnet Mask: 255.255.0.0

Default Gateway: 10.226.0.1 optional

Primary DNS: 10.226.0.10

Secondary DNS: optional

Tertiary DNS: optional

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

Proxy interface for inbound (user requests) and outbound (communication with Internet) on switch A1. If Netwo
use on this security blade, do not configure these interfaces.

Interfaces in use:

○ A1.P1 only

● A1.P1 and A1.P2

A1.P1

MAC Address: 00:16:3E:1E:88:61

Shared Setting

These settings are shared by A1.P1 and A1.P2.

Other enhancements

Security Blade Manager Help available in English only

Security Blade Manager Help is available only in English at this time.

Additions to the Command Line Utility

These commands have been added to the Command Line Utility:

Command	Description	Parameters
copy-MasterCA	Applies to the Websense Web Security module only. When TRITON console is located on the appliance and a new master certificate is created following changes to the certificate authentication root certificate, use this command to copy the new Master CA to the Websense Web Security module.	None
directory-agent-service	Applies to the Websense Web Security module only. This command disables and enables the directory agent service.	[Action]: Enter **enable** to enable the directory agent service. Enter **disable** to disable the directory agent service.
multiplexer	Applies to the Websense Web Security module only. Enables and disables the Multiplexer service that supports SIEM integrations. See TRITON – Web Security Help.	[Action]: Enter **enable** to enable the Multiplexer service. Enter **disable** to disable the Multiplexer service.
ping6	Checks that a hostname or IPv6 address exists, can accept requests from the selected module, and that DNS is resolving. Use this to test connectivity to another host and to measure response time. **Note:** ping6 is not supported in the Websense Web Security module.	[Destination]: Enter the hostname (for example myintranet.com) or IPv6 address of the host you want to test.
ping6 -I	Checks that a network interface can communicate with a hostname or IPv6 address and that DNS is resolving. Use this to test connectivity to another host, from one of the appliance NICs. **Note:** ping6 -I is not supported in the Websense Web Security module.	[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.

Command	Description	Parameters
route -A inet6 -n	Display the contents of the selected module's kernel IP routing table IPv6 entries in numeric format. This is useful in complex network environments—for example, those with proxy chaining—to see if the environment is set up properly.	None.
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.
traceroute6	Use this to determine the route taken by packets across a network to a particular host. **Note: traceroute6** is not supported in the Websense Web Security module.	[Destination]: Enter the hostname or IP address of the host destination you are investigating
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.	[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.

Additions to the Command Line Interface

Command	Description
admin email	Specify the email address to which password recovery email is sent.
password-logon disable	Disable password logon via IP address and credentials.

Command	Description
password-logon enable	Enable password logon via IP address and credentials.
show password-logon	Show the status of password logon.
show smtp server	Show the SMTP server settings through which password recovery email is routed.
smtp server	Specify the SMTP server through which password recovery email is routed.

Installation

Topic 44003 / Updated: 14-August-2012

Applies To:	Websense X-Series Appliances Version 7.7.1

X-Series appliances are delivered pre-loaded with the software needed for provisioning via the **firstboot** script.

The Quick Start poster and Getting Started Guide are your comprehensive resources for installing the physical unit, running **firstboot**, and completing initial configuration.

Security mode provisioning

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

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

You choose the mode of a blade server during initial *firstboot* configuration,

Web browsers with the Security Blade Manager

X-Series appliances are configured and maintained with a Web-based user interface called the Security Blade Manager. The Security Blade Manager should be used with one of these supported browsers:

- Microsoft Internet Explorer 8 and 9
- Mozilla Firefox versions 5 and later
- Google Chrome 13 and later

✓ **Note**

If you are using Internet Explorer, make sure that Enhanced Security Configuration is turned off.

When you access the Security Blade Manager for the first time, you will get a certificate warning because the Security Blade Manager offers a self-signed certificate. To eliminate the warnings, install the certificate into your browser's CA store. For instructions, see your browser documentation.

Downloading the TRITON Unified Security Center Installer

The TRITON Unified Security Center and several support components are installed off of the appliance, on separate servers.

To download the TRITON version 7.7 Installer:

1. Go to mywebsense.com and log in to your account.

   You are taken to the My Products and Subscriptions page.
2. Click the **Downloads** tab.
3. Under Download Product Installers, select your **Product and Version** (7.7).

   The available installers are listed under the form.
4. Click the plus sign ("+") next to an installer entry for more information about the installer.
5. Click the **download** link to download the installer.

Operating tips

Topic 44004 / Updated: 14-August-2012

Applies To:	Websense X-Series Appliances Version 7.7.1

Interface setup tip

If the A1.P2 interface is used and it is in the same subnet as A1.P1, the default gateway is automatically assigned to A1.P2, which is bound to eth1. You should perform a test to ensure that outbound packets can reach the Internet.

Avoiding port conflicts

See the ports list for a table of the Websense software module versions that are compatible with each appliance version.

Check the ports article to avoid port conflicts if you plan to make a change from a default port.

For example, if you want to use an HTTP proxy server port that is different from the default port (8080), be sure to check the ports list first, to avoid conflict with ports already in use by the X-Series.

Logging tip

If you want to examine log files for Network Agent in Security Blade Manager, be sure to turn on Network Agent logging in the TRITON - Web Security console first. To do this, log on to **TRITON - Web Security** and navigate to the **Settings > Network Agent > Global**. Hover over **Global** and select the Network Agent IP address that you're interested in. At the bottom of the page, open **Advanced Network Agent Settings**, go to the **Debug Settings** area, and set **Mode**, **Output**, and **Port**.

Deployment tips

- When Policy Broker is run on a X-Series appliance (configured as the **Full policy source**), all Policy Servers that point to that Policy Broker (configured as **User directory and filtering**) must be installed on X-Series appliances as well. You cannot install and run Policy Servers on off-box machines and point them to a Policy Broker that runs on an appliance. This configuration is not supported.

  However, you can run Policy Server on multiple appliances (**User directory and filtering** mode) and point these appliances to a Policy Broker running either on or off an appliance.
- When Web Security Gateway (Anywhere) is deployed and Content Gateway **Integrated Windows Authentication** (IWA) is configured, if the appliance hostname is changed, IWA will immediately stop working. To repair the IWA configuration, log onto Content Gateway Manager, unjoin the stale domain and join the domain with the new hostname.

- Websense Web Security Log Server now supports **SQL Server SSL encryption**. However, if you are running TRITON – Web Security (manager) on the appliance (not the recommended deployment), the connection from the console to the database **cannot be encrypted**. This means that if the Microsoft SQL Server "Force Protocol Encryption" option is set to Yes, no data will appear in the Web Security Dashboard or other reporting tools.

Subscription key tips

In a deployment with multiple Policy Server appliances, use the Web Security Gateway Anywhere subscription key for the policy source appliance (the Policy Server that connects to Sync Service), and use a Web Security Gateway subscription key for all other appliances. Otherwise, you receive superfluous hybrid filtering alerts.

Backup and restore tips

- When configuring schedule backups to a remote storage location (FTP server or Samba share), make sure that the account used for backup file creation has **read** and **write** permissions. If you plan to use the option to automatically delete backup files older than some period of time, you must use an account that has **delete** permissions for the backup file directory and its subdirectories.
- In a multiple security blade deployment, after restoring the configuration of a **Policy source** security blade, restart any **Filtering only** or **User directory and filtering** security blades in your network to ensure that user requests are filtered correctly.

Resolved and known issues

Topic 44005 / Updated: 14-August-2012

Applies To:	Websense® X-Series Appliances v7.7.1

A list of resolved and known issues in this release is available to customers with a current MyWebsense account.

If you are not currently logged in to MyWebsense, the link takes you to a login prompt. Log in to view the list.