



Release Notes for 3Com X Family of Unified Security Platforms, Release 2.5.2

This document contains information about Release 2.5.2 of the 3Com X family of Unified Security Platforms. This information is not available in the documentation that is included on the documentation CD.

Customer Support

For product support of the 3Com X family of Unified Security Platforms, contact 3Com in one of these ways:

Telephone:

USA and Canada toll free: 1 888 547 3266

International toll free: AT&T Access Code + 1 888 547 3266
(For a list of AT&T Access Codes, visit http://www.consumer.att.com/global/english/access_codes.html)

Toll number: + 1 407 235 7000

E-mail: tech_support@3com.com

Documentation

For complete documentation, see the following publications available from the Documentation CD or 3Com at <http://www.3com.com>:

- *X Family of Security Devices Hardware Installation Guide*
- *Quick Start 3Com X5*
- *Quick Start 3Com X506 Security Device*
- *1U Rack Mounting Bracket Installation (X506 only)*
- *X Family Concepts Guide*
- *X Family Local Security Manager User's Guide*
- *X Family Command Line Interface Reference*
- *TippingPoint Security Management System Installation and Configuration Guide*
- *TippingPoint Security Management System User's Guide*

For the most up-to-date version of documentation, check the 3Com Web site.

New Features at Release 2.5.2

As described in the following sections, several new features have been added at this release.

DIGITAL VACCINE SUPPORT

TippingPoint has made enhancements to the Digital Vaccine packages in Release 2.5.2. Digital Vaccine packages that support Release 2.5.2 will not work on older versions of the X family software.

CUSTOM SHIELD WRITER (CSW)

Release 2.5.2 supports Custom Shield Writer (CSW) packages.

PERFORMANCE PROTECTION FILTERS

New features have been added to Performance Protection filters. Performance Protection filters include the IM, P2P, and Streaming Media filter sub-categories.

- You can assign any action set that uses a Permit action to Performance Protection filters.
- Per-filter exceptions are now supported on Performance Protection filters.

For detailed information about working with Performance Protection filters, refer to the *Local Security Manager User's Guide*.

Issues Resolved at Release 2.5.2

INTERNET EXPLORER 7.0 SUPPORT

X family software now supports Microsoft Internet Explorer 7.

ENGINE MEMORY LEAK

Certain patterns of fragmented IP traffic could cause memory leaks. This issue has been resolved.

FALSE ERRORS IN THE CLI

The CLI command `clear configuration` no longer generates false "Unknown notification contact" errors.

FILE DESCRIPTOR LEAK

A file descriptor leak could interrupt device management. This issue has been resolved.

PORT SETTINGS

When you changed auto-negotiation, duplex, or port speed settings, the port could be disabled when the device was rebooted. This issue has been resolved.

SYSTEM LOG SEARCH AND DAYLIGHT SAVINGS TIME

During Daylight Savings Time, System Log search results now display correctly.

REMOTE SYSTEM LOG SERVER CONFIGURATION

The LSM would not allow configuration of remote system log servers for firewall session logs, VPN logs, system logs, and audit logs. This issue has been resolved.

WEB INTERFACE HANGS WHEN ACCESSING NETWORK > TOOLS

A problem has been resolved where the LSM might hang when entering the **Network > Tools** menu.

WINDOWS VISTA L2TP CLIENT AND NAT-T

A problem has been resolved when using a Windows Vista PC to create an L2TP tunnel to an X family device when there is also client-side NAT device between the two.

VIRTUAL SERVER LIMIT INCREASED

The maximum virtual server count has been increased for all X family platforms:

- X5: 25 (with 25-user license) or 50 (with unlimited license)
- X506: 500

Migration Issues

Before upgrading from Release V 2.5+ to Release 2.5.2, review the following migration issues to determine whether your system requires any configuration adjustments before or after migration.

- To upgrade from Release 2.5 to Release 2.5.2, you must first upgrade to Release 2.5.1.
- To upgrade your X family device to Release 2.5.2, first download and install the TOS Release 2.5.2 software package. Then, download and install a Release 2.5.2 Digital Vaccine package. You can install the updated packages from the LSM (**System > Update**). For details, see the *Local Security Manager User's Guide* or the Online Help.
- If you use the Security Management System (SMS) to manage your X family device, you must install SMS Release 2.5.2 on your management device before you upgrade the device to Release 2.5.2. Prior versions of the SMS will not support Release 2.5.2.
- If you see the following message in the system log after migration, verify the Traffic Threshold filter configuration on the device and update the configuration as required:

```
Traffic threshold profile cannot be assigned to a virtual segment
```

INTERNET EXPLORER CACHE SETTINGS AND COOKIES

Set your Internet Explorer cache setting for enhanced browser performance, as follows:

1. Select **Tools > Internet Options**. The Internet Options window opens.
2. On the General tab, select the Settings option for "Temporary Internet files."

3. In the “Check for newer versions” section of the tab, check “Every visit to the page.”
4. Click OK to save these settings.
5. Click OK to close the Internet Options window.

Cookies for previous versions of the LSM may conflict with cookies in Release 2.5.2. If your browser receives unexpected “404 Page Not Found” errors or displays blank LSM frames, the cookies on your computer may be out of sync. To remedy this, delete the existing cookies and open a new session, as follows:

1. Select **Tools > Internet Options**. The Internet Options window opens.
2. On the General tab, click “Delete Cookies.”
3. Click OK to save these settings.
4. Click OK to close the Internet Options window.
5. Restart Internet Explorer.
6. Connect to the LSM and continue as before.

Known Issues and Notes for Release 2.5.2

FILTER CONFIGURATION FOR TRAFFIC MANAGEMENT AND TRAFFIC THRESHOLD

When you define a Traffic Management Profile or Traffic Threshold filter, the specified zone pair must also have a security profile explicitly assigned to it. If a security profile is not defined, the traffic between the zones will not be inspected by the IPS service. For example, if the only security profile configured on a device is the default (ANY <==> ANY) and you create a Traffic Threshold profile to apply to traffic on the zone pair LAN <==> WAN, you must create a security profile that explicitly applies to the LAN <==> WAN zone pair, or add this zone pair to an existing security profile. If a security profile for a zone pair is missing, the Virtual Segments table on the LSM Security Profiles page table displays the following error message:

```
No security profile is assigned to the in/out pair. Traffic will NOT be inspected against DV filter policies
```

LINE SPEED SETTINGS USING THE CLI

The X family device does not support manual configuration of copper ports to a line speed of 1000 Mbps, and the LSM will not permit this action. However, the CLI still appears to let you set the line speed at 1000 Mbps. Avoid this action, as it will lead to link issues and inconsistencies between the settings displayed in the LSM and CLI.

RESETTING FILTERS

In Release 2.5.2, the Reset button (formerly labeled Reset Filters) resets security profiles, action sets, notifications, traffic threshold filters, and traffic management profiles.

If you want to reset your filter settings, instead of using the Reset button, we recommend that you remove the relevant security profile and then re-add it.

IPS FILTER OVERRIDES

When you create a filter override to enable a filter, you must select an Action for the filter. Do not leave the Action set as *Recommended*.

WEB-BASED SETUP WIZARD

IP Interface Setup

The web-based installation wizard allows you to configure basic X family settings. When you are initially configuring the IP interfaces, do not select the option to set up the GRE Tunnel interface. This advanced configuration option should not be selected or configured during initial setup.

After you complete the initial setup, you can configure GRE Tunnel interfaces from the IP Interfaces page in the LSM (**Network > Configuration > IP Interfaces**). For details on configuring a GRE tunnel, see the X Family Online Help.

Error Message “Unable to configure while NTP client is enabled”

If the device has already been configured and you return to the Setup Wizard to make configuration changes, you may see this error message: “Unable to configure while NTP client is enabled.” The installation wizard is trying to set the system clock manually even though NTP is enabled. Ignore this message and make any necessary configuration changes. When you save the changes, they will be applied correctly.

WEB FILTER CONFIGURATION

Web Filter Firewall Rule

When you enable Manual URL Filtering on the LSM (**Firewall > Web Filtering**, click Custom Filter List tab), you have an option to create a default firewall rule. This rule is required to use Web filtering. If you select this option and click Apply, the system automatically creates the required firewall rule and appends it to the end of the firewall rule table. However, in many configurations, adding the rule to the end of the table will have no effect: higher-precedence rules will be executed before the Web filtering rule, and the traffic will never be evaluated against the Web filters configured on the device.

Workaround: After you save your Manual URL filtering changes, go to the Firewall Rules table (**Firewall > Firewall Rules**) and move the Web filtering rule to the top of the list. Then any traffic to the device will first be evaluated against the manual Web filters configured on the device.

Custom Filter Lists

When you enter URL patterns or regular expressions in the Custom Filter List (**Web Filter > Custom Filter List**), limit the URL pattern or expression to 64 characters or fewer. If you enter a pattern or expression longer than 64 characters, the system may drop the pattern without issuing an error.

NTP SERVER CONFIGURATION

You can configure a maximum of four NTP servers on the device. If you try to configure a fifth NTP server, you will lose the settings for all of the NTP servers already configured on the device.

Workaround: If you have configured four NTP servers on the device and need to add another, delete one of the existing servers first.

HIGH AVAILABILITY

Release 2.5.2 supports redundant X family devices. The High Availability (HA) feature allows for a primary and a standby device, with the standby device automatically taking over if the primary device fails. Note the following requirements:

1. You need a separate DV license for the standby device.
2. To allow the standby device to automatically download DV updates, verify that both devices are configured with an HA management IP address on the external virtual interface and that this address can reach the Internet.

DHCP CONFIGURATION

To configure the X family device as a DHCP server, both of the following firewall rules are required to permit the DHCP protocol to and from the client:

Action	Source	Destination	Service
Permit	LAN	this-device	dhcp-server
Permit	this-device	LAN	dhcp-client

Documentation Errata

The following errors were discovered after the documentation was completed.

COMMAND LINE INTERFACE REFERENCE

On pages 62 and 63, replace the description of the command **conf t remote-syslog** with the following:

conf t remote-syslog [no] [logname] ip [-port port]

The **configure terminal remote-syslog** command configures a remote syslog server to record device notifications. Many operating systems and third-party remote syslog packages provide the ability to receive remote syslog messages. You can create multiple alert/block logs; in addition, you can create one audit, firewall session, system, and VPN log.



Note: For an alert/block log, designating a remote syslog server does not automatically send notifications to that server. Log entries must be generated that will be sent to the syslog server, normally as a result of inspecting network traffic. For the IPS Block log you must also select the appropriate Remote System Log contact by going to the Filters/Vulnerability filters/Action Sets area in the LSM and either creating or editing an action set. After you apply these changes, active filters that are associated with this action set will send remote messages to the designated server.

For a firewall log, the syslog server must be specified and then the appropriate firewall rules modified to enable remote syslog.



CAUTION: Only use remote syslog on a secure, trusted network. Remote syslog, in adherence to RFC 3164, sends clear-text log messages using the UDP protocol. It does not offer any additional security protections. You should not use remote syslog unless you can be sure that syslog messages will not be intercepted, altered, or spoofed by a third party.

logname

One of the following:

audit

Audit log

firewallsession

Firewall session log

system

System log

vpn

VPN log

ip [-port port]

IP address and port number (1–65535) of the remote syslog server.

delete ip [-port port]

Stop logging to a remote syslog alert/block collector at IP address *ip* and port number *port* (1–65535). (To stop other kinds of remote logs, use **no**.)

no

Stops logging to the remote syslog server for the specified log (audit, firewall session, system, or VPN).

update ip [-port port]

For the IPS Alert/Block log only, creates or updates a remote syslog alert/block collector. The facility numbers are optional.

[-alert-facility 0-31]

Optional facility setting for alerts. The range is 0–31.

[-block-facility 0-31]

Optional facility setting for blocks. The range is 0–31.

[-delimiter < tab | comma | semicolon | bar >]

Setting for the log delimiter. Valid delimiters are tab, comma (,), semicolon (;), and bar (|).

Using `conf t remote-syslog`

designate a system to receive remote syslog alert/block messages Use **configure terminal remote-syslog update ip -port port** to designate a remote syslog alert/block log. In this example, remote syslog alert/block logs are configured on the IP addresses 1.2.3.4, port 514 and 1.2.3.5, port 514:

```
hostname# conf t remote-syslog upd 1.2.3.4 -port 514
hostname# conf t remote-syslog upd 1.2.3.5 -port 514
```

designate a remote system to receive VPN messages Use **configure terminal remote-syslog vpn ip -port port** to designate a remote syslog VPN log. In this example, the remote syslog VPN log is configured on the IP address 1.2.3.4, port 514:

```
hostname# conf t remote-syslog vpn 1.2.3.4 -port 514
```

stop sending alert/block messages to a remote system Use **configure terminal remote-syslog delete ip -port port** to stop sending syslog alert/block messages to the remote system at 1.2.3.4, port 514:

```
hostname# conf t remote-syslog delete 1.2.3.4 -port 514
```

stop sending VPN messages to a remote system Use **configure terminal remote-syslog no vpn** to stop sending syslog VPN messages to the remote system:

```
hostname# conf t remote-syslog no vpn
```

On page 81, remove the description of the command `debug log syslog` and its parameters. This command is not supported.

Copyright © 2007, 3Com Corporation. All Rights Reserved.
Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may be registered in other countries.

3Com, the 3Com logo, TippingPoint, the TippingPoint logo, and Digital Vaccine are registered trademarks of 3Com Corporation or one of its subsidiaries. Other brand and product names may be registered trademarks or trademarks of their respective holders.

Part Number: TECHD-000000221 B01
August 2007