



3Com® X Family Local Security Manager User's Guide



X5 (25-user license) – 3CRTPX5-25-96
X5 (unlimited license) – 3CRTPX5-U-96
X506 – 3CRX506-96

Version 3.0

Part Number 10016444
Published November 2007
<http://www.3com.com/>



3Com Corporation
350 Campus Drive
Marlborough, MA
01752-3064

Copyright © 2005–2007, 3Com Corporation and its subsidiaries. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms, or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hardcopy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGENDS:

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

United States Government Legend: All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not 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.

Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Oracle is a registered trademark of Oracle Corporation.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

Contents

About This Guide	xi
Target Audience	xi
Knowledge, Skills, and Abilities	xi
Conventions	xii
Cross References	xii
Internal Cross References	xii
External Cross References	xii
Typeface	xii
Procedures	xii
Menu Navigation	xiii
Screen Captures	xiii
Messages	xiii
Warning	xiii
Caution	xiii
Note	xiv
Tip	xiv
Related Documentation	xiv
Online Help	xiv
Customer Support	xiv
Contact Information	xv
Chapter 1. System Overview	1
Overview	1
X Family Device	2
Core Functionality	3
X Family Environment	4
Local Clients	4
System Requirements	5
SMS Configuration	5
Chapter 2. LSM Navigation	7
Overview	7
Security Notes	7
Logging In	8
LSM Screen Layout	10
Main Menu Bar	11
Navigation	12
Content and Functionality	13
Title Bar	13

Auto Refresh	13
Tabbed Menu Options	13
System Summary	14
System Status	14
Health	14
Packet Stats	15
Network DHCP	15
Reboot Device	15
Log Summary	15
Product Specifications	16

Chapter 3. IPS Filtering 17

Overview	17
Using the IPS	18
Security Profiles	19
Managing Security Profiles	20
Security Profile Details	21
IPS Digital Vaccine Filters	24
Configuring DV Filters	24
Viewing DV Filters	24
Filter Search	25
Filters List (All Filters)	26
Editing DV Filter Category Settings	29
Configuring Filter Limits and Exceptions Based on IP Address	33
Resetting an Individual Filter	34
Port Scan/Host Sweep Filters	35
Traffic Threshold Filters	37
Managing Traffic Threshold Filters	38
Creating or Editing a Traffic Threshold Filter	40
Action Sets	42
Managing Actions	44
Rate Limit Action Set	46
Quarantine Action Set	46
Notification Contacts	49
Alert Aggregation and the Aggregation Period	49
IPS Services	52
Preferences	54
Reset Filters	55
Configuring the Threat Suppression Engine	55
Adaptive Filter Configuration	56
How Adaptive Filtering Works	57

Chapter 4. Firewall 59

Overview	59
----------	----

Default Firewall Rules	61
Setting Up Firewall Rules	62
Step 1: Creating Services	62
Step 2: Creating Service Groups	62
Step 3: Creating Schedules	63
Step 4: Creating Firewall Rules	63
Step 5: Allowing Access to Internal Servers	65
Step 6: Configuring One-to-One NAT	66
Managing Firewall Rules	66
Configuring Firewall Rule Components	68
Firewall Services	73
Firewall Services Page Field Descriptions	75
Configuring Service Groups	76
Schedules	77
Firewall Schedules Page Field Descriptions	78
Managing Schedules	78
Virtual Servers	80
Virtual Servers Page	80
Configuring Virtual Servers	81
Web Content Filtering	84
Setting Up Web Content Filtering	84
Web Filtering Page	85
Web Filter Profiles	87
Configuring URL Patterns	91
Anti-Spam	94
Anti-Spam Page	95
Setting Up Anti-Spam Filtering	96
Testing an IP Address	98

Chapter 5. Events: Logs, Traffic Streams, and Reports **99**

Overview	99
Logs	100
Alert Log	100
Audit Log	101
IPS Block Log	102
Firewall Block Log	103
Firewall Session Log	104
VPN Log	105
System Log	106
Configuring Remote System Logs	107
Managing Logs	108
Viewing Logs	109
Downloading a Log	109
Resetting a Log	110

Searching a Log	110
Managed Streams	111
Blocked Streams Page	112
Rate Limited Streams Page	114
Quarantined Addresses Page	115
Health	117
Device Health	118
Memory and Disk Usage	118
Module Health	119
Performance/Throughput	121
Port Health	121
Reports	122
Attack Reports	123
Rate Limit Reports	124
Traffic Reports	124
Traffic Threshold Report	124
Quarantine Report	125
Configure Adaptive Filter Events Report Page	125
Firewall Reports	126

Chapter 6. Network 129

Overview	129
Configuration Overview	130
Deployment Modes	131
Network Ports Page	133
Troubleshooting Port Link-Down Errors	135
Security Zone Configuration	135
Creating, Editing, and Configuring Security Zones	137
IP Interfaces	141
Configuration Overview	141
IP Interfaces Page	142
IP Addresses: Configuration Overview	143
Internal Interface: Static IP Address	144
External Interface: Static IP Address Configuration	145
External Interface: DHCP Configuration	146
External Interface: PPTP Client Configuration	146
External Interface: L2TP Client Configuration	147
External Interface: PPPoE Client Configuration	148
Configuring a GRE Tunnel	149
Managing Security Zones for IP Interfaces	150
Configuring Routing for IP Interfaces	151
Bridge Mode for IP Interfaces	151
OSPF for IP Interfaces	152
RIP for IP Interfaces	153
Multicast Routing for IP Interfaces	155

IP Address Groups Page	156
DNS Page	159
Default Gateway Page	159
Dynamic DNS Page	160
WAN Failover and Load Balancing Page	164
Link Monitoring	165
Failover	166
Load Balancing	166
Routing	167
Routing Table Page	167
Static Routes Page	169
RIP Setup Page	171
OSPF Setup Page	174
Troubleshooting OSPF Configurations	179
Multicast Routing (IGMP and PIM-DM)	180
IGMP Setup Page	181
PIM-DM Setup Page	183
DHCP Server	185
DHCP Server Page	185
Configuring the DHCP Server	187
DHCP Relay Page	189
Configuring DHCP Relay	189
Static Reservations Page	191
Network Tools	193
DNS Lookup	193
Find Network Path	194
Traffic Capture	194
Ping	195
Traceroute	196

Chapter 7. VPN 199

Overview	199
VPN Configuration Overview	200
IPSec Configuration	201
IPSec Status Details	202
IPSec Configuration Page	203
Configuring an IPSec Security Association	206
IKE Proposal	215
Managing IKE Proposals	215
Configuring IKE Proposals	217
Client-to-Site Configuration	223
Troubleshooting Client-to-Site Configuration	224
L2TP Configuration	225
L2TP/IPSec VPN Configuration	225
L2TP Status	229

L2TP Server Configuration Page	230
Configuring Client-to-Site VPNs for Windows Clients	232
Client PPTP VPN Access Configuration	232
Troubleshooting L2TP/IPSec Connections	235
PPTP Configuration	236
PPTP Status Page	236
PPTP Server Configuration Page	238
Troubleshooting PPTP Connections	240

Chapter 8. System 241

Overview	241
Updating TOS and Digital Vaccine Software	242
Viewing and Managing Current TOS and DV Software	243
Rolling back to a previous TOS version	244
Downloading and Installing a TOS or DV Update	246
Updating Digital Vaccine (Filters)	246
Updating the TOS Software	248
System Snapshots	251
Time Options	254
Internal Clock	255
NTP Server	256
Time Zones	257
Security Management System (SMS)	258
Management by Third-Party NMS Software	260
High Availability	260
Configuration Overview	260
Configuring High Availability with AutoDV	265
Troubleshooting High Availability with AutoDV	265
Thresholds to Monitor Memory and Disk Usage	265
Email Server	266
Syslog Servers	267
Setup Wizard	268

Chapter 9. Authentication 271

Overview	271
User List Page	272
TOS and Local User Accounts	272
TOS User Security Level	273
Username and Password Requirements	273
Managing User Accounts	274
User Account Parameter Details	275
Active User List	277
Privilege Groups Page	278
Privilege Group Parameter Details	279
RADIUS Page	280

LDAP Configuration Page	282
X.509 Certificates	286
Configuring X.509 Certificates	286
CA Certificate Page	287
Current CA Certificates Parameter Details	288
Certificate Revocation List (CRL) for a CA Certificate	289
X.509 CA Certificates Parameter Details	290
Certificate Requests Page	291
Certificate Requests Parameter Details	293
Managing Certificate Requests	293
Local Certificates Page	295
Local Certificate Parameter Details	296
Preferences Page	298
Preferences Parameter Details	298
Setting Up User Authentication	301

Appendix A. Browser Certificates 303

Overview	303
Client Authentication Message	304
Security Alert	306
Certificate Authority	306
Invalid Certificate Name	311
Example — Creating a Personal Certificate	313

Appendix B. Log Formats and System Messages 315

Overview	315
Log Formats	316
Alert and IPS Block Log Formats	316
Audit Log Format	319
Firewall Block Log Format	320
Firewall Session Log Format	323
VPN Log Format	324
System Log Format	325
Remote Syslog Log Format	326
High Availability Log Messages	327
System Update Status Messages	328

Appendix C. Device Maximum Values 331

Index 335

About This Guide

Explains who this guide is intended for, how the information is organized, where information updates can be found, and how to obtain customer support if you cannot resolve a problem.

Welcome to the Local Security Manager (LSM). The LSM is the control center from which you can configure, monitor, and report on the X family of Unified Security Platforms in your network.

This section covers the following topics:

- [“Target Audience” on page xi](#)
- [“Conventions” on page xii](#)
- [“Related Documentation” on page xiv](#)
- [“Customer Support” on page xiv](#)

Target Audience

This guide is intended for administrators who manage one or more X family devices.

Knowledge, Skills, and Abilities

This guide assumes that you are familiar with general networking concepts and the following standards and protocols:

- Transmission Control Protocol/Internet Protocol (TCP/IP)
- User Datagram Protocol (UDP)
- Internet Control Message Protocol (ICMP)
- Ethernet
- Simple Network Time Protocol (SNTP)
- Simple Mail Transport Protocol (SMTP)
- Simple Network Management Protocol (SNMP)

Conventions

This guide follows several procedural and typographical conventions to better provide clear and understandable instructions and descriptions. These conventions are described in the following sections.

This guide uses the following conventions for structuring information:

- [Cross References](#)
- [Typeface](#)
- [Procedures](#)
- [Screen Captures](#)
- [Messages](#)

Cross References

When a topic is covered in depth elsewhere in this guide, or in another guide in this series, a cross reference to the additional information is provided. Cross references help you find related topics and information quickly.

Internal Cross References

This guide is designed to be used as an electronic document. It contains cross references to other sections of the document that act as hyperlinks when you view the document online. The following text is a hyperlink: [Procedures](#).

External Cross References

Cross references to other publications are not hyperlinked. These cross references will take the form: see <chapter name > in the *Publication Name*.

Typeface

This guide uses the following typeface conventions:

Bold	used for the names of screen elements like buttons, drop-down lists, or fields. For example, when you are done with a dialog, you would click the OK button. See Procedures below for an example.
Code	used for text a user must type to use the product
<i>Italic</i>	used for guide titles, variables, and important terms
Hyperlink	used for cross references in a document or links to a Web site

Procedures

This guide contains step-by-step procedures that tell you how to perform a specific task. These procedures always begin with a phrase that describes the task goal, followed by numbered steps that describe what you must do to complete the task.

The beginning of every chapter has cross references to the procedures that it contains. These cross references, like all cross references in this guide, are hyperlinked.

Menu Navigation

The LSM provides drop-down menu lists to navigate and choose items in the user interface. Each instruction that requires moving through the menus uses a greater-than sign (>) to indicate the progression. For example, **Edit > Details** means to select the **Edit** menu item and then click the **Details** option.

Sample Procedure:

STEP 1 Click the **Filters** tab.

STEP 2 Place your mouse cursor over the **Open** menu.

Screen Captures

The instructions and descriptions in this document include images of screens. These screen captures may be cropped, focusing on specific sections of the application, such as a pane, list, or tab. See the application for full displays of the application.

Messages

Messages are special text that are emphasized by font, format, and icons. There are four types of messages in this guide:

- [Warning](#)
- [Caution](#)
- [Note](#)
- [Tip](#)

A description of each message type with an example message follows.

Warning

Warnings tell you how to avoid physical injury to people or equipment. For example:



WARNING The push-button on/off power switch on the front panel of the server does not turn off the AC power. To remove AC power from the server, you must unplug the AC power cord from either the power supply or the wall outlet.

Caution

Cautions tell you how to avoid a serious loss of data, time, or security. You should carefully consider this information when determining a course of action or procedure. For example:



CAUTION You should disable password caching in the browser you use to access the LSM. If you do not disable password caching in your browser, and your workstation is not secured, your system security may be compromised.

Note

Notes tell you about information that might not be obvious or that does not relate directly to the current topic, but that may affect relevant behavior. For example:



Note If the device is not currently under SMS control, you can find out the IP address of the last SMS that was in control by checking the SMS & NMS page (**System > Configuration > SMS/NMS**).

Tip

Tips are suggestions about how you can perform a task more easily or efficiently. For example:



TIP You can see what percentage of disk space you are using by checking the Monitor page (**Events > Health > Monitor**).

Related Documentation

The X family products have a full set of documentation. These publications are available in electronic format. For the latest information and associated documentation, go to the 3Com Web site (<http://www.3com.com/products>).

Online Help

In the Launch Bar of the application, the **Help** button opens the main welcome page to the online help.



Opens the online help at the opening page.

If you have problems finding help on a particular subject, you can review the Index or use the Search tab in the navigation pane. Each page also includes related topic links to find more information on particular subjects and functions.

Customer Support

We are committed to providing quality customer support to all customers. A customer is provided with detailed customer and support contact information. For the most efficient resolution of your problem,

please take a moment to gather some basic information from your records and from your system before contacting customer support.

Information	Location
Your device serial number	You can find this number in the LSM in the System Summary page, on the shipping invoice that came with the device, or on the bottom of the device.
Your TOS version number	You can find this information in the LSM in the Device Summary page, or by using the CLI <code>show version</code> command.
Your device boot time	You can find this information in the LSM in the System Summary page.

Contact Information

Please address all questions regarding the software to your authorized representative.

1 System Overview

The X family of Unified Security Platforms are high-speed, comprehensive security systems with a browser-based manager called the Local Security Manager (LSM). This section provides an overview of LSM functions and its use in an X family device.

Overview

Enterprise security schemes once consisted of a conglomeration of disparate, static devices from multiple vendors. Today, the X family of Unified Security Platforms provides the advantages of a single, integrated, highly adaptive security system that includes powerful hardware and an intuitive management interface.

This chapter describes the X family device and the Local Security Manager (LSM) client application, Command Line Interface (CLI), and Security Management System (SMS) used to interact with and manage the device.

This chapter includes the following topics:

- [“X Family Device” on page 2](#)
 - [“Core Functionality” on page 3](#)
 - [“X Family Environment” on page 4](#)
- [“Local Clients” on page 4](#)
 - [“System Requirements” on page 5](#)
 - [“SMS Configuration” on page 5](#)



Note Check the **Release Notes** for specific limitations and known issues regarding the current release.

X Family Device

The X family device offers an integrated system that includes a stateful packet inspection firewall, IPSec virtual private network (VPN) management, bandwidth management, and Web content filtering functions along with TippingPoint™ Intrusion Prevention System (IPS) functionality.

Firewall functionality provides service-level, stateful inspection of network traffic. It incorporates filtering functionality to protect mission-critical applications. An administrator can use firewalls and content filters to determine how the device handles traffic to and from a particular service. These filters are specified by the source, destination, and service or protocol of the traffic. The device maintains an inventory of the active hosts and services on those hosts.

IPSec VPN management provides the ability to apply all X family functionality across the enterprise, monitoring network traffic at the enterprise level and also between main office and branch locations.

Bandwidth management, or policy-based traffic shaping, allows the device to control both inbound and outbound traffic streams as well as inside and outside IPSec VPN tunnels. Using these policies, the device allows users to prioritize real-time business-critical applications including video and conferencing, IP telephony, and interactive distance-learning over non-essential traffic, such as peer-to-peer file sharing.

Web content filtering provides the tools to enforce network policy by prohibiting the download of non-work related Web sites and offensive or illegal Web content. In addition, spam filtering blocks spam, phishing, and virus email based on real-time analysis of the IP addresses of senders.

The IPS functionality provides total packet inspection and intrusion prevention to detect and block malicious traffic such as worms, viruses, trojans, phishing attempts, spyware, and VoIP threats. Using filters defined by the Digital Vaccine security team, the device scans traffic to recognize header or data content that signals an attack along with the protocol, service, and the operating system or software the attack affects. Each filter includes an action set, which determines how the device responds when it detects packets that match filter parameters. In a broad sense, the device either drops matching packets or permits them. The Digital Vaccine security team continually develops new attack filters to preemptively protect against the exploit of new and zero-day vulnerabilities. To ensure up-to-date network protection, you can configure the device to automatically check for and install DV updates.

Core Functionality

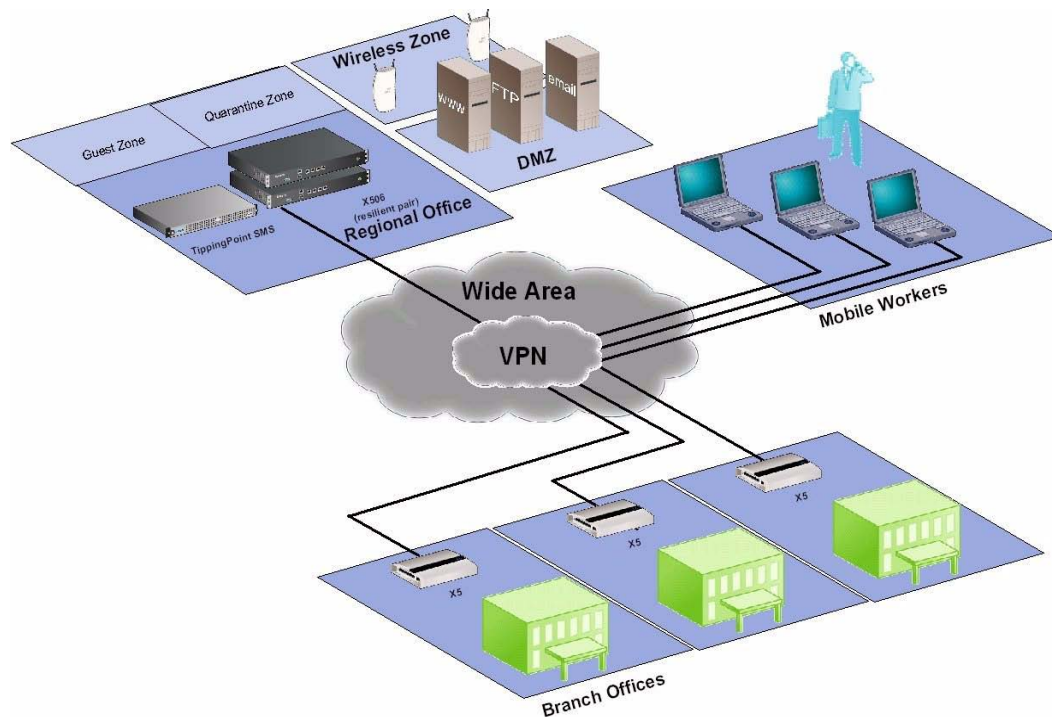
The X family device provides the following core functionality:

- Stateful packet inspection firewall — flexible configuration of object-based firewall rules and unified control of multiple services, virtual servers, network address translation (NAT), and routing.
- Security Zones — logically section your network for the purposes of applying firewall rules and IPS filters between internal sections of your network, between your network and the Internet, and between your network and remote office locations.
- Standards-based IPSec Virtual Private Networks (VPNs), including:
 - Hardware-accelerated encryption using DES, 3DES, and AES encryption protocols
 - Feature-rich client VPN capability using PPTP or L2TP protocols
 - Inspection and control of traffic both inside and outside of all VPN tunnel types using firewalls or IPS to ensure secure VPN connectivity
- Flexible user authentication — control access to the device and the Internet, authenticating via the device itself or through an external RADIUS database.
- Web content filtering and anti-spam filtering — URL filtering with configurable permit/block lists and regular-expression URL matching as well as a Web content filtering subscription service to enforce network security and usage policy by prohibiting downloads from non-work related Web sites and offensive or illegal Web content. IP address filtering of known senders of spam, phishing attacks, and viruses.
- Bandwidth management — enforce network usage policy by rate-limiting applications such as peer-to-peer file sharing and instant messaging applications.
- Prioritization of traffic inside and outside VPN tunnels with flexible, policy-based controls.
- IP multicast routing (PIM-DIM) over IPSec, supporting next-generation IP conferencing applications — prioritizes real-time traffic and provides secure connectivity for IP multicast traffic.
- Device management — option to configure, monitor, and manage the device using either the Web-based LSM client application or the command line interface (CLI).
- Centralized Management — option to configure, monitor, and manage individual or multiple X family devices using SMS.
- The TippingPoint Intrusion Prevention System — IPS identifies and stops malicious traffic on the edge of the network using filters that detect and block malicious traffic. Customize default filters to meet the specific needs of your enterprise.
- Digital Vaccine real-time protection — the Threat Management Center monitors global network security threats and continually develops new attack filters which are automatically distributed to preemptively protect against the exploit of new and zero-day vulnerabilities.

The following sections describe the X family environment and system components in more detail.

X Family Environment

An X family device can be installed at the perimeter of your network, in your remote offices, on your intranet, or in all three locations. The following diagram shows an example of a corporate network with X family devices deployed in a variety of locations:



When the X family device is installed and configured, it protects your network zones (LAN, WAN, and VPN, for example) using firewall rules and IPS filters. The device scans and reacts to network traffic according to the actions configured in the firewall rule or IPS filter. Each security zone and device can use a different set of firewall rules and IPS filters. Actions configured on the firewall rules and IPS filters provide the instructions for the device and can include blocking, rate limiting, or permitting the traffic and sending a notification about the action to a device or email address. Options are also available to block traffic and quarantine the source IP address for the traffic.

For users who will deploy multiple X family devices across the enterprise, 3Com provides the TippingPoint Security Management System (SMS). SMS lets you coordinate the management of multiple devices for administration, configuration, and monitoring. Most importantly, SMS includes enterprise-wide reporting and trend analysis.

Local Clients

You can access the X family device for monitoring, management, and configuration from any of the following client applications:

- **Local Security Manager (LSM)** — Web-based GUI for managing one IPS device. The LSM provides HTTP and HTTPS (secure management) access. This access requires Microsoft Internet Explorer 6.0 or later or Firefox 1.5 or later. Using the LSM, you have a graphical display for reviewing, searching,

and modifying settings. LSM also provides graphical reports for monitoring device traffic, triggered filters, and packet statistics.

- **Command Line Interface (CLI)** — Terminal interface for reviewing and modifying settings on the device. The CLI is accessible through SSH (secure access).
- **Secure Management System (SMS)** — SMS lets you remotely manage multiple X family devices. You can configure security zones, profiles, and policy (firewall rules and IPS filters) from the SMS and distribute the configuration to multiple devices. The SMS also lets you view, manage and edit device configuration, and review logs and reports for all devices under SMS management.
- **Third-party network management system (NMS)** — You can configure the X family device to accept management by a third-party NMS such as HP OpenView.



Note The device allows for 10 web client connections, 10 SSH connections (for the CLI), and one console connection at once.

System Requirements

The LSM is software accessed using a web browser. The browser's hardware and software requirements are not as technical as systems loading the software locally. To access the LSM, you need one of the following:

- Microsoft Internet Explorer (MSIE) 6.0 or later with 128-bit encryption and support for JavaScript and cookies
- Firefox 1.5 or later

SMS Configuration

If you will maintain your device using the Security Management System (SMS) or you will no longer use the SMS, you need to configure a setting on the device. This setting identifies whether the device is controlled by the SMS.

For more information, see [“Security Management System \(SMS\)” on page 258](#).

2 LSM Navigation

LSM Navigation describes the LSM interface, how to log in, and the general sections of the application.

Overview

The Local Security Manager (LSM) includes a graphical user interface (GUI) that makes configuring and monitoring your X family device easy by providing a user-friendly interface to accomplish administrative activities. You access the LSM through a Web browser. See [“Logging in to the LSM” on page 9](#) for more information.

This chapter details the login and navigation procedures of the LSM user interface. It includes the following information:

- [“Security Notes” on page 7](#)
- [“Logging In” on page 8](#)
- [“LSM Screen Layout” on page 10](#)
- [“System Summary” on page 14](#)

Security Notes

The LSM enables you to manage your X family device using a Web browser.



CAUTION Some browsers offer a feature that stores your user login and password for future use. 3Com recommends that you turn this feature off in your browser. It is counter to standard security practices to store login names and passwords, especially those for sensitive network equipment, on or near a workstation.

In addition, you can configure the LSM to communicate using either an HTTP or an HTTPS server. The default configuration is to use an HTTPS server. Whenever the device is connected to your network, you should run the HTTPS server, not the HTTP server. HTTP servers are not secure because your user name and password travel over your network unencrypted. You should only use the HTTP server when

you are sure that communications between the device and the workstation from which you access the LSM cannot be intercepted.



Note You can modify the server configuration using the **conf t server** command. For details, see the **Command Line Interface Reference**.

Logging In

When you log in to the LSM, you are prompted for your username and your password. This login gives you access to the areas of the LSM permitted by your user role. See [Chapter 9, “Authentication”](#) for information on user roles and accesses,



TIP Most Web browsers will not treat addresses beginning with HTTP and HTTPS interchangeably. If your browser cannot find your LSM, make sure that you are using `http://` or `https://` depending on which Web server you are running.



Note The device supports up to 10 Web client connections, 10 SSH connections (for the CLI), and 1 console connection at once.

Depending on your security settings, warnings may display when accessing the client. See [Appendix A, “Browser Certificates”](#) for information on accessing the device without warnings.

You are presented with the login screen under the following situations:

- When you first log in to the LSM
- If the LSM Web session times out

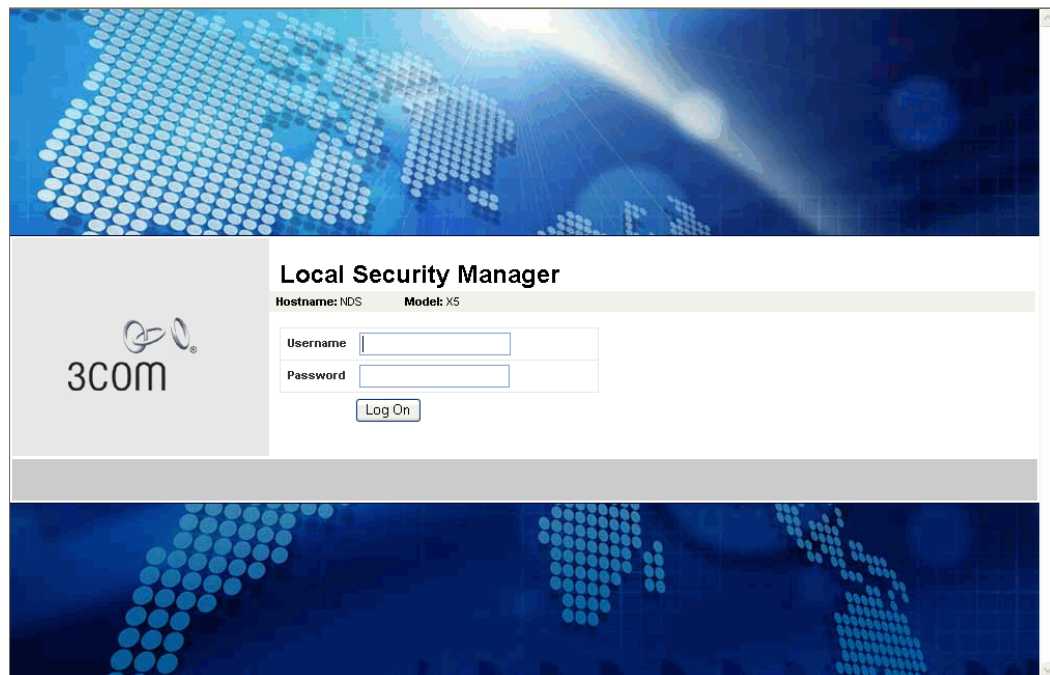
Logging in to the LSM

STEP 1 Enter the IP address or hostname of your IPS device in your browser **Address** bar. For example:

```
https://123.45.67.89
```

The LSM displays a login page. The page provides the name and model of your device.

Figure 2–1: LSM Logon Page



STEP 2 Enter your **Username**.

STEP 3 Enter your **Password**.

STEP 4 Click **Log On**.

The LSM validates your account information against the permitted users of the software. If the information is valid, the LSM software opens. If the account information is not valid, the Logon page is redisplayed.

LSM Screen Layout

The LSM provides features in two main areas of the browser window ([Figure 2-2](#)):

- **Main Menu Bar** — Located at the top of the browser window (item 1 in the figure). This area provides quick access to the System Summary page, online help, and current user and device status.
- **Navigation** — Located on the left side bar of the browser window (item 2 in the figure). The navigation pane provides access to the LSM menu functions. To view all the options available for a main menu item (for example, IPS), click the menu label. On an expanded menu, options with a + indicate that an additional sub-menu is available. When you select a menu item, the content and functionality area displays the content and available options. If you click the << icon in the upper right corner of the navigation pane, the menu collapses to provide more screen space for the current page displayed in the Content and Functionality area. Click >> to re-open the pane.
- **Content and Functionality** — Located on the right side of the browser window (item 3 in the figure). This area displays pages from which you can monitor device operation and performance, view current configuration settings, and modify the configuration. When you first log in, the [System Summary](#) page opens. Most page content is automatically refreshed; you can disable this auto-refresh function. Pages are also refreshed when you click a link in the LSM menu, or when you select buttons or links within a page. Links may display new content or open dialog boxes.

Figure 2-2: LSM Screen Layout

The screenshot shows the LSM Monitor Summary page. The browser window title is "Monitor Summary | LSM - Device (device34) - Mozilla Firefox". The address bar shows "https://10.100.34.100/monitor/ju1_monitor_view.html". The page content is organized into three main areas:

- Item 1 (Main Menu Bar):** Located at the top, it displays the current user "labuser" and "Auto Log Off in 60 minutes".
- Item 2 (Navigation):** A vertical sidebar on the left containing menu items: IPS, Firewall, VPN, Events (with sub-items: Logs, Managed Streams, Health, Monitor, Performance, Port Health, Reports), System, Network, and Authentication.
- Item 3 (Content and Functionality):** The main content area, which includes:
 - Device Health:** A table showing components and their states.

Component	State	Graph	Details
Memory	● (Normal)		46 percent used
Disk /000	● (Normal)		135 of 486 Mbytes used
 - Module Health:** A table showing modules and their configurations.



Module	Configuration	Module State	Qualifier-1	Qualifier-2	Port State
Management Processor	Simplex	● (Active)	No Info	No Info	● (Active)
<u>Threat Suppression Engine</u>	Simplex	● (Active)	No Info	No Info	N/A
<u>Ethernet Ports</u>	Simplex	● (Active)	No Info	No Info	● (Active with Faults)
 - Performance/Throughput:** A table showing performance metrics.

Component	State	Graph	Details
Performance	● (Normal)		0 percent of 100 Mbps used

Main Menu Bar

The dark blue bar at the top of the LSM screen provides quick access to basic logon information. The following table lists the available options in the Main Menu Bar:

Table 2–1: Main Menu Bar Options

Option	Description
<p data-bbox="394 468 591 495">System Summary</p> 	<p data-bbox="717 468 1398 569">To display the System Summary, click the System Summary icon. For information about this page, see “System Summary” on page 14.</p>
<p data-bbox="394 625 529 653">Online Help</p> 	<p data-bbox="717 625 1365 653">To access the online help, click the Launch Help Window icon.</p>
<p data-bbox="394 783 537 810">Current User</p>	<p data-bbox="717 783 1170 810">Displays the login name for the current user.</p>
<p data-bbox="394 840 643 867">Current date and time</p>	<p data-bbox="717 840 1409 968">Displays the current date and time on the device. The date and time settings on the device are determined by the time synchronization method and time zone configured for the device. For details, see “Time Options” on page 254.</p>
<p data-bbox="394 997 537 1024">Auto Log Off</p>	<p data-bbox="717 997 1166 1024">To log off of the LSM, click the Log Off link.</p> <p data-bbox="717 1066 1409 1304">For security purposes, LSM sessions have a timeout period. This timeout period determines how long the LSM can remain idle before automatically ending the session and logging off the user. The default timeout period is 60 minutes. LSM administrators with super-user access can change the default timeout period from the Preferences page (Authentication > Preferences). For details, see “Preferences Page” on page 298.</p>

Navigation

You can access the available features of the LSM by selecting an option from the navigation area. The LSM displays the page you select in the content and functionality area of the browser. Each option list displays a tier of links and features for maintaining and monitoring the device.

The following table lists the available options in the navigation area:

Table 2–2: Navigation Options

Option	Description
IPS	<ul style="list-style-type: none"> • Create and manage security profiles used to monitor traffic between security zones. This includes reviewing category settings, creating filter overrides, and specifying limits and exceptions for user-specified IP address. • Create and manage traffic threshold filters, action sets, and ports for IPS services. • Manage and configure settings for IPS filters, the Threat Suppression Engine (TSE), and global Adaptive Filter. <p>See “Chapter 3, “IPS Filtering” for more information.</p>
Firewall	<ul style="list-style-type: none"> • View and configure settings for the firewall. • View and configure web content filtering for the Web Content Filtering Service and create a custom filter list to permit or block traffic based on user-specified URLs. • View and configure anti-spam functions. <p>See Chapter 4, “Firewall” for more information.</p>
VPN	<p>View, configure and manage settings for site-to-site and/or client-to-site VPN connections. See Chapter 7, “VPN” for more information.</p>
Events	<ul style="list-style-type: none"> • View, download, print, and reset Alert, Audit, Block, and System logs. • View graphs reporting on traffic flow, traffic-related events, and statistics on firewall hit counts and triggered filters (attack, rate limit, traffic threshold, quarantine and adaptive filter). • Monitor, search, and maintain traffic streams for adaptive filtering, blocked streams, and rate-limited streams. Manually quarantine an IP address or release a quarantined IP address. • View reports on traffic flow, traffic-related events, and statistics on firewall hit counts and triggered filters (attack, rate limit, traffic threshold, quarantine and adaptive filter). • View the status of hardware components, performance (throughput), and system health. <p>See Chapter 5, “Events: Logs, Traffic Streams, and Reports” for more information.</p>

Table 2–2: Navigation Options (Continued)

Option	Description
System	<ul style="list-style-type: none"> • Configure system controls such as time options, SMS/NMS interaction, and High Availability. • Download and install software and Digital Vaccine (filter) updates. See Chapter 8, “System” for more information.
Network	<ul style="list-style-type: none"> • Configure network ports, security zones, IP interfaces, IP address groups, the DNS server, the default gateway, dynamic DNS, WAN failover and load balancing, routing, and DHCP server information. • Access network tools for DNS lookup, find network path, traffic capture, ping, and trace route functionality. See Chapter 6, “Network” for more information.
Authentication	Create, modify, and manage user accounts. Configure authentication. See Chapter 9, “Authentication” for more information.

Content and Functionality

The LSM displays all data in the central area of the browser window. As you browse and select linked options from the navigation area, pages display allowing you to review information, configure options, or search data. Links selected on these pages may display additional pages or dialog boxes depending on the feature selected.

Title Bar

On each page, you can see the position of the page in the menu hierarchy provided in the title bar. For example, on the Alert Log page, the menu hierarchy indicates that the page is located off the **EVENTS > LOGS** sub-menu. On tabbed menu pages, you can navigate up the hierarchy from the current location by clicking on the link in the hierarchy listing.

Auto Refresh

Some pages (such as System Summary) automatically refresh themselves periodically.

- To disable the auto refresh function, deselect the **Auto Refresh** check box.
- To manually refresh: click the **Refresh** link.
- To reconfigure the **Page Refresh Time**, see [“Preferences Page” on page 298](#).

Tabbed Menu Options

Some sub-menu options previously available in the left-hand navigation menu are now accessible as a tab on the main page for the menu. For example, from the Tools page, the following tabs are available: **DNS Lookup**, **Find Network Path**, **Traffic Capture**, **Ping**, and **Traceroute**.

System Summary

The System Summary page automatically displays when you first log onto the LSM. To redisplay the System Summary page at any time, click the **System Summary** icon, in the [Main Menu Bar](#).

The System Summary page includes the following:

- [System Status](#) — Displays summary information about the device health, packet statistics, and network DHCP. Also provides access to the **Reboot Device** function.
- [Log Summary](#) — Displays summary information about all the Event Logs.
- [Product Specifications](#) — Displays product, version, time, and encryption information.

System Status

Health

The **Health** section of the Statistics frame displays a color indicator of the hardware health of the device. For detailed information about each of the health indicators, click on the corresponding link above the color indicator. The **Health** section includes indicators for the following components:

- System Log
- Traffic Threshold
- Performance
- Disk Space
- Memory
- Web Filtering
- HA Status

The colors indicate the current state of each component:

- Green if there are no problems
- Yellow if there is a major warning
- Red if there is a critical warning
- Grey if the service is disabled

You can set the thresholds for warnings. This defines when the indicator color will change based on the usage of those components. For more information, see [“Thresholds to Monitor Memory and Disk Usage” on page 265](#), and select **System > Thresholds** in the Navigation area.

If the System Log is other than green, you can click on the indicator to view the error that caused the condition.



Note When you view the logged error, the indicator resets and changes to green under **System Summary**.

Packet Stats

The Packet Stats section provides basic traffic statistics including the following:

- **Received** — Total number of packets received and scanned by the Threat Suppression Engine
- **Blocked** — Total number of packets that have been blocked by the Threat Suppression Engine
- **Rate Limited** — The number of packets that matched a filter configured to a permit action set
- **Dropped** — Total number of packets that have been dropped as malformed or misformatted

To reset the counters, click the **Reset** link.

Packet counters provide a snapshot of the traffic going through your network. The packet totals give a partial account of blocked activity according to the filters. All other filter results affect the packet totals.



Note The counters are not synchronized with each other; packets may be counted more than once in some situations.

The counters display the amount of packets tracked. If the number is less than 1M, the Packet Statistics section displays the full amount. If the amount is greater than 999,999 K, the information is abbreviated with a unit factor. For example, 734,123K would display fully whereas 4,004,876,543 displays as 4.00B. When the number reaches the million and billion mark, the number displays as a decimal amount with a letter (such as G for gigabytes). The unit factors include, M for mega, G for giga, and T for tera. To view the full amount, hover your mouse over the displayed amount. A Tool Tip pops up, displaying the full packet amount.

Network DHCP

The Network DHCP section displays the following information:

- Current Leases
- Available Leases

Reboot Device

To reboot the device, click the **Reboot Device** link.

Log Summary

The **Log Summary** section displays the number of entries and events for each type of Event Log. In addition, it lets you perform functions on those logs.

- System Log.
- Audit Log. This log is only available to those with Super User access.
- Alert Log.
- Block Log.
- Firewall Block Log.
- Firewall Session Log.
- VPN Log.

For more detailed information about these logs, select **Events > Logs**.

Product Specifications

The Product Specification section displays the following information:

- **Model Number** — Model number of the device.
- **Product Code** — The device product code.
- **Serial Number** — Serial number of the device.
- **TOS Version** — Version number of the TOS software.
- **Digital Vaccine** — Version number of the Digital Vaccine.
- **Boot Time** — Time when the device was last started.
- **Up Time** — How long the device has been operating continuously.
- **Encryption** — Current encryption method being used. By default all new X family devices are supplied with 56-bit DES encryption only. To enable strong encryption functionality (3DES, 128-AES, 192-AES, 256-AES), install the correct Strong Encryption Service Pack for your device. You can download encryption service packs from the TMC Web site.

3 IPS Filtering

The Intrusion Protection System filters out unwanted or malicious traffic. This section describes how to set up security profiles, action sets, and Digital Vaccine and Traffic Threshold filters.

Overview

The X family of Unified Security Platforms provides the TippingPoint Intrusion Prevention System (IPS) with Digital Vaccine (DV) filters that can be used to police your network to screen out malicious or unwanted traffic such as:

- Vulnerability attacks and exploits
- Worms
- Spyware
- Peer-to-peer applications

In addition to DV filters, the IPS function also provides **Traffic Threshold** filters you can use to profile and shape network bandwidth.

All IPS filtering occurs inline on traffic that has been permitted through the X family firewall. Filtering is performed at the packet level by the **Threat Suppression Engine**, custom software designed to detect and block a broad range of attacks at high speed. When a packet matches an IPS filter, the device handles the packets based on the **action** configured on the filter. For example, if the action set is *block*, then the packet is dropped. The device provides default actions to block or permit traffic with options to quarantine or rate-limit traffic and to notify users or systems when an action executes. Logging options are also available so you can review the types of traffic being filtered by the device. You can customize the default actions, or create your own based on your network requirements.

A **security profile** defines the traffic to be monitored and the DV filters to be applied. Traffic monitoring is based on security zone pairs. For example, to create a security profile to monitor traffic coming from the WAN zone to the LAN zone, you select the security zone pair WAN ==> LAN, then configure the DV filters to apply to that pair. The security zone pair specifies both the zone and the traffic direction, which lets you define separate security profiles for traffic into and out of a zone.

The default security profile is set to the ANY ==> ANY security zone pair with all IPS filters configured with the default DV settings. With the default profile in place, all incoming and outgoing traffic in any security zone configured on the device is monitored according to the recommended IPS filter configuration. You can edit the default security profile to customize the security zones to which it applies and create custom filter settings, or you can create your own security profiles as required.



Note Before creating security profiles, verify that the network and system configuration on the device is set up correctly for your environment. In particular, you need to configure all required security zones before you can create the security profiles to protect them. See [Chapter 8, “System”](#) and [Chapter 6, “Network”](#) for details.

You can monitor and configure IPS from the IPS menu pages available in the LSM. For additional information, see the following topics:

- [“Using the IPS” on page 18](#)
- [“Security Profiles” on page 19](#)
- [“IPS Digital Vaccine Filters” on page 24](#)
- [“Traffic Threshold Filters” on page 37](#)
- [“Action Sets” on page 42](#)
- [“Notification Contacts” on page 49](#)
- [“IPS Services” on page 52](#)
- [“Preferences” on page 54](#)

Using the IPS

You can monitor and configure IPS settings from the IPS menu pages available in the LSM. The following menu options are available:

- **Security Profiles** — View and manage the security profiles available on the device; view the security profile coverage by security zone.
- **Traffic Threshold** — View, manage, and create Traffic Threshold filters to monitor network traffic levels. These filters can be triggered when traffic is either above or below normal levels.
- **Action Sets** — View, manage, and create actions that define the operations a filter performs when a traffic match occurs.
- **IPS Services** — Add and manage non-standard ports supported by the device. Use this feature to configure additional ports associated with specific applications, services, and protocols to expand scanning of traffic. When filters scan traffic against the standard ports for listed services, the engine then accesses and scans traffic against the list of additional ports.
- **Preferences** — Reset IPS filters to the factory default values; configure timeout, logging, and congestion threshold settings to manage performance of the Threat Suppression Engine; configure the Adaptive Filter feature used to protect performance from the effects of overactive filters.

For details on each menu option, see the following topics:

- [“Security Profiles” on page 19](#)
- [“Traffic Threshold Filters” on page 37](#)
- [“Action Sets” on page 42](#)
- [“IPS Services” on page 52](#)
- [“Preferences” on page 54](#)

Security Profiles

On the X family device, **security profiles** are used to apply DV filter policies. A security profile defines the traffic to be monitored based on security zones (for example, ANY ==> ANY, LAN ==> WAN, or WAN ==> LAN) and the DV filters to be applied.

A security profile consists of the following components:

- **Identification** — Profile name and description.
- **Security Zones** — Specifies the incoming and outgoing security zones to which the security profile applies.
- **IPS Filter Category Settings** — Determines the state and action that applies to all filters within a given Filter Category group.
- **Filter overrides** — Configure filter-level settings that override the category settings (optional.)
- **Global Limits and Exceptions** — Configure settings to apply filters differently based on IP address. You can limit filters to apply only to traffic between a source and destination IP address or address range, or apply filters to all traffic except the traffic between specified source and destination IP addresses or address ranges.

When a security profile is initially created, the recommended settings for all filter categories are set.

For additional information on security profiles, see the following topics:

- [“Managing Security Profiles” on page 20](#)
- [“Configuring DV Filters” on page 24](#)
- [“Configuring Filter Limits and Exceptions Based on IP Address” on page 33](#)

Managing Security Profiles

Use the Security Profiles page (**IPS > Security Profiles**) to create and manage the security profiles used to apply IPS filtering to security zone traffic.

Figure 3–1: Security Profiles Page




The following table provides a summary of tasks available to configure and manage security profiles from the Security Profiles menu pages in the LSM:

Table 3–1: Security Profile Tasks

Task	Procedure
View all security profiles	From the navigation pane, select IPS > Security Profiles . Then, click a security profile name to open the profile. You can view a list of the security profiles as well as a listing that shows which security profiles provide DV filtering for the different Security Zones configured on the device. Note You cannot delete the default security profile.
Create a security profile	From the navigation pane, select IPS > Security Profiles . On the Security Profile page, click Create .
Edit a security profile	From the navigation pane, select IPS > Security Profiles . On the Security Profile page, click Edit .
Delete a security profile	On the Security Profiles page, click X . When you delete the profile, all the global and filter level settings are deleted.

Table 3–1: Security Profile Tasks (Continued)

Task	Procedure
Change category settings for a group of filters	On the Edit Security Profile page in the Profile Details (Advanced) section, change the State and Action setting for the category you want to modify. Then, Save the updated profile.
Override global filter settings (create filter level settings)	On the Edit Security Profile page in the Profile Details (Advanced) Filters section, click Search Filters . On the Search Filters page, locate the filter to override. Click the + icon to add the filter to the security profile. Then, edit the filter to customize the settings.
Restore filter to global category settings (delete filter override)	On the Edit Security Profile page in the Profile Details (Advanced) Filters section, locate the filter override to delete. Then, click  .
Edit Port Scan/Host Sweep Filters	Port Scan/Host Sweep filters are a special type of filter used to protect the network against Port Scan/Host Sweep attacks. These filters can only be applied to security zones that include physical ports. For additional information on these filters, see “Port Scan/Host Sweep Filters” on page 35 .

For additional information, see the following topics:

- [“Security Profile Details” on page 21](#)
- [“Creating a security profile” on page 22](#)
- [“Editing a security profile” on page 23](#)
- [“Viewing DV Filters” on page 24](#)
- [“Editing DV Filter Category Settings” on page 29](#)
- [“Port Scan/Host Sweep Filters” on page 35](#)


Security Profile Details

The following table describes the information available on the Security Profiles page:

Table 3–2: Security Profile Details

Parameter	Description
Current Profiles: This section lists all the security profiles currently configured on the device.	
Profile Name	The name assigned to the security profile. The Default security profile is preconfigured on the device. You can customize this profile to add security zone pairs or modify global and individual filter settings, but you cannot delete or rename this profile.
Description	Displays the description entered for the security profile if any exists.

Table 3–2: Security Profile Details (Continued)

Parameter	Description
Function(s) 	The functions available to manage security profiles: <ul style="list-style-type: none"> • Edit the security profile to configure security zones, category settings, filter overrides, or global limits and exceptions • Delete the security profile
<p>Security Zones: This section lists all the security zone pairs that are currently protected by a security profile.</p> <p>Note If a Traffic Threshold has been configured with a security zone pair that is not protected by a security profile, the pair will be listed in the table in red along with the following message:</p> <p>No security profile is assigned to the security zones. Traffic will NOT be inspected by the IPS.</p> <p>To correct the error, add the security zone pair to an existing security profile, or create a new Profile to protect it.</p>	
Incoming	The security zone that is the traffic source.
Outgoing	The security zone that is the traffic destination.
Security Profile	The name of the security zone configured on the device.

For additional information, see the following topics:

- [“Creating a security profile” on page 22](#)
- [“Editing a security profile” on page 23](#)
- [“Viewing DV Filters” on page 24](#)
- [“Editing DV Filter Category Settings” on page 29](#)


Creating a security profile

STEP 1 From the navigation pane, select **IPS > Security Profiles**.

The Security Profiles page opens.

STEP 2 Click **Create Security Profile**.

The Create Security Profiles page opens.

STEP 3 Click the  (**edit**) icon to edit the desired security profile.

STEP 4 In the **Security Zones** section, specify the security zone pairs for the security profile:

STEP A Select the **Incoming** and **Outgoing** security zone.

STEP B Click **Add to table**.

Repeat this process until you have added all the required security zone pairs.



Note For additional information about setting up the security zones, see [“Security Zone Configuration” on page 135](#).

STEP 5 Review or configure advanced configuration options. If the advanced options are not visible, click **Show Advanced Options**. In the **Profile Details (Advanced)** section in the **Category Settings** table, change the global State or Action for a filter Category Group if required. For more detailed instructions, see [“Editing category settings for a filter group” on page 29](#).


STEP 6 Click **Create**.

After you create the security profile, you can edit the security profile and perform additional advanced configuration to create filter overrides and specify global limits and exceptions.

Editing a security profile

STEP 1 From the navigation pane, select **IPS > Security Profiles**.

The Security Profiles page opens.


STEP 2 Click the  (**edit**) icon to edit the desired security profile.

STEP 3 In the **Security Zones** section, modify the security zone pair configuration, if necessary.

STEP A Select the **Incoming** and **Outgoing** Security Zone.

STEP B Click **Add to table**.

Repeat this process until you have added all the required security zone pairs.

STEP C Click  to delete a security zone.

STEP 4 Review or configure advanced configuration options. If the advanced options are not visible, click **Show Advanced Options**. Do any of the following as needed:

- In the **Profile Details (Advanced)** section in the **Category Settings** table, change the global State or Action for a filter Category Group if required. For more detailed instructions, see [“Editing category settings for a filter group” on page 29](#).
- To review filters or add a filter to the security profile for customization, locate the filter using the **Search Filters** button or **View all filters** link. For details, see [“Editing individual filter settings” on page 31](#).
- Configure global IP address limits or exceptions if required. For details, see [“Configuring global IP address limits/exceptions” on page 33](#).

STEP 5 Click **Save** to update the security profile.

For additional information, see the following topics:

- [“Viewing DV Filters” on page 24](#)
- [“Editing DV Filter Category Settings” on page 29](#)
- [“Port Scan/Host Sweep Filters” on page 35](#)

IPS Digital Vaccine Filters

TippingPoint IPS Digital Vaccine filters are used to monitor traffic passing between network security zones. Based on the security profiles configured on the device, the X family device applies the filters to traffic passing between network security zones. Each security profile has its own filter settings. Within a security profile, you can modify the filter (recommended) settings for a filter category and, if necessary, customize individual filters based on your network environment and security needs.

Configuring DV Filters

You configure filters separately for each security profile configured on the X family device. When a profile is initially created, all filters are set to the default category settings. You can change the category settings for filters or edit individual filters from the Edit Security Profile page.

Because of the large number of DV filters available on the device, the LSM provides a search interface to view and edit filters. For instructions on using this interface and on editing filters, see the following topics:

- [“Viewing DV Filters” on page 24](#)
- [“Editing DV Filter Category Settings” on page 29](#)
 - [“Editing category settings for a filter group” on page 29](#)
 - [“Editing individual filter settings” on page 31](#)
 - [“Configuring Filter Limits and Exceptions Based on IP Address” on page 33](#)
 - [“Editing a port scan/host sweep filter” on page 36](#)
- [“Resetting an Individual Filter” on page 34](#)

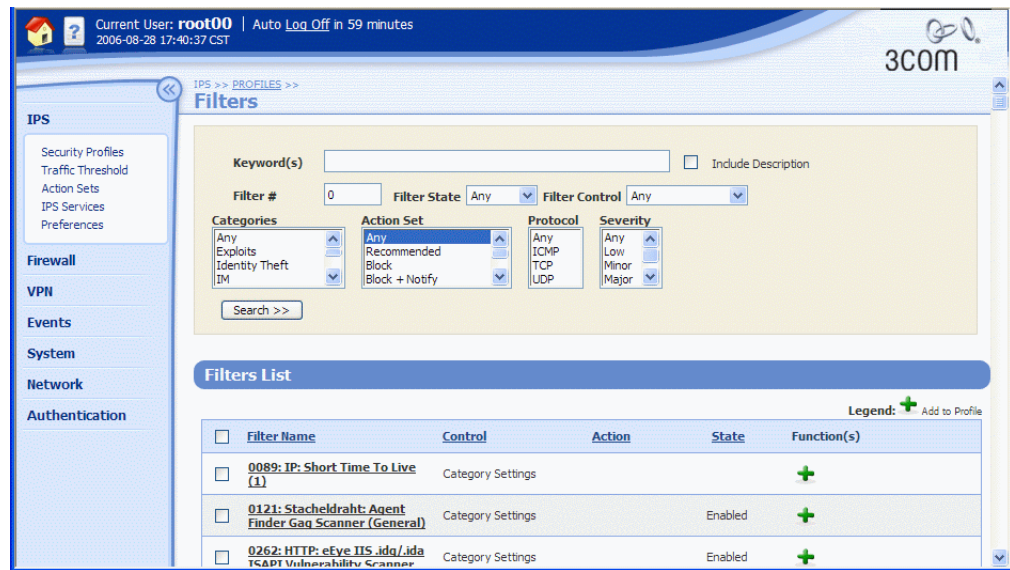
Viewing DV Filters

You can view and manage filters configured for a security profile using either the Filters and Filter Search pages. Both pages can be accessed from the Advanced Options Filters section of the Security Profile pages.

- To access the Filters page, use the **View all filters** link
- To access the Filter Search page, click **Search Filters**

The following figure shows the Filters page:

Figure 3–2: Filters Page with Search



You can complete the following tasks from these pages:

- Viewing current filters
- Sorting the filter list
- Locating a filter or group of filters
- Adding a filter to the filter override list for the current security profile
- Viewing the filter description page, which includes information about the filter, recommended settings, and the current filter state
- Adding or removing a filter from selected security profiles

For additional information, see the following topics:

- [“Filter Search” on page 25](#)
- [“Filters List \(All Filters\)” on page 26](#)
- [“Resetting an Individual Filter” on page 34](#)
- [“Port Scan/Host Sweep Filters” on page 35](#)

Filter Search

Filter search provides options to view all filters or only those matching user-specified search criteria. You can access the Filter Search page by clicking **Search Filters** when you are editing a security profile (**IPS > Security Profiles**, then edit a profile).

You can sort filter search results by filter name, control type, action, or state by clicking a column heading in the **Filters List** table. The search is a string search and is not case sensitive.

The following table describes the available search criteria that can be configured:

Table 3–3: Search Filter Criteria Parameters

Parameter	Description
Keywords	Type a word or phrase to search for in the filter names. The keyword Filter Search is a string search, not a Boolean search. You can search for a specific filter number, or for a specific substring in the filter name. If you enter more than one word, the search will look for the exact phrase entered, not a combination of words. For example, if you enter “ICMP reply” the search will not return a filter whose description is “ICMP: Echo Reply.”
Include Description	Check this option to search for the specified keyword(s) in the filter descriptions, as well as in the filter names.
Filter #	Search by filter number; type the filter number in this field.
Filter State	Search by current operating state; select from the following: Any, Disabled, or Enabled.
Filter Control	Search for filters configured with category settings or filters that have been customized (overridden).
Categories	Search by IPS filter category group. Selection list includes all groups in the Application Protection, Infrastructure Protection, and Performance Protection categories.
Action Set	Search by action set assigned to filter. The selection list includes all the default and custom action sets configured on the device.
Protocol	Search by transport protocol that the filter applies to: ANY, ICMP, TCP, and UDP.
Severity	Search by the Severity Level assigned to the filter.

For details on performing a filter search see the following topics:

- [“filters:Viewing filters with recommended \(default\) settings” on page 28](#)
- [“Viewing filters:filter overrides and custom settings” on page 28](#)

Filters List (All Filters)

The Filters List page provides a listing of all filters configured for the security profile. You can access the page by selecting the **View all filters** link when you are editing the security profile. Because of the large number of filters, it may take some time for the device to display the page.

Filter List Details

The following table describes the information and functions available on the Filters List page:

Table 3–4: Filter List Details

Parameter	Description
Search Interface	For details on the search criteria fields, see “Search Filter Criteria Parameters” on page 26 .
Check Box	<p>Use the check box for a filter entry to select it for editing. After checking the desired filters, use the Add Selected Filters button to add the filters to the security profile so you can edit them.</p> <p>If a filter entry has no check box, that filter has already been added to the security profile. You can manage these filters from the Security Profiles page Filters table.</p>
Filter Name	<p>The name of the filter. The name contains the filter number and additional information relating to the protocol the filter applies and other descriptive information about the purpose of the filter (for example, <i>0079: ICMP:Echo Reply</i>). These names are assigned by the DV team.</p> <p>To view filter information, click the name of the filter.</p>
Control	<p>Indicates whether the filter configuration is:</p> <ul style="list-style-type: none"> • Category Settings — uses the global category settings configured for the filter’s category. To view the category and category group for filter, click the filter name. • Filter — uses custom settings configured from the Security Profile page. You can manage customized filters from the Filters table on the Security Profile page.
Action Set	<p>Indicates the action set currently assigned to the filter. If the filter uses category settings and the action set is recommended, the Action field lists Disabled to indicate that the filter is under the control of the default configuration.</p> <p>If the filter has an override, the Action selected in the override is displayed.</p>
State	Indicates whether the filter is enabled (in use) or disabled.
Function(s)	<p>Available functions for the filter:</p> <ul style="list-style-type: none"> • Add to security profile so you can edit the filter settings. <p>If the filter has been overridden, the Add function is not available. You can edit the filter settings from the Filter Override list on the Security Profile page.</p>


From this page you can complete the following tasks:

- Viewing filters with recommended (default) settings
- Viewing filter overrides and custom settings

filters:Viewing filters with recommended (default) settings

STEP 1 From the navigation pane, select **IPS > Security Profiles**.

The Security Profiles page opens.

STEP 2 Click the  (**edit**) icon to edit the desired security profile.

STEP 3 On the Edit Security Profile page, if the **Profile Details (Advanced)** table is not visible, click **Show Advanced Options**.

STEP 4 In the **Profile Details (Advanced)** table, scroll down to the Filters section. You can click either **View all filters** or **Search Filters**.

- **View all filters** displays the Filters page. Because of the large number of filters, this action may take some time to execute.

If you select this option, the Search Filters page displays a list of the available IPS filters. You can sort the filters by filter name, control type, action, or state by clicking the appropriate column heading in the Filters List table. To specify new search criteria, use the search interface available at the top of the page.

- **Search Filters** displays the Search Filters page so you can specify filter search criteria and perform the search.

If you select this option, select the desired Search criteria. Then, click **Search**. Note that the Search facility performs string searches. If you select **Search Filters**, the Search Filters page displays with only the search interface displayed. To locate filters, specify one or more search parameters, then click **Search**. Note that the search is a string search.

Viewing filters:filter overrides and custom settings

STEP 1 From the navigation pane, select **IPS > Security Profiles**.

The Security Profiles page opens.

STEP 2 Click the **Profile Name** you want to edit.

STEP 3 On the Edit Security Profile page, if the **Profile Details (Advanced)** table is not visible, click **Show Advanced Options**.

STEP 4 In the **Profile Details (Advanced)** table, scroll down to the **Filters** section.

In the Filters section, the table lists all filters that have been added to the Profile.

STEP 5 To view and/or edit a filter, click the **Filter Name**.

If you want to remove the filter override and return the filter to its default, recommended settings, click the **Delete** icon.

Editing DV Filter Category Settings

By default, a security profile uses the category settings for all filters available in the Digital Vaccine package. In some cases you may not need a particular filter or category of filters. For example, you may want to disable filters that protect a particular type of Web server against attack if that server is not installed on your network. From the LSM, you can modify the filter configuration for a security profile by category or by changing individual filter settings. You can make the following types of changes:

- Edit a Filter Category Group to enable or disable all filters in the group or change the assigned action for all filters in the group.
- Edit an individual filter or group of filters to modify the following settings: State, Action, Adaptive Filter Configuration State, Exceptions.

When you edit a filter, the changes only affect the security profile in which you make the edits. This lets you have different filter configurations for different security zones.

For details on editing filters, see the following topics:

- [“Editing category settings for a filter group” on page 29](#)
- [“Editing individual filter settings” on page 31](#)
- [“Editing a port scan/host sweep filter” on page 36](#)



Note If the category setting is enabled and you disable the filter, the filter may still display as enabled.

Editing category settings for a filter group



Note When you change the category settings for a group of filters, the settings will not affect any filters that have been customized (overridden). Filters that have been customized display on the Edit Security Profiles page in the Filters section. On the Filters List page, these filters are listed with Control = Filter.

STEP 1 From the navigation pane, select **IPS > Security Profiles**.

The Security Profiles page opens.

STEP 2 In the **Current Profiles** table, click the **Edit** icon for the security profile you want to change.

The Edit Security Profile page opens.

STEP 3 In the **Advanced Options** section, locate the Filter Category group in the **Category Settings** table.

The following figure shows the Category Settings table:

Figure 3–3: Edit Security Profile Page - Advanced Options - Category Settings



Click **Show Advanced Options** if the **Advanced Options** table is not displayed.

STEP 4 Modify the settings as required:

- In the **State** field for the Category group, clear the check box to disable all filters in the group, or check it to enable all filters in the group.
- In the **Action** field, select the action set to be used for all filters in the group.

The Recommended Action Set is the system default for all category groups. If this action is selected, each filter in the group is configured with the recommended settings. Filters within the group may have different settings for *State* and *Action*.

The following action set selections are available for each filter category:

- For all **Application Protection** filters, the selection list includes all available actions sets.
- For **Infrastructure Protection** filters, the selection list includes all available actions sets.
- For **Performance Protection** filters, the selection list includes all available block action sets.

STEP 5 After making the desired changes, click **Save** (at the bottom of the Security Profile page).

Editing individual filters to override category settings

For the best system performance, 3Com recommends that you use global category settings and the Recommended action set for all DV filters. However, in some cases, you may need to override the category settings and recommended action for individual filters due to specific network requirements, or in cases where the recommended settings for a filter interact poorly with your network.

Filter override settings specify custom settings to be applied to the filter in the security profile. Once a filter has been customized, it is not affected by the global category settings that apply to all other filters in the category group. For details, see [“Editing individual filter settings” on page 31](#).

Editing individual filter settings



Note These instructions are for editing all Application Protection, Infrastructure Protection, and Performance Protection filters with the exception of the Port Scan/Host Sweep filters available in the Application Protection: Reconnaissance category. For details on Port Scan/Host Sweep filters, see [“Port Scan/Host Sweep Filters” on page 35](#).

STEP 1 From the navigation pane, select **IPS > Security Profiles**.

The Security Profiles page opens.

STEP 2 In the **Current Profiles** table, click the **Edit** icon for the security profile you want to change.

The Edit Security Profile page opens.

STEP 3 In the **Advanced Options** section, locate the **Filters** table.

STEP 4 In the **Filters** table, find the filters that you want to edit. Do one of the following:

- Click **Search Filters**. Then, on the Search Filters page, specify the search criteria. Click **Search** to display the filter search results.
- Click **View all filters** to display the Filters page with all IPS filters available.
Because of the large number of IPS filters, this operation may take a few moments to complete.

STEP 5 To view filter details including filter name description and default settings, click the filter name to display the details on the View Filter page.

On the View Filter page, you can also add or remove the filter from security profiles using the check boxes in the Security Profiles table. After making changes, click **Save**.

STEP 6 In the **Filters List** table, select the filter or filters to edit:

- To select a single filter, click **+** to add the filter to the security profile.
- To select multiple filters, select the check box for each filter. Then, click **Add Selected Filters** at the bottom of the Filters page.

The Security Profiles page displays with the selected filters in the **Advanced Options - Filters** table as shown in the following figure:

Filter Name	Control	Action	State	Function(s)
0303: IPeye Scanner: TCP NULL Probe	Category Settings			
7002: TCP: Host Sweep	Filter	Block		
0087: ICMP: Modem Hangup (+++ATH) Echo Request	Filter	Block / Notify		

STEP 7 To edit the filter settings, click the filter name or the **Edit** icon.



- STEP 8** On the Edit Filter page in the **Action/State** section, select **Use Category Settings** or **Override**. If you select **Override** to use a different action set for the filter, do the following:
- STEP A** Select **Override** in the **Parameters** section.
 - STEP B** Check **Enabled** to enable the filter, or clear the check box if you want to disable the filter.
 - STEP C** Choose an **Action** from the drop-down list.

If the action for the filter is *Recommended* and you do not change it, the filter may remain disabled even when you select the **Enabled** check box. This happens because the recommended setting for the filter state is *disabled*. To enable a filter configured in this manner, you must change the action from *Recommended* to another option.
- STEP 9** Optionally, set adaptive filter settings for flow control. In the **Adaptive Filter Configuration State** section, select one of the following:
- **Use adaptive configuration settings** — Applies the global adaptive filter settings
 - **Do not apply adaptive configuration settings to this filter** — Removes any global adaptive filter settings for this filter
- STEP 10** Optionally, define IP address exceptions for the filter. For details, see [“Configuring Filter Limits and Exceptions Based on IP Address” on page 33](#).
- STEP 11** Click **Save**.

Configuring Filter Limits and Exceptions Based on IP Address

Limits and exceptions let you configure the device so that the filters in a security profile can be applied differently based on IP address. For example, you can specify a limit setting so that filters only apply to specified source and destination IP addresses or address ranges. You can configure the following limits and exceptions:

- **Filter Exceptions** (specific)— Allow traffic that would normally trigger a filter to pass between specific addresses or address ranges without triggering the filter. Configured from the Filter Edit page, these exceptions apply only to the filter on which they are configured.
- **Limit Filter to IP Addresses** (global) — Only apply filters to traffic between specified source and destination IP address pairs. You can configure IP address limits that apply to all the following filter types: Application Protection, Traffic Normalization, and Network Equipment Protection filters. You can configure separate limits that apply only to Performance Protection filters.
- **Exceptions** (global) — Exclude traffic between specified source and destination IP address pairs. You can configure exceptions for the following filter types: Application Protection, Traffic Normalization, Network Equipment Protection, and Performance Protection filters. These exceptions are global for all specified filters.

If a filter has both global and filter-level exception settings, the Threat Suppression Engine uses the filter-level settings to determine how to apply the filter.

The following sections describe the procedures to configure and delete global limits and exceptions from the Security Profile page.

- [“Configuring global IP address limits/exceptions” on page 33](#)
- [“Deleting a global IP address limit/exception setting” on page 34](#)
- Configure filter-level exceptions: [“Editing individual filter settings” on page 31](#)

Configuring global IP address limits/exceptions

STEP 1 From the navigation pane, select **IPS > Security Profiles**.

The Security Profiles page opens.

STEP 2 Click the name of the profile you want to edit.

The Edit Security Profile page opens.

STEP 3 In the **Advanced Options** section, scroll down to the **Limits/Exceptions** table. (Click **Show Advanced Options** if the **Advanced Options** table is not displayed.)

STEP 4 In the **Limits/Exceptions** section, specify the Application Protection Filter Exclusives (limits) for Application Protection, Traffic Normalization, and Network Protection filters:

STEP A Enter the **Source Address**.

Source and Destination IP Addresses can be entered in CIDR format, “any,” or “*.”


STEP B Enter the **Destination Address**.

STEP C Click **add to table below**.

STEP D Repeat this process for each IP address exception required.

- STEP 5** In the **Application Protection Filter Setting Exceptions** section, specify the IP address exceptions for Application Protection, Traffic Normalization, Network Equipment Protection, and Performance Protection filters.
- STEP 6** In the **Performance Protection Filter Settings** section, specify IP address limits for Performance Protection filters.
- STEP 7** Click **Apply**.

Deleting a global IP address limit/exception setting


- STEP 1** From the navigation pane, select **IPS > Security Profiles**.
The Security Profiles page opens.
- STEP 2** Click the name of the profile you want to edit.
The Edit Security Profile page opens.
- STEP 3** In the **Advanced Options** section, scroll down to the **Limits/Exceptions** table. (Click **Show Advanced Options** if the **Advanced Options** table is not displayed.)
- STEP 4** Review the global limit and exception address entries. Click  to delete an entry.
To delete a filter-level exception, edit the filter. For details, see [“Editing individual filter settings” on page 31](#)
- STEP 5** When you finish, click **Apply**.

Resetting an Individual Filter

If you have created a filter override in a security profile, you can restore the filter to its default settings by deleting the filter from the Security Profile Filters table.

You can also reset all filters to their factory default settings from the IPS Preferences page. If you do this, all the filters will be set to their recommended state and all action sets, rate limits, and thresholds (other than defaults) will be deleted. You will also lose the security profiles you have created along with any custom settings configured on the default security profile. For details, see [“Reset Filters” on page 55](#).

Deleting a filter override

- STEP 1** From the navigation pane, click **Security Profiles**.
The Security Profiles page opens.
- STEP 2** In the **Current Profiles** table, click Profile Name for the profile you want to change. The Edit Security Profile page opens.
- STEP 3** In the **Advanced Options** section, locate the **Filters** table.
- STEP 4** In the **Filters** table, find the entry for the filter override you want to remove and click . The filter is restored to the recommended settings for the category it belongs to.

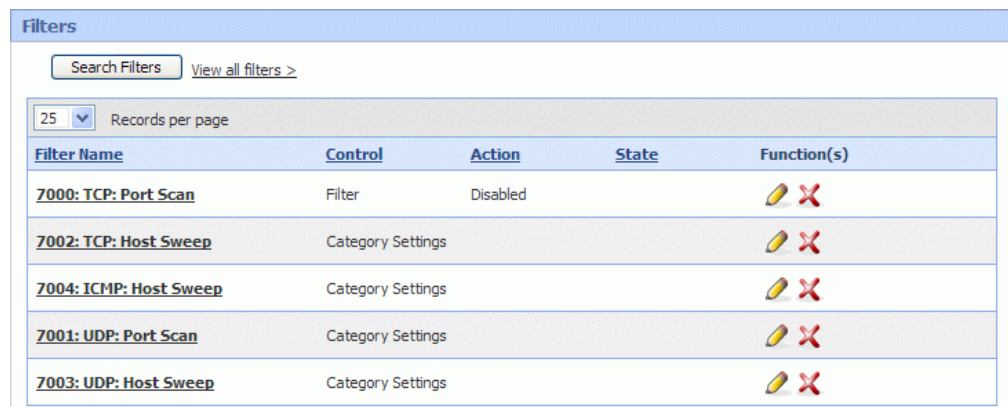
Port Scan/Host Sweep Filters

A port scan attack scans a host looking for any open ports that can be used to infiltrate the network. A host sweep scans multiple hosts on the network looking for a specific listening port that can be used to infiltrate the network.

The Port Scan/Host Sweep Filters (Filter numbers 7000–7004) available in the *Application Protection Category - Reconnaissance* group are designed to protect the network against these types of attacks. These filters monitor the rate of connections generated by hosts on the network. The filter triggers when the connection rate during a specified interval goes above a given threshold.

The following figure shows the Port Scan/Host Sweep Filters added to the security profile for editing:

Figure 3–4: Security Profile: Port Scan/Host Sweep Filter Overrides



The screenshot shows a web interface titled "Filters". It includes a search bar, a "View all filters >" link, and a "Records per page" dropdown set to 25. Below is a table with the following data:

Filter Name	Control	Action	State	Function(s)
7000: TCP: Port Scan	Filter	Disabled		
7002: TCP: Host Sweep	Category Settings			
7004: ICMP: Host Sweep	Category Settings			
7001: UDP: Port Scan	Category Settings			
7003: UDP: Host Sweep	Category Settings			

The Port Scan/Host Sweep Attack filters can only be used to monitor traffic on security zone that include physical ports. That is, you cannot run Port Scan/Host Sweep filters on VLANs or zones configured with a virtual server.

In the category settings, all Port Scan/Hosts Sweep filters are disabled. To apply these filters to the security profile, enable the filters, tune the *threshold* and *timeout* interval settings, and assign an action set based on your network requirements. Because the *Recommended* setting for Port Scan Host/Sweep filters is disabled, you have to assign a specific action to the filter to enable it.

Filter Tuning

You can tune the sensitivity of Port Scan/Host Sweep filters by adjusting their *Timeout* and *Threshold* parameters. The timeout value is used in combination with the threshold value to determine whether or not an alert is sent.

For example, if the time interval is 300 seconds (5 minutes) and the connection threshold is 100 hits, then the filter is triggered every time the rate of connections exceeds 100, or exceeds a multiple of the threshold (101, 201, 301...) within the time interval.

The filters support any of the configured action sets available on the device. You can also configure IP address exceptions.

Editing a port scan/host sweep filter

- STEP 1** From the navigation pane, click **Security Profiles**.
- The Security Profiles page opens.
- STEP 2** In the **Current Profiles** table, click Profile Name for the profile you want to change.
- The Edit Security Profile page opens. The security profile must contain zones that have physical ports.
- STEP 3** On the Security Profile page, scroll down to the **Advanced Options, Filters** section.
- STEP 4** Locate the Port Scan/Host Sweep filters:
- STEP A** Click **Search Filters**. Then, on the Filter Search page, specify the search criteria:
 - STEP B** In the **Categories** selection list, click **Reconnaissance**.
 - STEP C** In the **Severity** selection list, click **Low**.
 - STEP D** Click **Search**.
 - STEP E** In the Filters List with the search results, click the >> page control button to go to the last page of the results.
- STEP 5** To add the Port Scan/Host Sweep filters to the security profile for editing, do one of the following:
- To add an individual filter, click the **Add** icon in the **Functions** column for that filter.
 - To add multiple filters, check each filter, then click **Add Selected Filters**.
- STEP 6** On the Edit Security Profile page in the **Filters** section, click the **Filter Name** to edit the settings.
- STEP 7** In the **Action/State** section, select **Use Category Settings** or **Override**. If you select **Override** to use a different action set for the filter, do the following:
- STEP A** Select **Override** in the **Parameters** section.
 - STEP B** Check the **Enabled** check box.
 - STEP C** Choose an **Action** from the drop-down list.
- STEP 8** Optionally, you can set adaptive filter settings for flow control. In the **Adaptive Filter Configuration State** section, select one of the following:
- **Use adaptive configuration settings** — Applies the global adaptive filter settings
 - **Do not apply adaptive configuration settings to this filter** — The filter will not be monitored by the Adaptive Filter mechanism
- STEP 9** In the **Scan/Sweep Parameters** section, do the following:
- STEP A** Enter the number of seconds for the **Timeout**.
 - STEP B** Enter the number of hits allowed for the **Threshold**.

STEP 10 Optionally, you can add exceptions to the filter so that the filter will not be used to monitor traffic from specified IP addresses. In the **Exceptions** section, do the following:

STEP A Enter the **Source Address**.

STEP B Enter the **Destination Address**.

STEP C Click **add to the table below**.

STEP 11 When you finish, click **Save**.

Traffic Threshold Filters



Note The default device configuration does not include any Traffic Threshold filters. You must create them based on your network requirements.

Traffic threshold filters alert you and the device when network traffic varies from the norm. The device determines normal traffic patterns based on the network statistics over time. You can set four types of thresholds for each filter:

- **major increase** — Traffic is greatly over the set threshold.
- **minor increase** — Traffic is slightly over the set threshold.
- **minor decrease** — Traffic is slightly below the set threshold.
- **major decrease** — Traffic is greatly under the set threshold.

Thresholds are expressed as a percentage of normal traffic. For example, a threshold of 150% would fire if traffic exceeded the normal amount by 50%. A threshold of 60% would fire if the level of traffic dropped by 40% from normal amount of traffic.



Note Network traffic rates are inherently erratic and can vary as much as 50% above or below the normal level on a regular basis. When you set up Traffic Threshold filters, avoid setting small variation percentages for minor and major thresholds to prevent the Traffic Threshold filter from triggering too often.

You can configure an action set for each threshold level configured for the Traffic Threshold filter. When the filter triggers, the device executes the action specified for the threshold setting that triggered the filter. You can also configure traffic thresholds to monitor traffic on the network without taking any action. All traffic threshold activity is recorded in the Traffic Threshold report (which you can view by selecting **Events > Reports > Traffic Threshold**).

Thresholds trigger when the traffic flow is above the *Above Normal* threshold, or below the *Below Normal* threshold by the set amounts. When traffic exceeds a threshold and returns to normal levels, the device executes the action specified for the threshold that triggered the filter and generates an alert. These alerts inform you of the triggered filter, when the thresholds are exceeded and return to normal,

and the exceeded amount. After the filter triggers, you must reset it to re-establish it for use in the device. The filter is not disabled, but it does require resetting.

 **Note** A triggered Traffic Threshold filter will not be applied to traffic until you manually reset it.

Traffic Threshold filter events are recorded in the Alert and Block logs (which you can view by selecting **Events > Logs**) based on the action set specified for the filter. Information on traffic threshold events is also available in the Traffic Thresholds report (which you can view by selecting **Events > Reports > Traffic Threshold**).

For additional information on managing and configuring Traffic Threshold filters, see the following topics:

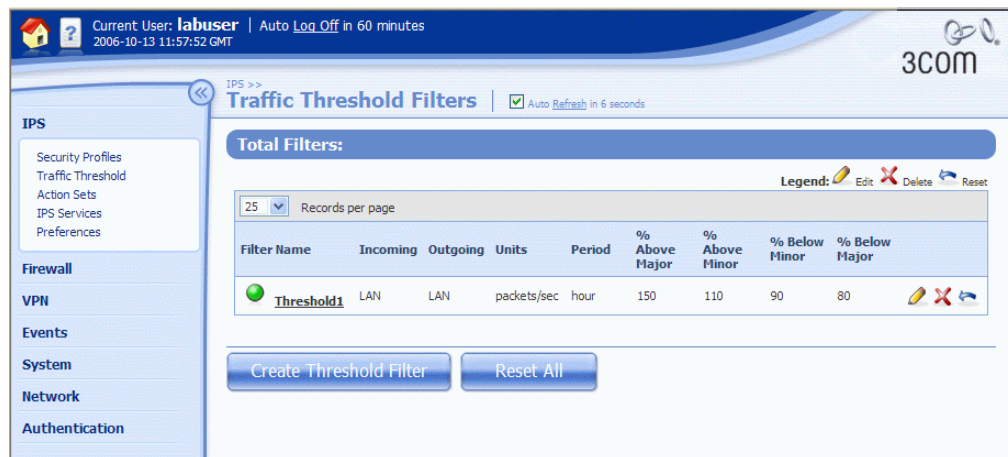
- [“Managing Traffic Threshold Filters” on page 38](#)
- [“Creating or Editing a Traffic Threshold Filter” on page 40](#)

Managing Traffic Threshold Filters

You can manage Traffic Threshold filters from the Traffic Threshold Filters page (**IPS > Traffic Threshold filters**).

The following figure shows the Traffic Threshold Filters page:

Figure 3–5: Traffic Threshold Filters Page



You can complete the following tasks from the Traffic Threshold Filters page:

- Creating a filter
- Editing a filter
- Resetting a Traffic Threshold filter — after a filter triggers, it does not resume monitoring until it is reset.
- Deleting a filter




For additional information, see the following topics:

- [“Traffic Threshold Details” on page 39](#)
- [“Creating or Editing a Traffic Threshold Filter” on page 40](#)
- [“Traffic Threshold Report” on page 124](#)
- [“Logs” on page 100](#)

Traffic Threshold Details

The following table describes the information and functions available on the Traffic Threshold Filters page:

Table 3–5: Traffic Threshold Filters Details

Column	Definition
Filter Name	Name of the filter.
Incoming	The security zone that is the traffic source.
Outgoing	The security zone that is the traffic destination.
Units	The number of selected units per second. The unit values include packets, bytes, and connections
Period	The period of time for historical data: the last minute, hour, day, 7 days, 30 days, and 35 days.
% Above Major % Above Minor	Major % — Percentage of traffic highly over the threshold. Minor % — Percentage of traffic slightly over the threshold.
% Below Minor % Below Major	Minor % — Percentage of traffic slightly under the threshold. Major % — Percentage of traffic highly under the threshold.
Functions	<p>The functions available to manage Traffic Threshold filters:</p> <ul style="list-style-type: none">  • Edit the filter to change configuration parameters.  • Delete the filter.  • Reset the Traffic Threshold filter. After a Traffic Threshold is triggered, it cannot resume monitoring until it has been reset.

Creating or Editing a Traffic Threshold Filter

Use the Create or Edit Traffic Threshold Filter pages to configure the Traffic Threshold filter for your environment. You must create a separate filter for each security zone pair that you want to monitor.

Traffic Threshold Filter Configuration Parameters

The following table describes the Traffic Threshold filter configuration parameters:

Table 3–6: Traffic Threshold Filter Configuration Parameters

Column	Definition
Filter Name	Name of the filter.
Incoming Security Zone Outgoing Security Zone	Select the security zones for the traffic source (incoming) and destination (outgoing). Only zones with a physical port are included in the selection list. Note The security zone pair that you select must be configured on a security profile. Otherwise, traffic between the zones is not inspected by IPS and the Security Profile page displays the following message: <code>No security profile is assigned to the security zones. Traffic will NOT be inspected by the IPS.</code>
Units per Second	Select the type of traffic units to track: Packets, Bytes, and Connections . Then, select the period of time for the historical data used to calculate changes in traffic rates: hour, day, 7 days, 30 days, 35 days .
Monitoring	Select the action for the Traffic Threshold filter: <ul style="list-style-type: none"> • Monitor only — The device generates a Traffic Threshold report without triggering traffic threshold (no alerts are generated). • Monitor with thresholds — When the threshold is triggered, the device performs the action configured for the threshold.
<p>Thresholds: The Thresholds parameters specify the high and low rates that will trigger the filter. Thresholds are expressed as a “% of normal” traffic. For example, a threshold of 120% would fire if traffic exceeded the “normal” amount by 20%. A threshold of 80% would fire if the level of traffic dropped by 20% from “normal” amount of traffic. Also set the state of the filter (enabled/disabled) and the action to perform when the filter triggers.</p>	
Enabled	For each threshold setting, check to enable the threshold. To disable the threshold, clear the check box.
Action	For each threshold setting, select an action to perform when the filter triggers. The action only executes if the Traffic Threshold filter monitoring state is set to Monitor with thresholds .
Above Normal	Major % — Percentage of traffic highly over the threshold Minor % — Percentage of traffic slightly over the threshold

Table 3–6: Traffic Threshold Filter Configuration Parameters (Continued)

Column	Definition
Below Normal	Major % — Percentage of traffic highly under the threshold Minor % — Percentage of traffic slightly under the threshold
Type	Select the traffic protocol or application type of the traffic to be monitored: <ul style="list-style-type: none"> • Protocol — Monitor traffic from the selected protocol: TCP, Other, ICMP, and UDP. • Application — Monitor traffic for the selected application type on the specified port: TCP or UDP and the Port. Apply to: specify whether the filter monitor tracks requests , replies , or both .
Period	The period of time for the historical data used to calculate the baseline traffic rate: minute , hour , day , 7 days , 30 days , and 35 days .

Configuring a traffic threshold filter

STEP 1 From the navigation pane, select **IPS > Traffic Threshold**.

The Traffic Threshold Filters page opens.

STEP 2 Click **Create** or click on the name of the Traffic Threshold filter you want to edit.

STEP 3 On the Create/Edit Traffic Threshold Filters page in the **Filter Parameters** section, type or edit the **Filter Name**.

STEP 4 Select the traffic source and destination security zones in the **Incoming Security Zone** and **Outgoing Security Zone** drop-down lists.

STEP 5 In the Units per Second field, select the traffic units you want to track: **Packets**, **Bytes**, or **Connections**. Then, specify the historical time period used to calculate the baseline traffic level to compare against: **minute**, **hour**, **day**, **7 days**, **30 days**, or **35 days**.

STEP 6 For **Monitoring**, select an option: **Monitor only** or **Monitor with thresholds**. (The **Monitor only** option sets the device to generate a report without triggering traffic thresholds.)

STEP 7 Configure up to four threshold parameter settings, the state (enable/disable), and the action for the filter:

Thresholds settings are specified as a percentage change from the “normal” baseline:

STEP A For **Above Normal Major Threshold**, select the **Enabled** check box, enter a percentage amount of normal. Then, select the action to perform when the filter triggers.

STEP B For **Above Normal Minor**, select the **Enabled** check box, enter a percentage amount of normal. Then, select the action to perform when the filter triggers.

STEP C For **Below Normal Major**, select the **Enabled** check box, enter a percentage amount of normal. Then, select the action to perform when the filter triggers.

STEP D For **Below Normal Minor**, select the **Enabled** check box, enter a percentage amount of normal. Then, select the action to perform when the filter triggers.

STEP 8 Select either the protocol or application **Type** for the traffic to be monitored:

- **Protocol** — Select the type of protocol from the drop-down list: **TCP**, **Other**, **ICMP**, or **UDP**.
- **Application** — Select the type of application: **TCP** or **UDP**; enter the **Port**. Then, select one of the following to apply the type to: **requests**, **replies**, or **both**.

STEP 9 When you finish, click **Save/Create**.

Action Sets

Action sets determine what the X family device does when a packet triggers a filter. An action set can contain more than one action, and can contain more than one type of action. The types of action that can be specified include the following:

- **Flow Control** — determines where a packet is sent after it is inspected. A *permit* action allows a packet to reach its intended destination. A *block* action discards a packet. A block action can also be configured to *quarantine* the host and/or perform a *TCP reset*. A *rate limit* action enables you to define the maximum bandwidth available for the traffic stream.
- **Packet Trace** — lets you capture all or part of a suspicious packet for analysis. You can set the packet trace priority and packet trace verbosity for action sets.
 - **Priority** — sets the relative importance of the information captured. Low-priority items will be discarded before medium-priority items if there is a resource shortage.
 - **Verbosity** — determines how much of a suspicious packet will be logged for analysis. If you choose *full* verbosity, the whole packet will be recorded. If you choose *partial* verbosity, you can choose how many bytes of the packet (from 64 to 1600 bytes) the packet trace log records.
- **Notification Contacts** — indicates the contacts to notify about the event. These contacts can be systems, individuals, or groups.



Note You must create or modify a notification contact before configuring an action set that uses the contact. For details, see [“Notification Contacts” on page 49](#).

TCP Reset and Quarantine Actions

For Block action sets, you can configure TCP Reset and Quarantine options.

- **TCP reset** allows the device to reset the TCP connection for the source or destination IP when the Block action executes.



Note Globally enabling the TCP Reset option may negatively impact system performance. 3Com recommends using this option for issues related to mail clients and servers on email-related filters.

- **Quarantine** allows the device to block packets based on the IP addresses in the packet that triggers the filter. When a filter with a quarantine option triggers, the device installs two blocks, one for the flow (as is normally done with Block actions) and another for the quarantined IP address. In

In addition to installing the two blocks, the device quarantines the IP address based on the instructions in the action set. For example, the user can display a Quarantine web page to notify the user of the problem and optionally provide instructions for fixing it, or the action may redirect all traffic from the quarantined IP address to a quarantine server that provides instructions to correct the problem.

Action Set Configurations

The following table describes various action set configurations that can be configured:

Table 3- 7: Action Set Configurations

Action Name	Description
Recommended	This is a default action set that cannot be modified. When this action set is assigned to a filter, the filter uses the recommended action setting based on the default category settings for the filter. The device uses this action set to allow filters within the same category to have different configurations. For example, if you set an entire category of filters to recommended, some filters may be disabled while others are enabled; some may have permit actions assigned while others are set to block.
Block (+TCP Reset) (+Quarantine)	Blocks a packet from being transferred to the network. TCP Reset is an option for resetting blocked TCP flows. Quarantine is an option that redirects the host IP address to a quarantine page or area to protect the network from being infected or compromised.
Block + Notify (+TCP Reset) (+Quarantine)	Blocks a packet from being transferred and notifies all selected contacts of the blocked packet. TCP Reset is an option for resetting blocked TCP flows. Quarantine is an option that redirects the host IP address to a quarantine page or area to protect the network from being infected or compromised.
Block + Notify + Trace (+TCP Reset) (+Quarantine)	Blocks a packet from being transferred, notifies all selected contacts of the blocked packet, and logs all information about the packet according to the packet trace settings. TCP Reset is an option for resetting blocked TCP flows. Quarantine is an option that redirects the host IP address to a quarantine page or area to protect the network from being infected or compromised.
Permit + Notify	This is a default action set. Permits a packet and notifies all selected contacts of the packet.
Permit + Notify + Trace	This is a default action set. Permits a packet, notifies all selected contacts of the packet, and logs all information about the packet according to the packet trace settings.

Default Action Sets

The X family device is preconfigured with a collection of default action sets. You can edit the default settings for an action set, or create a new one. You cannot delete a default action set. The following actions sets are available:

- Recommended
- Block
- Block + Notify
- Block + Notify Trace
- Permit + Notify
- Permit + Notify + Trace

Managing Actions

Use the Action Sets page to review, create and modify action sets.

The following figure shows the Action Sets page:

Figure 3–6: Action Sets Page

Action Set	Action(s)	TCP Reset	Quarantine	Packet Trace	Contact(s)	Function(s)
Recommended	Category Dependent					
Block	Block					Management Console
Block + Notify	Block				Management Console	
Block + Notify + Trace	Block		Enabled		Management Console	
Permit + Notify	Permit				Management Console	
Permit + Notify + Trace	Permit		Enabled		Management Console	

You can complete the following tasks from the Action Sets page:

- Viewing and managing existing actions — to sort the Actions listing by characteristics, use the link at the top of each column in the **Action Sets** list table
- Accessing the Create and Edit options
- Accessing the Notification Contacts page to configure contact information



For additional information, see the following topics:

- [“Action Sets Details” on page 45](#)
- [“Configuring an action set” on page 45](#)
- [“Rate Limit Action Set” on page 46](#)
- [“Quarantine Action Set” on page 46](#)

Action Sets Details

The Action Sets page provides the following information for each action configured on the device:

Table 3–8: Action Sets Details

Column	Description
Action Set	The name of the action set
Action(s)	The settings for the actions included in the action set
TCP Reset	Indicates whether the option to reset a TCP connection is enabled. With TCP reset enabled, the device can reset the TCP connection for the source or destination IP when the Block action executes. This option can be configured on Block action sets.
Quarantine	Indicates whether the option to Quarantine an IP address is enabled.
Packet Trace	Whether or not packet tracing is enabled.
Contact(s)	Where notifications will be sent if a Notification Contact is configured on the action set.
Function(s)  	<p>The functions available to manage the action set:</p> <ul style="list-style-type: none"> • Delete a custom action set. You cannot delete a default action set or an action set that is currently assigned to a filter. • Edit the action set configuration. (You cannot edit the <i>Recommended</i> action set.)

Configuring an action set

STEP 1 From the navigation pane, select **IPS > Action Sets**.

The Actions Sets page opens.

STEP 2 Click **Create Action Set**, or click the **Edit** icon for the action set you want to edit.

STEP 3 On the Create/Edit Action Set page, type or edit the **Action Set Name**.

STEP 4 For **Actions**, select a flow control action setting:

- **Permit** — Allows traffic.
- **Rate Limit** — Limits the speed of traffic. Select a **Rate**.
- **Block** — Does not permit traffic.

TCP Reset — Used with the **Block** action, resets the source, destination, or both IPs of an attack. This option resets blocked TCP flows.

Quarantine — Used with the **Block** action, blocks an IP (source or destination) that triggers the filter. See [“Configuring a Quarantine action set” on page 48](#).

STEP 5 Optionally, click the **Packet Trace** check box:

STEP A Select the **Priority** from the drop-down list: **High, Medium, or Low**.

STEP B Select the **Verbosity** from the drop-down list.

If you choose partial verbosity, choose how many bytes of the packet to capture (between 64-1600).

STEP 6 Choose one or more **Contacts** by checking the box next to the appropriate **Contact Name**. If there are no contacts displayed, you must create one first.



Note If using Quarantine on a managing SMS, you must add the SMS notification contact to the action sets for filters. Only filters with the SMS contact enabled on actions sets are accessible through the SMS for quarantine.

STEP 7 Click **Create**.

Rate Limit Action Set

A Rate Limit action set defines a maximum bandwidth that can be used by traffic that matches filters assigned to that action set. Incoming traffic in excess of this bandwidth is dropped. If two or more filters use the same rate limiting action set, then all packets matching these filters share the bandwidth. For example, if filters 164 (ICMP Echo Request) and 161 (ICMP Redirect Undefined Code) use the same 10 Mbps action set, then both “Echo Requests” and “Redirect Undefined Codes” filters share the 10 Mbps “pipe” as opposed to each filter getting a dedicated 10 Mbps pipe.

The supported rates are subject to restrictions based on the device model. Any of these listed rates can be used as long as it does not exceed 25% of the total bandwidth of the product.

See [Appendix C, “Device Maximum Values”](#) for supported rates for X family devices.

Quarantine Action Set

Quarantine action sets are Block action sets configured to block or redirect traffic from the host IP address for the filtered traffic. By enabling quarantine with a Block action set, you reduce the exposure of your network to internal and external threats.

When a filter with a quarantine option is triggered, the device installs two blocks, one for the flow (as is normally done with Block actions) and another for the quarantined IP address. In addition to installing the two blocks, the device quarantines the IP address based on the instructions in the action set. For example, the user can display a Quarantine web page to notify the user of the problem and optionally provide instructions for fixing it, or the action may redirect all traffic from the quarantined IP address to a quarantine server that provides instructions to correct the problem.

You can review the list of currently quarantined IP addresses from the Quarantined Streams page (which you can view by selecting **Events > Managed Streams > Quarantined Streams**). You can also force an address into quarantine, or release a quarantined address. For additional information, see [“Quarantined Addresses Page” on page 115](#).

Quarantine Action Set Configuration Parameters

The following table describes the Quarantine Action Set configuration parameters:

Table 3–9: Quarantine Action Set Configuration Parameters

Parameter	Description
Web Requests	Select an option to specify how the Quarantine action manages HTTP traffic: <ul style="list-style-type: none"> • Block the requests entirely • Redirect the client to another web server • Display quarantine web page with information on the triggered filter and any customized message specified. For details, see “Configuring a Quarantine action set” on page 48.
Other Traffic	Determines how the device handles other non-HTTP traffic when the Action set is triggered: Block or Permit .
Limit quarantine to the following IP address(es)	Create a list of “limit to” IP addresses. This option limits the filter using this action set to quarantine only those connections and systems matching the IP addresses listed.
Thresholds	Specifies a threshold to prevent network users from being quarantined the first time their network traffic triggers a filter configured with a quarantine action set: <ul style="list-style-type: none"> • Quarantine Threshold is the number of hits before the threshold is reached • Quarantine Threshold Period is the time interval for the hit count For example, if you enter 5 for the Quarantine Threshold and 30 for the Quarantine Threshold Period, only hosts which match a filter 5 times in 30 minutes are quarantined. <p>Threshold parameter limits are 1 to 10,000 hits during a period from 1 to 60 minutes.</p> <p>If thresholds are not configured, a host is quarantined the first time its traffic matches a filter configured with a quarantine action set.</p>
Do not quarantine the following IP addresses	Create a list of excluded IP addresses which will not be quarantined. Even if a quarantine filter is triggered, these IP addresses will not be quarantined, continuing with other commands in the action set. For example, the action set may include quarantine commands to block the traffic and redirect web requests to a particular server.
Allow Quarantined Host Access	Configure a list of IP addresses that a quarantined host is still allowed to access if traffic from the host triggers the Quarantine action set.

Configuring a Quarantine action set

- STEP 1** From the navigation pane, click **Action Sets**.
The Action Sets page opens.
- STEP 2** Click **Create Action Set**, or click the Edit icon for a filter you want to edit.
- STEP 3** On the Create/Edit Action Sets page, type or edit the **Action Set Name**, as needed.
- STEP 4** On the Create/Edit Action Sets page in the **Actions** table, select **Block**. Then, select the **Quarantine** check box. The page is updated to display the Quarantine Options table.
- STEP 5** Select one of the following options to configure **Web Requests**:
- Select **Block** to block web requests entirely.
 - Select **Redirect to a web server** and type a web server address to redirect any received web requests to this web server.
 - Select **Display quarantine web page** to display a quarantined web page. Then, check the types of information to include on the quarantine page. Optionally, enter custom text to display additional information.
- STEP 6** To determine how the device manages quarantine when non-HTTP traffic matches a filter, choose an action: **Block** or **Permit**.
- STEP 7** To limit the quarantine actions to a specific IP addresses, do the following:
- STEP A** In the **Limit quarantine to the following IP address(es)** table, enter a **Source Address**.
- STEP B** Click **add to table below**.
- STEP C** Repeat to add multiple IP addresses.
- STEP 8** Configure **Threshold** settings to specify the number of filter matches required before the quarantine action is executed.
- STEP 9** To perform the quarantine actions without affecting specific IP addresses, do the following:
- STEP A** In the **Do not quarantine the following IP address(es)** table, enter a **Source Address**.
- STEP B** Click **add to table below**.
- STEP C** Repeat to add multiple IP addresses.
- STEP 10** To allow quarantined clients access to hosts:
- STEP A** In the **Allow quarantined hosts to access the following IP address(es)** table, enter a **Destination Address**.
- STEP B** Click **add to table below**.
- STEP C** Repeat to add multiple hosts.
- STEP 11** When you finish, click **Create/Save**.

Notification Contacts

Configuring notification contacts lets you send messages to a recipient (either human or machine) in response to a traffic-related event. The traffic-related event can be the result of triggering an IPS filter configured with an action set that specifies a notification contact, or by triggering a Firewall Block rule with syslog logging enabled. A notification contact can be any of the following:

- **Remote System Log** — Sends messages to a syslog server on your network. This is a default contact available in all IPS action sets. Before using this contact, configure the IP address and port for the syslog server (by selecting **System > Configuration > Syslog Servers**). The Remote System Log is also the destination for all messages from Firewall Block rules with the **enable syslog logging** option turned on.
- **Management Console** — Sends messages to the LSM or SMS applications. This default contact is available in all action sets. If this contact is selected messages are sent to the Alert or IPS Block Log in the LSM, depending on whether a permit or block action has executed. When the device is under SMS management, messages are also sent to the SMS client application. This notification contact does not require any configuration, although you can change the default name and aggregation period.
- **Email or SNMP** — Sends messages to the email address or specified SNMP contact. All email or SNMP contacts must be added from the Notification Contacts page. If the default email server is not configured on the device, you will be prompted to configure it before adding a contact.

After configuring notification contacts, you can select them for IPS filter events when you create or edit the action set assigned to the filter. For Firewall Block rules, you can specify that messages be sent to the Remote System Log contact by selecting the **enable syslog logging** option when you edit the rule.

Alert Aggregation and the Aggregation Period

The X family device uses Alert Aggregation to protect system performance. Because a single packet can trigger an alert, attacks with large numbers of packets could potentially flood the alert mechanism used to send out notifications. Alert aggregation lets you receive alert notifications at intervals to prevent this flooding. For example, if the aggregation interval is five minutes, the device sends an alert at the first IPS filter trigger, then collects subsequent alerts and sends them out every five minutes.

On the device, alert aggregation is controlled by the *aggregation period* that you configure when you create a notification contact. This setting is required for all notification contacts. For email contacts, the aggregation period works in conjunction with the *Email Threshold* setting configured for the email server. By default, the device allows ten email alerts per minute. On the first email alert, a one-minute timer starts. The device sends email notifications until the threshold is reached. Any notifications received after the threshold is reached are blocked. After one minute, the device resumes sending email alerts. The device generates a message in the system log whenever email notifications are blocked.



CAUTION Short aggregation periods can significantly affect system performance. The shorter the aggregation period, the higher the system load. In the event of a flood attack, a short aggregation period can lead to system performance problems.

In addition to the user-configured aggregation period, the device also provides alert aggregation services to protect the device from over-active filters that can lower performance.

For details on configuring Notification Contacts, see the following topics:

- [“Creating an email or SNMP notification contact” on page 50](#)
- [“Configuring the remote system log contact” on page 50](#)
- [“Configuring the Management Console contact” on page 51](#)
- [“Deleting a notification contact” on page 51](#)

Creating an email or SNMP notification contact



Note Before creating an email or notification contact, you must configure email and SMTP server settings on the device from the Email Server page (**System > Configuration > Email Server**). For details, see [“Email Server” on page 266](#).

- STEP 1** From the navigation pane, select **IPS > Action Sets**.
The Action Sets page opens.
- STEP 2** Choose the **Notification Contacts** tab.
The Notification Contacts page opens.
- STEP 3** Click **Add Contact** or select the **Edit** icon for the contact you want to edit.
- STEP 4** Type **Contact’s Name**. This name is used to manage the contact information on the Notification Contacts page.
- STEP 5** Enter the address where notifications will be sent in the **To Email Address** field.
- STEP 6** Enter the **Aggregation Period**. (Longer aggregation periods improve system performance.)
- STEP 7** Click **Create** to save the changes.
- STEP 8** Optionally, click **Test Email**. The device attempts to send an email message, using the server defined in the default email settings, to the email contact you are creating.

Troubleshooting Email Notification

If the email fails to send properly, check for the following possible causes:

- Is the default email server configured? See [“Email Server” on page 266](#).
- The email server must be reachable from the device. In the CLI, use the `ping` command to see if you can reach the email server IP address.
- The email server may not allow mail relaying. Make sure you use an account/domain that the email server accepts.

Configuring the remote system log contact



CAUTION In adherence to RFC 3164, remote syslog, sends clear-text log messages using the UDP protocol with no additional security protections. Therefore, you should only use remote syslog on a secure, trusted network to prevent syslog messages from being intercepted, altered, or spoofed by a third party.

- STEP 1** From the navigation pane, select **IPS > Action Sets**.
The Action Sets page opens.
- STEP 2** Click the **Notification Contacts** tab.

The Notification Contacts page opens.

STEP 3 In the **Contacts List**, click the **Remote System Log** link.

The Edit Notification Contact page opens.

STEP 4 Type the **IP Address** and **Port** for the host that receives the offloaded log messages.

STEP 5 Type the **IP Address** and **Port** for the host that will receive remote system log messages.



TIP Verify that the device can reach the remote system log server on your network. If the remote system log server is on a different subnet than the device management port, you may have to add static routes (see [“Static Routes Page” on page 169](#)).

STEP 6 Select an **Alert Facility** and a **Block Facility**: **none** or select from a range of 0 to 31. These numbers identify the message source.

STEP 7 Select a **Delimiter** for the generated logs: **tab**, **comma**, **semicolon**, or **bar**.

STEP 8 Click **Add to table below** to add the remote syslog server.

STEP 9 Enter a **Remote system log aggregation period** in minutes.

STEP 10 When you finish, click **Save**.

Configuring the Management Console contact

STEP 1 From the navigation pane, select **IPS > Action Sets**.

The Action Sets page opens.

STEP 2 Click the **Notification Contacts** tab.

The Notification Contacts page opens.

STEP 1 Click the **Edit** icon next to the Management Console entry.

STEP 2 Edit the **Contact Name**. By default, it is Management Console.

STEP 3 Enter the **Aggregation Period** for notification messages in minutes.

STEP 4 When you finish, click **Save**.

Deleting a notification contact



Note You cannot delete the default remote system log and Management Console contacts.

STEP 1 From the navigation pane, select **IPS > Action Sets**.

The Action Sets page opens.

STEP 2 Click the **Notification Contacts** tab.

The Notification Contacts page opens.

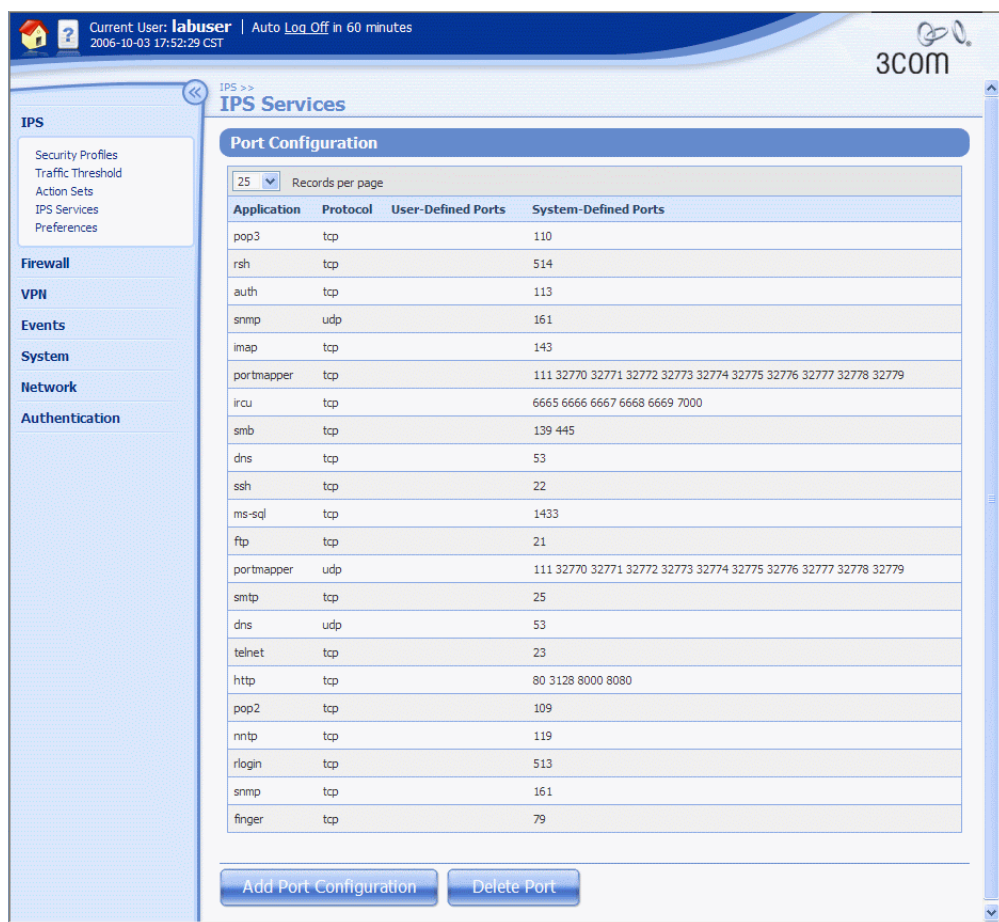
- STEP 3** Click the **Delete** icon to remove the notification contact.
 You cannot delete a Notification Contact if it is currently configured on an action set.
- STEP 4** On the confirmation dialog, click **OK**.

IPS Services

Use the IPS Services page (**IPS > Services**) to add and manage non-standard ports supported by the device. This feature lets you configure additional ports associated with specific applications, services, and protocols to expand traffic scanning. First, filters scan traffic against the standard ports for listed services, then the device accesses and scans traffic against the list of additional ports. Each service supports up to 16 additional ports.

The following figure shows the IPS Services page:

Figure 3–7: IPS Services Page



From the IPS Services page, you can complete the following tasks:

- Adding an additional port configuration
- Deleting a custom port configuration

For additional information, see the following topics:

- [“IPS Services Page Details” on page 53](#)
- [“Adding a port” on page 53](#)
- [“Deleting a port” on page 53](#)

IPS Services Page Details

The IPS Services page provides the following information:

Table 3–10: IPS Services Details

Parameter	Definition
Application	Type of application/network service.
Protocol	The protocol for the application.
User-Defined Ports	The list of the custom ports defined on the device. Ports are listed in order with a space between each number.
System-Defined Ports	The list of supported ports per application. Ports are listed in order with a space between each number.

Adding a port

STEP 1 From the navigation pane, click **IPS Services**.

The IPS Services page opens.

STEP 2 Click **Add Port Configuration**.

The Create Port Configuration page opens.

STEP 3 In the Application Type/Port Assignment table, select the **Application Type**. Then, enter a **Port Number**.

STEP 4 Click **Create**. Then, click **OK** on the confirmation pop-up.

Deleting a port



Note You cannot delete any of the default port configurations configured on the device.

STEP 1 From the navigation pane, click **IPS Services**.

The IPS Services page opens.

STEP 2 Click **Delete Port**.

The Delete Port Configuration page opens.

STEP 3 Select the **Application Type** for the port configuration to delete.

The selection list only includes applications that have been configured with a custom port.

- STEP 4** Select a **Port Number** to delete.
You can only delete one port at a time.
- STEP 5** Click **Delete** to delete the port and return to the IPS Services page.

Preferences

Use the IPS Preferences page (**IPS > Preferences**) to configure settings related to the Threat Suppression Engine and filtering performance. From this page you can complete the following tasks:

- Resetting all filters to the factory default settings
- Configuring timeouts, logging, and other settings for the Threat Suppression Engine
- Changing the global settings for the Adaptive Filter function
- Viewing the most recent filters affected by the Adaptive Filter configuration

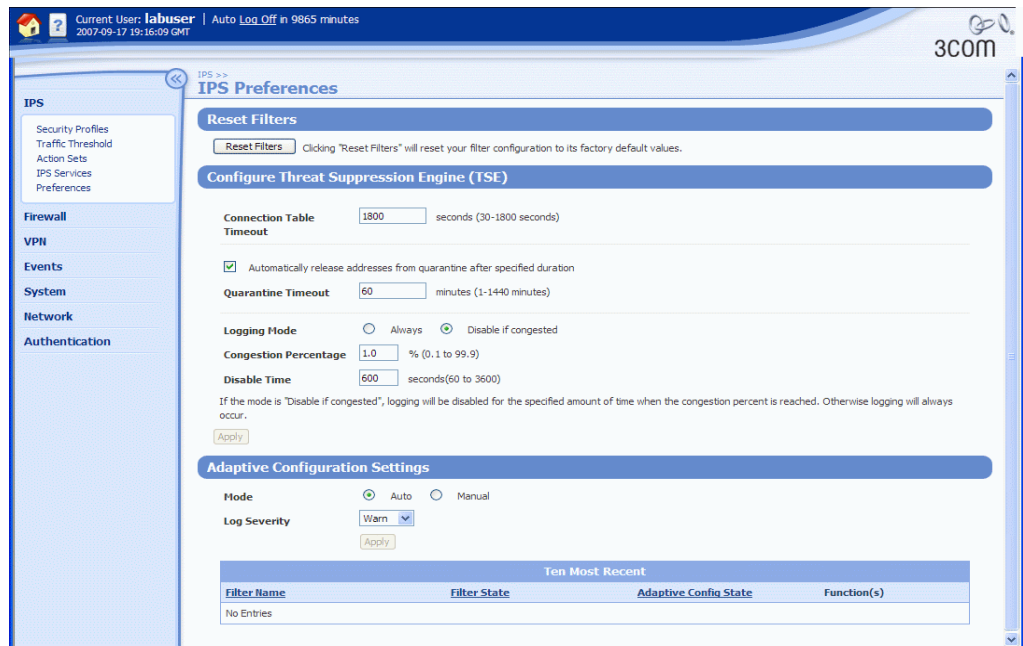
[Reset Filters](#)

[Configuring the Threat Suppression Engine](#)

[Adaptive Filter Configuration](#)

The following figure shows the IPS Preferences pane:

Figure 3–8: IPS Preferences Page



Reset Filters

To restore IPS filters and associated settings to the factory default settings, use the Reset Filters option, available on the Preferences page.



CAUTION The Reset Filter action restores all filters back to their recommended category settings. You will lose any filter customizations made in the security profiles. You will also lose any user-created action sets, rate limits, traffic thresholds, and so forth. You cannot undo this action.

Resetting the IPS filters to factory default settings

STEP 1 From the navigation pane, select **IPS > Preferences**.

The IPS Preferences page opens.

STEP 2 Click **Reset Filters**. Then, click **OK** on the confirmation pop-up.

Configuring the Threat Suppression Engine

You can configure global settings for the TSE on the IPS Preferences page, in the Configure Threat Suppression Engine table. The following table describes the TSE configuration parameters:

Table 3–11: IPS Preferences: TSE Configuration Parameters

Parameter	Description
Connection Table Timeout	<p>Specifies the global timeout interval for the connection table. For blocked streams in the connection table, this value determines the time interval that elapses before the blocked connection is cleared from the connection table. Before the timeout occurs, any incoming packets for that stream are blocked at the device. After the connection is cleared (the timeout interval expires), the incoming connection is allowed until or unless traffic matches another blocking filter.</p> <p>Note Blocked streams can also be cleared from the connection table manually from the Blocked Streams page (Events > Managed Streams > Blocked Streams).</p>
Quarantine Timeout	<p>The value for the quarantine timeout. This value applies to all quarantined addresses and determines the amount of time that elapses before the address is released from quarantine.</p> <p>Note Quarantined streams can also be released manually from the Quarantined Streams page (Events > Managed Streams > Quarantined Streams).</p>

Table 3–11: IPS Preferences: TSE Configuration Parameters (Continued)

Parameter	Description
Logging Mode	<p>Configure settings to prevent traffic-related event notifications (such as those generated when a triggered filter is configured with a Block+Notify or Permit+ Notify action set) from causing network congestion.</p> <ul style="list-style-type: none"> • Logging Mode determines whether logging is enabled or disabled when the network becomes congested. Always indicates that the device continues logging even if traffic is dropped under high load. Disable if congested indicates the logging will be disabled when the device reaches the specified congestion percentage. • Congestion Percentage can be configured if the disable logging option is selected. This value specifies the amount of network congestion that can occur before the device disables logging functions. • Disable Time specifies the amount of time (default is 10 minutes) that logging is disabled before the service is restarted. When the downtime expires, the device re-enables logging and displays the number of missed notifications.

Configuring global settings for the TSE

STEP 1 From the navigation pane, select **IPS > Preferences**.

The IPS Preferences page opens.

STEP 2 In the **Configure Threat Suppression Engine (TSE) table**, change the configuration parameters as required:

- To configure the Quarantine Timeout, check **Automatically release addresses from quarantine after specified duration**.
- To configure **Congestion Percentage** and **Disable Time** for the disable logging feature, select **Disabled if congested in** the **Logging Mode** field.

STEP 3 When you finish, click **Apply**.

Adaptive Filter Configuration

You can configure the global settings for the Adaptive Filter from the IPS Preferences page (**IPS > IPS Preferences**) and the Configure Adaptive Filter Events page (**Events > Reports > Adaptive Filter**). At the filter level, you have the option to disable Adaptive Filter configuration so that a filter is never affected by Adaptive Filter settings on the device. For details, see [“Editing DV Filter Category Settings” on page 29](#).

For additional information, see the following topics:

- [“How Adaptive Filtering Works” on page 57](#)
- [“Restrictions” on page 57](#)
- [“Tuning Adaptive Filter Configuration” on page 57](#)

How Adaptive Filtering Works

Adaptive Filtering is a mechanism to configure the Threat Suppression Engine to automatically manage filter behavior when the X family device is under extreme load conditions. This feature protects your network against the potential adverse affects of a filter that interacts poorly with the network environment by preventing the device from entering High Availability mode.

Adaptive filtering works by monitoring each filter to identify any suspected of causing congestion. When it identifies a filter, it manages the filter using one of the following methods, depending on how the global or filter-level Adaptive Filtering is configured:

- **Automatic Mode** — This setting enables the device to automatically disable and generate a system message regarding the problematic filter.
- **Manual** — This setting enables the device to generate a system message regarding the problematic filter. However, the filter is not disabled.

Restrictions

You cannot configure adaptive filter settings for Traffic Threshold, Reconnaissance, or Traffic Normalization filters.

Tuning Adaptive Filter Configuration

You can view the ten filters most recently affected by the Adaptive Filter Configuration in the **Ten Most Recent** table, available on the IPS Preferences page and the Configure Adaptive Filter Events page (**Events > Reports > Adaptive Filter**). From this table, you can click on a filter name to change the global or filter-level AFC settings. For details on this table, see [Table 5–16, “TSE Adaptive Filter Configuration Details,” on page 125](#). You can manage global AFC configuration by modifying the Mode and Log Severity settings on either the IPS Preferences page or the Configure Adaptive Filter Events page.

Configuring the global TSE Adaptive Filter setting

STEP 1 From the navigation pane, select **IPS > Preferences**.

The IPS Preferences page opens.

STEP 2 In the **Adaptive Configuration Settings** table, select the mode:

- **Automatic Mode** — This setting enables the device to automatically disable and log any defective filter.
- **Manual** — This setting enables the device to log any defective filter without disabling it.

STEP 3 Select the **Log Severity** of the system log message that is automatically generated when a filter triggers the Adaptive Filter function.

STEP 4 When you finish, click **Apply**.

4 Firewall

The Firewall section describes how to enable, disable, and modify firewall rules and various features using the Firewall Rules table. This section also details virtual servers, services, service groups, and schedules.

Overview

The X family of Unified Security Platforms provides a stateful packet inspection firewall, providing session level control for IP-based protocols. The firewall can perform advanced session-oriented functions including Network Address Translation (NAT), Web content filtering, spam filtering, virtual servers (DMZ), and traffic prioritization.

The firewall only opens TCP or UDP ports between two IP addresses when the firewall rules permit the communication. Secondary connections (for protocols such as FTP and SIP) are opened automatically where appropriate, and only for the duration of the primary session.

Firewall rules control the flow of traffic between security zones, provide bandwidth management, and ensure quality of service. You can use firewall rules to:

- Determine when and how traffic will be classified and controlled by the device.
- For local users who have been authenticated, determine whether the user has permission to access the requested service, based on the privilege group the user belongs to.
- Prioritize specific types of network traffic.
- Allow or deny a session request.
- Apply Web content filtering to specific categories of Web site or by URL (with wildcard support).
- Filter email by IP address.
- Schedule when a service will be denied or allowed.
- Allocate bandwidth resources to a service and ensure that a service has available bandwidth.
- Limit bandwidth resources to certain services.
- Time out idle sessions.
- Monitor network traffic.

For a full description of firewall rules, together with configuration examples, see the *Concepts Guide*.

You can view and manage firewall rules and configuration options from the Firewall menu pages. The menu provides the following options:

- **Firewall Rules** —Manage and configure security policy to monitor traffic between security zones. You can also specify IP hosts, subnets, or ranges to monitor traffic within a specified zone. You can optionally configure services, rate limiting, scheduling, authentication, and Web content filtering as part of each firewall rule.
- **Services** —Manage services based on applications and protocols to police the traffic. The device supports a predefined list of services and also lets you define custom services and IP protocol numbers. You can also create a **Service Group** so you can configure one firewall rule to apply to multiple services without having to configure each service separately. You only need to configure services if you want to change the port and protocol settings for an existing service or create a new service.
- **Schedules** —Create schedules to limit when a firewall rule operates. Schedules contain intervals of days and hours when the firewall rule applies. You only need to configure schedules if you require a firewall rule that will only apply at certain days and times.
- **Virtual Servers** —Configure virtual servers on your LAN, protected by the device firewall, that can be accessed from the Internet or another security zone without exposing the internal network IP addresses. You should configure virtual servers for internal servers that need to be reached from the Internet. A common application for virtual servers is to create a Demilitarized Zone (DMZ).
- **Web Filtering** —Web filtering lets you configure a subscription-based Web content filtering service and/or specify URL filters to permit or deny traffic based on specific URLs or URL patterns.
- **Anti-Spam** —Anti-spam lets you configure a subscription-based spam filtering service and/or specify filters to permit or deny email based on specific IP addresses.



Note Before setting up firewall rules, verify that the network configuration (IP address groups, virtual interfaces, and security zones) has been set up correctly for your environment. See [Chapter 6, “Network”](#) for more information.

For details, see the following sections:

- [“Default Firewall Rules” on page 61](#)
- [“Setting Up Firewall Rules” on page 62](#)
- [“Schedules” on page 77](#)
- [“Virtual Servers” on page 80](#)
- [“Web Content Filtering” on page 84](#)
- [“Anti-Spam” on page 94](#)

Default Firewall Rules

The following table lists the default firewall rules available on the X family device. You can add, delete, or edit these rules. However, be careful when editing or deleting the default rules, as this may prevent you from configuring the device or accessing some services on the device. If this does happen, you can restore access by resetting the device to factory default settings, using the instructions provided in the *Hardware Installation and Safety Guide*.

Table 4–1: Default Firewall Rules Configuration

ID	Action	Source Zone	Dest Zone	Service	Logging	State	Description
1	Permit	LAN	WAN	ANY	Off	Enabled	Allow LAN unrestricted access to WAN
2	Permit	ANY	this-device	vpn-protocols	Off	Enabled	Allow VPN termination
3	Permit	LAN	this-device	management	Off	Enabled	Allow management access from LAN via https, ssh, snmp, or ping
4	Permit	LAN	this-device	network protocols	Off	Enabled	Allow DNS and DHCP-server from LAN
	Permit	this-device	ANY	ANY		Enabled	This is an implicit firewall rule that cannot be modified or viewed from the LSM. It is needed for AutoDV, Web content filtering, and other features. This rule also allows the Network Tools to operate.
	Block	ANY	ANY	ANY		Enabled	Implicit rule that blocks all other traffic with a silent drop.

The default firewall rules configured for the *this-device* zone use the LAN security zone. The management IP address of the X family device is any of the IP interface addresses. The device IP address is not generally accessible to the LAN by ping (or other services) unless a firewall rule allows such access. The device lets you configure a firewall rule to prevent access to the management interface, even from the LAN security zone.



Note If you delete the **this-device** zone, you may only be able to access the device using the command line interface (CLI) on the serial port.

For additional information on managing firewall rules from the LSM, see the following topics:

- [“Setting Up Firewall Rules” on page 62](#)
- [“Configuring Firewall Rule Components” on page 68](#)

Setting Up Firewall Rules

This section provides an overview of setting up policies on the device.

1. Create services (optional).
2. Create service groups (optional).
3. Create schedules (optional).
4. Create firewall rules with your services and schedules.
5. Allow access to internal servers (optional).
6. Allow one-to-one NAT (optional).

Step 1: Creating Services

To create a service:

1. Go to **Firewall > Services**. Add a new service.
2. Select the protocol applicable to the service (**TCP/IP** or **ICMP**); for IP, enter the protocol number.
3. Enter the port ranges for your service.

Configuration Example

The following table shows a configuration for the service Kamanda:

Table 4–2: New Service Configuration Example

Fields	Value
Name	Kamanda
Protocol	TCP
Destination Ports	10081

Step 2: Creating Service Groups

To create a service group:

1. Go to **Firewall > Service Groups**. Create a Service Group.
2. Add the services that you want to associate with the group.

All the services associated with the group are listed in the **Current Services in Group** table.

Configuration Example

The following table shows configurations for two service groups, created for Internet access and VPN:

Table 4-3: Service Group Configuration Example

Service Group	Services
Internet-access	HTTP, HTTPS, POP3, FTP
VPN	IPSec, LT2P, GRE

Step 3: Creating Schedules

If you are not applying schedule restrictions to your policies, then this step is optional.

To create a schedule:

1. Go to **Firewall > Schedules**. Add a new schedule.
2. Select the days of the week that you want to add to the schedule.
3. Select the time interval (in hours:minutes) during which the schedule will run.
4. You can optionally add multiple day and time interval combinations to the schedule.

All the times associated with the schedule are listed in the **Current Schedule** table.

Configuration Example

The following table shows a schedule defining access to HTTPS services for a local college:

Table 4-4: Schedule Configuration Example

Name	Schedule
School-hours	Monday–Friday, 08:30 to 19:00
Weekend-roster	Saturday 09:00 to 12:00 Saturday 14:00 to 16:00 Sunday 14:00 to 16:00
Mid-week	Tuesday–Thursday, 09:30 to 17:00

Step 4: Creating Firewall Rules

To create a new firewall rule:

1. Go to **Firewall > Firewall Rules**.
2. Determine where in the list of policies you want your new firewall rule to be placed. Highlight the rule that you want to appear immediately after the new rule in the list and click **Add**. This will place your new rule above the one selected.
3. Define the action applied by the rule: **Permit** or **Block**.
4. If you want to apply the firewall rule, check **Enable Firewall Rule**.
5. To record sessions using this firewall rule in the Traffic Log, check **Enable logging**.

6. Select the service that the rule covers (for example, HTTP). Select a service group if you want your firewall rule to apply to a service group that you have created. For example, HTTP, HTTPS, FTP, and POP3 email could all be grouped together in an Internet Access service group.
7. Define a schedule for the rule. By default, the device applies the rule **Always**.
8. Check **Enable Anti-Spam** and **Enable Web-Filter** (optional).
9. Configure network source and destination zones, and IP address ranges:
 - Select one of the configured security zones, or the **ANY** option, if you wish the firewall rule to be applied to any source/destination zone.
 - You can also select an IP Address Group, or define a specific IP range for the source/destination (this is displayed in parenthesis in the Firewall Rules list).



Note Your firewall rule cannot use the same source and destination zones (since firewall restrictions are not applied to traffic within the same zone).

10. In the **Advanced Options** section, define bandwidth management (optional):
 - Apply bandwidth **Per Session** or **Per Rule**. **Per Session** allocates a fixed bandwidth for the duration of the session. **Per Rule** divides the available bandwidth by the number of concurrent sessions.
 - Select the **Guaranteed Bandwidth** you want to be applied to this firewall rule/service.
 - Select the **Maximum Bandwidth** you want to be applied to this firewall rule/service. This sets the limit to the amount of available bandwidth that the device can allocate to the service.
 - Select the **Bandwidth Priority**. The top priority queue minimizes latency for latency-sensitive traffic (such as voice).
11. Select whether to apply authentication. If applied, then select one of the following options:
 - Enable access to authenticated users from all privilege groups. Check **Any privilege group with firewall authentication**.
 - Restrict access to authenticated users within a specified privilege group. Select the privilege group from the drop-down list.
12. Check that the rules are in the correct order. A new firewall rule is placed just before the firewall rule currently selected, or at the end of the **Firewall Rules** table, if no firewall rule is selected. To move the rule higher or lower in the list, select the rule and then click the Move Up or Move Down buttons.



Note To improve throughput, put the most frequently used rules at the top of the list. If the device goes through the list and cannot find a matching rule, it will deny the session.

Configuration Example

The following table shows a new firewall rule created for FTP access:

Table 4–5: Firewall Rules Configuration Example

Field	Value
Firewall Rule	Staff access to FTP
Action	Permit
Service	FTP
Schedule	Monday–Friday, 09:00–17:00 Saturday–Sunday, 10:00–14:00
Source Zone	LAN
Destination Zone	WAN
Bandwidth management	Type: per rule Guaranteed bandwidth: 1000 Kbps Maximum bandwidth: 2000 Kbps Priority 3
Authentication	Permit users in privilege group “Staff”

Step 5: Allowing Access to Internal Servers

To allow access to an internal server, you must define a virtual server. To define a virtual server:

1. Go to **Firewall > Virtual Servers**. Add a new virtual server.
2. Select the service for which you want to define the private LAN server IP address.
3. Enter the **Local IP address** used to map to the external (public) IP address.
4. Define the Public IP address (either **Use External Interface IP Address** of the device or manually enter the external IP address that is part of the device’s subnet).
5. Configure the port. For example, use HTTP port 80.
6. Add a firewall rule to permit the incoming service from the appropriate source IP address.

Configuration Example

The following table shows an example that applies to a virtual server mapping a local IP address to a public IP address for an HTTP service:

Table 4–6: Virtual Server Configuration Example

Field	Value
Service	HTTP
Public IP	10.20.1.2
Local IP	192.168.1.1

Table 4–6: Virtual Server Configuration Example (Continued)

Field	Value
Local Port	80

Step 6: Configuring One-to-One NAT

One-to-one NAT allows a device on the private LAN to appear to the external network with a public IP address. The steps in configuring a one-to-one NAT include:

1. Go to **Firewall > Virtual Servers**. Add a new virtual server.
2. Select **All** for the Service.
3. Enter the local IP address of the LAN device.
4. Enter the corresponding public IP address for this device.

Managing Firewall Rules

The Firewall Rules page (**Firewall > Firewall Rules**) displays a list the firewall rules currently configured on the device. From this page, you can view, edit, enable, disable, and re-order firewall rules.

The following figure shows the Firewall Rules page:

Figure 4–1: Firewall Rules Page

Current User: labuser | Auto Log Off in 9998 minutes
2007-08-30 21:56:05 GMT

3COM

FIREWALL > Firewall Rules

Firewall Rules List

Filter Firewall Rules by Zone

Show Firewall Rules from source: All to destination: All [Filter Rules] [Cancel]

Firewall Rules are applied in order of precedence. In the case of any conflicting rules, the rule with a higher precedence will be applied. (To move a Firewall Rule up in order of precedence, simply click and hold to drag the rule into a higher position.)

ID	Action	Source Zone	Dest Zone	Service	Advanced	Comment	State	Function(s)
5	Permit	any	this-device	any	<input checked="" type="checkbox"/>		Enabled	
6	Permit	this-device	any	any			Enabled	
1	Permit	LAN	WAN	any		Allow LAN unrestricted access to WAN	Enabled	
2	Permit	WAN	this-device	vpn-protocols		Allow VPN termination	Enabled	
3	Permit	LAN	this-device	management		Allow management access from LAN	Enabled	
4	Permit	LAN	this-device	network-protocols		Allow DNS and DHCP from LAN	Enabled	

[Apply]

Create Firewall Rule

You can complete the following tasks from the Firewall Rules page:

- Creating or editing a firewall rule.
- Deleting a firewall rule.
- Filtering the firewall rules list to display only those rules configured for a user-specified source and destination zone.

When the firewall rules list is filtered, the LSM only shows filters that match the criteria selected in the **Filter Firewall Rules by Zone** filter options.

Firewall Rules List Details

The Firewall Rules List page displays the following information for each rule in the list:

Table 4–7: Firewall Rules List Details









Column	Description
ID	A unique ID system-assigned to the firewall rule.
Action	The action that will be applied when this firewall rule is matched for a given session: Permit or Block.
Source Zone (Addresses)	Indicates the source security zone for the session request. By default, the source zone includes all IP addresses within the given zone. If the firewall rule has been configured to apply only to a subset of IP addresses, the subset (IP address group, subnet, or IP address range) is displayed.
Dest Zone (Addresses)	Indicates the destination security zone where traffic will be directed if it is permitted. By default, the destination zone includes all IP addresses within the given zone. If the firewall rule has been configured to send permitted traffic to only a subset of IP addresses, the subset (IP address group, subnet, or IP address range) is displayed.
Service	The service or service group associated with the firewall rule. The firewall rule only applies to a session request for the specified service or service within the specified Service Group. If ANY is specified, the firewall rule applies to all services available.
Advanced	<p>The icons indicate which advanced options are enabled for the firewall rule. If a feature is enabled, an icon representing the feature is displayed in the Firewall Rules List page. Available options are:</p> <ul style="list-style-type: none">  Bandwidth Management (traffic shaping) — If this option is configured, any traffic permitted by the firewall rule is given the bandwidth priority and rate specified in the firewall rule.  Schedule — If this option is configured, the firewall rule is only applied during the days and times configured in the firewall rule schedule.  User Authentication — If this option is configured, the firewall rule is only applied to local users who have been authenticated by the device.  Web Filtering Enabled — If this option is configured, any URL that triggers the firewall rule is examined.

Table 4–7: Firewall Rules List Details (Continued)

Column	Description
	<ul style="list-style-type: none"> • Logging Enabled — If this option is configured, any event triggered by the firewall rule (Permit or Block) is entered into the appropriate log.
Comment	The firewall rule description entered when the rule was created.
State	Whether the firewall rule is enabled (checked) or disabled (not checked)
Function(s)	<p>Icon representing functions available to manage the firewall rule:</p> <ul style="list-style-type: none">  • Edit the firewall rule.  • Delete the firewall rule.  • Add firewall rule — clicking this icon in a firewall rule entry lets you create a firewall rule that will be added above the rule selected.

Configuring Firewall Rule Components

When configuring a firewall rule, you must define the action, logging options, and other components that make up the rule. Before you can configure the firewall rule, the components should be configured so that they are available for selection during the configuration process. The following describes the firewall rule components:

- **Action** — This is a required component that determines how the device manages packets when the firewall rule is matched. You can configure the firewall to permit or block traffic that matches the firewall rule.
- **Services** — When you configure a firewall rule, you must select the service or service group to which it will be applied. The device provides predefined services which are applications known to the device such as HTTP, HTTPS, and DNS. You can also configure custom services to manage any IP protocol. For details on configuring services and service groups, see [“Firewall Services” on page 73](#).
- **Schedule** — Optionally, you can configure the firewall rule to only be applied during certain days and times. For details on configuring schedules, see [“Schedules” on page 77](#).
- **Inactivity Timeout** — Optionally, you can configure the firewall rule to terminate an established session if there is no activity for a specified period of time.
- **Logging Options** — Determines whether the device creates a log entry when the firewall rule is triggered. For example, if logging is enabled on a firewall that blocks traffic, the device generates an entry in the Firewall Block log. If remote system logging is enabled, the device generates an entry and sends it to the remote Syslog server as well. If logging is enabled on a firewall permit rule, the device generates a session start and session end log entry in the Firewall Session Log. For details on the

syslog servers, see [“Configuring Remote System Logs” on page 107](#). By default, when you create a firewall rule, logging is disabled.

- **IPS Filtering** — Determines whether the device uses IPS filtering. By default, IPS filtering is enabled; turning off IPS might be appropriate to improve performance if the source or destination networks, or the range of IP addresses, are trusted.
- **Spam Filtering**— Determines whether the device uses the Anti-Spam Service to examine the IP addresses of email senders. For details, see [“Anti-Spam” on page 94](#).
- **Web filtering** — Determines whether the device uses the Web Content Filtering Service to examine requested URLs according to a predefined Web filter profile. For details on setting up Web filter profiles, see [“Web Filter Profiles” on page 87](#).
- **Source and Destination Zones** — All firewall rules must specify the source and destination addresses of the devices to which the firewall rule applies. This is specified using security zones. If necessary, you can limit the rule to apply to certain IP addresses within a security zone. For details on setting up security zones, see [“Security Zone Configuration” on page 135](#).
- **IP Addresses** — To limit the firewall rule to apply only to certain devices within a security zone, you can specify an IP address group, subnet, or range. For IP address group configuration details, see [“IP Address Groups Page” on page 156](#). The default IP address setting for the source and destination zones is all IP addresses within the zone.

Advanced Options

When creating or editing a firewall rule, you can configure advanced options to enable bandwidth management and user authentication for the firewall rule:

- **Bandwidth Management** — If this option is selected, you can define the guaranteed and maximum bandwidth available for your sessions, to apply the guaranteed bandwidth on a per-session or per-rule basis, and to prioritize the bandwidth for a session.
- **User Authentication** — If this option is selected, the rule will only be applied if the rule otherwise matches the selection (for example, correct service and IP address), and a local user with appropriate matching privileges has previously been authenticated with the X family device. This authentication may be the result of logging in using the HTTP or HTTPS interface, or by using a VPN client terminating on the device. If a local user has not been authenticated, the rule is ignored and lower priority rules are examined to find a match the session. This option can be used to create a “captive portal” environment in which users can only browse Internet Web pages after they authenticate themselves by username and password.



Note For additional information on the advanced options, see the **Concepts Guide**.

Configuration Notes

Firewall rules provide great flexibility to implement policy. Consider the interaction of the various components of a firewall rule as you configure the rule. For example, you can define a rule that permits traffic except for certain services, URLs, or IP addresses; or you can define a rule that blocks traffic except for certain services, URLs, or IP addresses.

When a firewall rule is created, the default settings are as follows:

- The rule is enabled
- The rule is applied to all services and service groups
- All services are examined
- The rule is always checked
- A session is terminated in 30 minutes if there is no activity
- IPS is enabled
- Spam filtering is disabled
- Web content filtering is disabled
- Logging is disabled
- The rule is positioned at the end of the firewall rules table (that is, it is applied last)

After configuring a firewall rule, it will appear in the firewall rules table. You can disable firewall rules so that the device ignores the rule when inspecting traffic. If necessary, you can re-enable the rule later.

Creating or editing a firewall rule



Note For firewall configuration examples, see the **Concepts Guide**.

STEP 1 From the navigation pane, select **Firewall > Firewall Rules**.

The Firewall Rules page opens.

STEP 2 Do one of the following:

- To create a new rule, click **Create Firewall Rule** at the bottom of the page. (You may have to scroll down to access the button.)
- To edit an existing rule, click the **Edit** icon for the rule you want to edit.
- To create a firewall rule above another rule in the table, click the **+** icon on the existing rule.

The Create/Edit Firewall Rule page opens.

STEP 3 In the Firewall Rule Setup (Basic) section, enter the setup information:

STEP A If you want to apply the firewall rule, click **Enable Firewall Rule**.

STEP B Select the **Action** you want the rule to apply to the traffic: **Permit** (the default) or **Block**.

STEP C From the **Service** drop-down list, select the service or service group that the rule will apply to.



Note To add a new service or service group, select **Firewall > Services** to open the Firewall Services page. Then, define the service. You can then define firewall rules for that service or service group.

STEP D From the **Schedule** drop-down list, select the schedule you want the rule to use. The default is **Always**.

- STEP E** In the **Inactivity Timeout** field, enter the interval (between 1 and 999 minutes) after which you want any established session to be terminated if there is no activity. The default is 30 minutes.
- STEP F** Optionally, type a description for the rule in the **Comment** field.
- STEP G** To record sessions matching this firewall rule in the Firewall Session Log (for permitted sessions) or Firewall Block Log (for blocked sessions), check **Enable logging**.
- STEP H** To bypass IPS processing for traffic that matches this firewall rule, regardless of the IPS security profile defined, check **Skip IPS**. (This is appropriate to improve performance if the source or destination networks, or the range of IP addresses, are trusted.)
- STEP I** To enable anti-spam filtering for traffic that matches this firewall rule, check **Enable Anti-Spam**. The Service setting must include SMTP port 25 for this setting to have effect.
- STEP J** To enable Web content filtering for traffic that matches this firewall rule, check **Enable Web-Filter**. The Service setting must include HTTP or HTTPS for this setting to have effect. (For information on creating a Web filter profile, see [“Creating or editing a Web filter profile” on page 89.](#))

If you enable Web content filtering, additional options become available:

- If you check **Require Users to Authenticate**, users affected by this firewall rule are first required to authenticate themselves by entering their username and password. Select a Web filter profile from the drop-down list that is used if the user has no defined privilege group or the authentication service does not return one.
- If you do not check **Require Users to Authenticate**, select a Web filter profile from the drop-down list that is used for all Web requests from the source zone.

If you do not permit HTTP/HTTPS service, users cannot access any Web site. If you permit HTTP/HTTPS service but do not enable Web content filtering, users can access any Web site.

- STEP 4** In the **Network** section, configure the **Source** and **Destination** zone parameters:
- STEP A** From the **Source Zone** drop-down list, select the source security zone for this firewall rule.
- Select **Any** if you want the firewall rule to match traffic from any source zone.
 - Select **this-device** if you want to match traffic from the device itself; for example, to allow the device to send HTTP packets, Auto DV Update requests, or Web Content Filtering Service requests to the LAN.



Note An implicit this-device ==> ANY rule is provided by default at the end of the firewall rule table. 3Com recommends not overriding this implicit rule.

- STEP B** For **Source IP**, select the IP addresses in the source zone to which you want to apply the rule.
- Select **All IP addresses**. This is the default selection.
 - Select **IP Address Group** and then select the group from the drop-down list.
 - Select **IP Subnet** and type the IP address/subnet mask.

- Select **IP Range** and type the range of IP addresses.

STEP C From the **Destination Zone** drop-down list, select the destination security zone for this firewall rule.

- Select **Any** if you want the firewall rule to match traffic to any destination zone.
- Select **this-device** if you want to match traffic destined for the device itself; for example, to let you manage the device using HTTPS, allow Auto DV Updates, or Web content filtering.

STEP D For **Destination IP**, select the IP addresses in the destination zone to which you want to apply the rule.

- Select **All IP addresses**. This is the default setting.
- Select **IP Address Group** and then select the group from the drop-down list.
- Select **IP Subnet** and enter the IP address/subnet mask.
- Select **IP Range** and enter the range of IP addresses.

STEP 5 If required, click **Show Advanced Options**.

The **Firewall Rule Setup (Advanced)** section appears.

STEP 6 If required, check **Enable Bandwidth Management**. Bandwidth management only works on Permit rules.

To control the rate of traffic flow between zones, configure bandwidth management as follows:

STEP A In the **Type** field, choose the type of bandwidth management to be applied, either:

- **Per Rule** to indicate that the total bandwidth will be shared by all sessions that match the rule.
- **Per Session** to indicate that the specified amount of bandwidth will be available to every session that matches the rule.

STEP B Enter the **Guaranteed Bandwidth** (between 1 and 1000000 Kbps).

This value mainly provides pre-allocated bandwidth for particular traffic. The device ensures that a session that matches this firewall rule is provided with this bandwidth. (In effect, the device throttles other non-prioritized traffic to ensure this.)

STEP C Enter the **Maximum Bandwidth** (between 1 and 1000000 Kbps).

If a session attempts to use more than its maximum bandwidth, the excess packets are dropped.

STEP D Select the **Bandwidth Priority** you want to apply to the session from the drop-down list, where 0 is the highest priority and 3 is the lowest priority.

The device transmits higher priority session packets before lower priority session packets. Use priority 0 for applications such as VoIP that require low latency.



Note Generally, bandwidth management works best if a small amount of traffic is prioritized as priority 0 over all other traffic via a single bandwidth management rule. A good example is prioritizing voice traffic over everything else. 3Com does not recommend using priorities 1-3 to form complex bandwidth management policies. Such configurations are hard to define and harder to verify as working.

STEP 7 When you finish, click **Create** to save the firewall rule, or click **Cancel** to return to the **Firewall Rules** page without saving the changes.

Enabling or disabling a firewall rule

STEP 1 From the navigation pane, select **Firewall > Firewall Rules**.

The Firewall Rules page opens.

STEP 2 In the **Firewall Rules List** table, click the **Edit** icon for the firewall rule you want to edit.

The Edit Firewall Rule page opens.

STEP 3 In the **Firewall Rule Setup (Basic)** section, check **Enable Firewall Rule** to enable the rule.

To disable the rule, clear the check box.

STEP 4 When you finish, click **Save**.

Changing the order in which firewall rules are applied

STEP 1 From the navigation pane, select **Firewall > Firewall Rules**.

The Firewall Rules page opens.

STEP 2 Select the rule you want to move and drag it to the desired location.

STEP 3 When you finish, click **Apply**.

Firewall Services

Firewall services and service groups are used to specify firewall rules and virtual servers. See [“Appendix C, “Device Maximum Values”](#) for device maximum configurable values.

- **Firewall service** — A TCP or UDP port, ICMP type, or IP protocol that can be monitored by a firewall rule to police traffic. For example, to monitor all FTP traffic, select “ftp” from the pull-down menu when you configure the firewall rule for this policy.
- **Firewall service group** — A logical grouping of services that lets you configure a firewall rule or virtual server to apply to traffic from more than one service. For example, the “web” service group includes the http and https services. To monitor both HTTP and HTTPS traffic, select the web service group when you configure the firewall rule.

Service groups let you configure a single firewall rule or virtual server to apply to traffic from a collection of services rather than creating individual configurations for each service. After the service and service groups have been configured, you can assign them to firewall rules or virtual servers based on your network security requirements.

Use the Firewall Services page (**Firewall > Services**) to view and manage services and service groups. The following figure shows the Firewall Services page:

Figure 4–2: Firewall Services Page

The screenshot displays the Firewall Services page with the following data:

Service	Protocol	Ports
3com-nbx	17	2093 - 2096
audio-call-control	6	1731
dhcp-client	17	68
dhcp-server	17	67
dns-tcp	6	53
dns-udp	17	53
eigrp	88	-
finger-tcp	6	79
ftp	6	21
gopher-tcp	6	70
gre	47	-
h323	6	1720
http	6	80
https	6	443
igmp	2	-
ike	17	500
imap	6	143
imapv3	6	220
ipsec-ah	51	-
ipsec-esp	50	-
kerberos-tcp	6	88
kerberos-udp	17	88
l2tp	17	1701
ldap-tcp	6	389
ldap-udp	17	389

Service Group	Service(s)
dns	dns-tcp, dns-udp
email	pop3, smtp, imap, imapv3
ipsec	ike, ipsec-ah, ipsec-esp
ldap	ldap-udp, ldap-tcp
management	https, ssh, ping, snmp-request
netmeeting	h323, audio-call-control, t120
network-protocols	dns-tcp, dns-udp, dhcp-server
nfs	portmapper-tcp, portmapper-udp, nfsd-tcp, nfsd-udp
pptp	pptp-tcp, gre
secure-management	https, ssh
sip	sip-tcp, sip-udp
sms-config	http, https, sms-client, snmp-request, ssh
sms-get	ntp, sms-trap
snmp	snmp-request, snmp-trap
vnc	vnc-browser, vnc-viewer
voice	3com-nbx, sip-tcp, sip-udp
vpn-protocols	pptp-tcp, l2tp, gre, ike, nat-tipsec
web	http, https

You can complete the following tasks from the Firewall Services page:

- Adding a service to add or change a port and protocol configuration, or to define an arbitrary IP protocol
- Editing a service to add or change a port and protocol configuration
- Adding a service group
- Editing a service group to add or remove services
- Deleting a service or service group



For additional information, see the following topics:

- [“Firewall Service and Service Group Information” on page 75](#)
- [“Adding a service” on page 75](#)
- [“Editing a service” on page 76](#)
- [“Configuring Service Groups” on page 76](#)
- [“Adding a service group” on page 76](#)
- [“Editing a service group” on page 77](#)

Firewall Services Page Field Descriptions

The following table describes the fields available on the Firewall Services page:

Table 4–8: Firewall Service and Service Group Information

Column	Description
Firewall Services	
Service	The name of the service. This name appears in the Service drop-down selection list for firewall and virtual interface configuration.
Protocol	The IP protocol used by the service.
Ports	The TCP or UDP port numbers associated with the service, or the ICMP type for services that use the ICMP protocol.
Firewall Service Groups	
Service Group	The name of the service group. This name appears in the Service dropdown selection list for firewall and virtual interface configuration.
Service(s)	The services associated with the service group.
Functions	
<p>The functions available for services and service groups are:</p> <p>Note You cannot edit or delete default services. You can only edit services that you have created.</p> <ul style="list-style-type: none">  • Edit a service or service group to add or remove services  • Delete a service or service group 	

Adding a service

STEP 1 On the LSM menu, select **Firewall > Services**.

The Firewall Services page opens.

STEP 2 Click **Add Service** to add a service.

The Create Firewall Service page opens.

STEP 3 Configure the service details:

STEP A If this is a new service, type the **Service Name**. Names cannot contain spaces.

STEP B Select a **Protocol** for the type of connection to be established from the drop-down list. Protocol types supported are TCP, UDP, ICMP, and IP.

STEP C Depending on the protocol you selected, do one of the following:

- If the protocol is TCP or UDP, in the **Destination Ports** fields, type the port numbers associated with the service.

- If the protocol is IP, type the IP protocol number in the field.

STEP 4 Click **Create**.

Click **Cancel** to return to the Firewall Services page without saving the changes.

Editing a service



Note You cannot edit the default services.

STEP 1 On the LSM menu, select **Firewall > Services**.

The Firewall Services page opens.

STEP 2 Click the service name or **Edit** icon to edit an existing user-defined service.

The Edit Firewall Service page opens.

STEP 3 Configure the service details:

STEP A Select a **Protocol** for the type of connection to be established from the drop-down list.

STEP B Depending on the protocol you selected, do one of the following:

- If the protocol is TCP or UDP, in the **Destination Ports** fields, type the port numbers associated with the service.
- If the protocol is ICMP, type the **ICMP Type**.

STEP 4 Click **Save**.

Click **Cancel** to return to the Firewall Services page without saving the changes.

Configuring Service Groups

Service groups let you configure a single firewall rule or virtual server to apply to traffic from a collection of services rather than creating individual configurations for each service. After service groups are configured, you can assign them to firewall rules or virtual servers based on your network security requirements.

Adding a service group

STEP 1 On the navigation menu, select **Firewall > Services**.

The Firewall Services page opens.

STEP 2 At the bottom of the **Firewall Service Groups** table, click **Add Group**.

The Create Service Group page opens.

STEP 3 Type a **Service Group Name**. Names cannot contain spaces.

STEP 4 For each service you want to add to the group, select the service from the **Service** drop-down list and click **Add to table below**.

STEP 5 After adding all services, review the **Service** table to verify the changes.

STEP 6 When you finish, click **Create** to save the new service group.

Editing a service group

STEP 1 From the navigation pane, select **Firewall > Services**.

The Firewall Services page opens.

STEP 2 In the **Firewall Service Groups** table, click the name of the service group you want to edit.

The Edit Service Group page opens.

STEP 3 To add a service, select a service from the **Service** drop-down list and click **Add to table below**. To delete a service, locate the service in the table and click its **Delete** icon.

STEP 4 When you finish, click **Save**.

The service group definition is updated.

Schedules

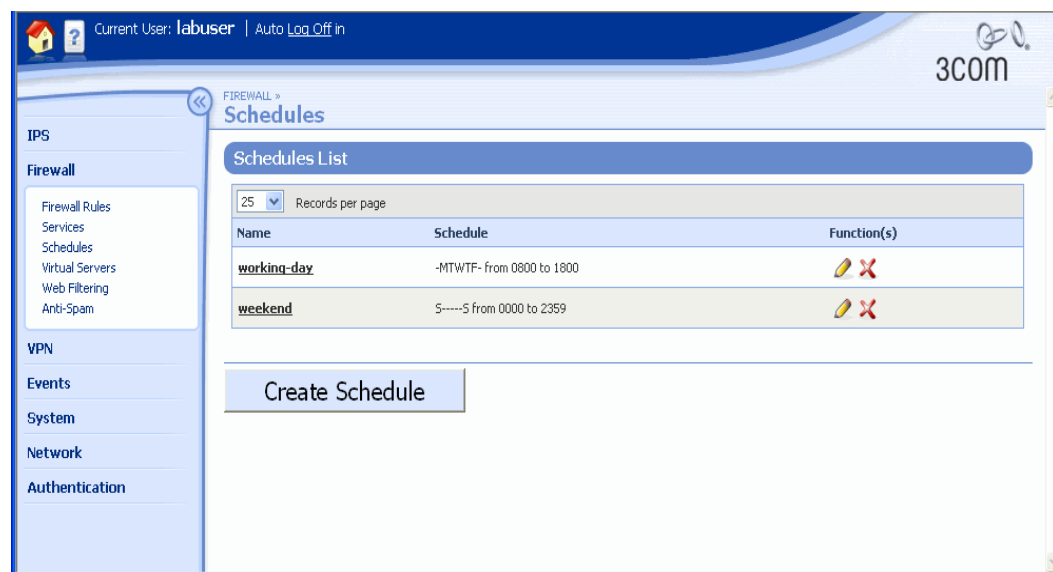
The X family device lets you create schedules that determine when a firewall rule is in use. Schedules contain intervals of days and hours when the firewall rule applies. For example, Monday to Friday, 8 AM to 6 PM could be a “work hours” schedule. Use the **Always** (default) option if you want the firewall rule to always be applied. Schedules can include multiple entries to specify different time intervals for different days.

You can apply the same schedule to as many firewall rules as required. see [“Appendix C. “Device Maximum Values”](#) for device maximum configurable values.

Use the Schedules page (**Firewall > Schedules**) to view and manage Firewall schedules.

The following figure shows the Schedules page:

Figure 4–3: Schedules Page





You can complete the following tasks from the Schedules page:

- Adding or editing a schedule
- Deleting a schedule
- Deleting days and times from an existing schedule

Firewall Schedules Page Field Descriptions

The Schedules page displays and provides the following information about existing schedules:

Table 4–9: Schedules Page: Field Descriptions

Field	Description
Name	The name of the schedule.
Schedule	<p>The days and time ranges that define the schedule.</p> <p>Note The value 00:00 is used to specify midnight as either a start or end time. A schedule cannot cross midnight (for example, 22:00 to 09:00). To achieve the effect, create two schedules, one for each side of midnight; for example, 22:00 to 23:59, and 00:00 to 09:00.</p>
Function(s)	<p>The functions available for the schedules:</p> <ul style="list-style-type: none">  • Edit a schedule to add or remove scheduled time intervals. (Click the linked Schedule name to edit the schedule.)  • Delete a schedule.

Managing Schedules

Schedules are only required if you want to configure firewall rules that are only applied to traffic at particular periods of the day, or days of the week. The default schedule for all firewall rules is to always apply, 24 hours a day, 7 days a week.

When configuring a schedule, select the days of the week that you want to add to the schedule and the time interval (in hours and minutes) during which the schedule will run. You can optionally add multiple day and time interval combinations to the schedule.

Adding or editing a schedule

STEP 1 From the navigation pane, select **Firewall > Schedules**.

The Schedules page opens.

STEP 2 Click **Create Schedule** to add a new schedule or click the **Edit** icon to edit a schedule.

The Create/Edit Schedule page opens.



Note You cannot delete or edit default schedules (that is, the schedules with which the device is pre-configured).

STEP 3 In the **Firewall Schedule** section, type the **Schedule Name**.

STEP 4 In the **Schedule Details** section, configure the days and times for the schedule:

STEP A Check the **Days** on which you want the schedule to run.

STEP B To specify the timing for the selected days, select the start and end time in the **Time: From** and **To** drop-down lists.

STEP C Click **Add to table below** to add the schedule.

Repeat Step 4 until you have configured all the required schedules.

STEP 5 When you finish, click **Create** or **Save**.

Click **Cancel** to return to the Schedules page without saving the schedule.

Deleting days and times from an existing schedule

STEP 1 From the navigation pane, select **Firewall > Schedules**.

The Schedules page opens.

STEP 2 In the **Schedules List** section, click the linked Schedule name. The Edit Schedule page opens.

STEP 3 In the **Schedule** section, click the **Delete** icon next to the schedule entry you want to delete.

STEP 4 When you finish, click **Save**.

Virtual Servers

You can configure an X family device to deploy a virtual server. A virtual server lets you define a private LAN server IP address for each service passing through the firewall. Any external request for a service directed at the device's WAN IP address is forwarded to the virtual server.

Outgoing sessions from the private server or device to the public network will use the public IP address configured for the virtual server. This allows one private IP address to be mapped to one public IP address. If you select **all services** for the service, this provides one-to-one Network Address Translation (NAT) for devices on the private LAN.

In a **one-to-one NAT** configuration, each internet IP address is associated with one LAN IP address. Effectively, each of these LAN IP addresses has its own public IP address. By using one-to-one NAT you can allow servers on your LAN, which are protected by the device firewall, to be accessed from the Internet without exposing the internal IP addresses of these hosts on your network to the Internet. Individual PCs can appear to have a public IP address if necessary.

After creating a virtual server, you must configure firewall rules that allow external devices to access internal servers. You can define a private LAN server IP address for each service passing through the firewall. Any external request for a service, directed at the specified public IP address of the virtual server, is forwarded to the virtual server.

For additional information, see the following topics:

- [“Virtual Servers Page” on page 80](#)
- [“Configuring Virtual Servers” on page 81](#)

Virtual Servers Page



Use the Virtual Servers page (**Firewall > Virtual Servers**) to view and configure virtual servers. You can complete the following tasks from this page:

- Viewing a list of existing virtual servers
- Creating a virtual server
- Editing or deleting an existing server

Virtual Servers Summary Information

The Virtual Servers page displays and provides the following information about existing virtual servers:

Table 4–10: Virtual Servers Summary Information

Column	Description
Service	The name of the service running on the server.
Public IP	The IP address for users to access the service, that is, the virtual server IP address.
Local IP	The IP address of the server on the LAN to which the virtual server is redirecting traffic. Through one-to-one NAT or Port Address Translation (PAT), accesses to the public IP addresses are changed to accesses to the local IP address/port.
Local Port	The port number on which the LAN server is running the service. Only used if PAT is enabled. For details, see “Virtual Servers Configuration Parameters” on page 82 .
Function(s)	<p>The functions available for the existing virtual servers are:</p> <ul style="list-style-type: none">  • Edit a the configuration for a virtual server. (Click the linked virtual server name to edit the schedule.)  • Delete a virtual server.

For additional information, see the following topics:

- [“Configuring Virtual Servers” on page 81](#)
- [“Configure a virtual server and provide one-to-one NAT” on page 82](#)

Configuring Virtual Servers



See [“Appendix C, “Device Maximum Values”](#) for the maximum number of virtual servers supported by your device. The following information applies to virtual server configuration:

- Virtual server traffic is subject to firewall rules. You must set up a firewall rule to allow the traffic for the desired services through the device firewall. To allow incoming traffic, use the IP address or the zone containing the IP address of the LAN device as the destination address of the firewall rule.
- When a virtual server is created for **all services** on the external IP interface of the device, all incoming sessions not otherwise intercepted as other private LAN servers for other services are directed to the server’s IP address. This configuration will result in loss of management access to the device from the WAN.

Virtual Servers Configuration Parameters

The following table describes the configuration parameters for virtual servers:

Table 4–11: Virtual Servers Configuration Parameters

Column	Description
Service	The name of the services or service group that are allowed to run on the virtual server.
Local IP	The IP address of the server on the LAN to which the virtual server is redirecting traffic. Through one-to-one NAT or PAT, accesses to the public IP address will be changed to accesses to the local IP address/port.
Public IP Address	The IP address for users to access the service or group of services (that is, the virtual server IP address): <ul style="list-style-type: none"> • Select Use external IP interface address to use the external IP interface address for the device. • Select IP address and then type an IP address that is part of the device's WAN IP subnet, but different from the one the device is currently using.
PAT Local Port	Check PAT to enable Port Address Translation. Then, specify a local port number to map a service to a different local port.
Function(s)	The functions available for the virtual servers: <ul style="list-style-type: none">  • Edit a the configuration for a virtual server. (Click the linked virtual server name to edit the schedule.)  • Delete a virtual server.

Configure a virtual server and provide one-to-one NAT

STEP 1 From the navigation pane, select **Firewall > Virtual Servers**.

The Virtual Servers page opens.

STEP 2 To add a new virtual server, click **Create**. To edit an existing one, click the **Edit** icon for that server.

The Create/Edit Virtual Server page opens.

STEP 3 Select the **Service** that will run on this virtual server.



Note To provide one-to-one NAT to a LAN client, select **ALL** from the Service drop-down list.

STEP 4 In the **Local IP Address** field, enter the IP address of the server on the LAN to which you want traffic redirected.

For one-to-one NAT, this address is the LAN client address.

STEP 5 For the **Public IP Address**, do one of the following:

- Select **Use External interface IP address**.
- Select **IP Address** and type a public IP Address that is different from the device public WAN IP address.

This option can only be used if you have been provided with multiple IP addresses. You must select this option for one-to-one NAT.

- STEP 6** If you want a default port number used by the service to be translated to a different port number by the device, check **Enable PAT** and enter the port number you want in the **Local Port** field.



Note The **Enable PAT** checkbox and the **Local Port** field are disabled if you have selected **ALL** from the Service drop-down list.

- STEP 7** When you finish, click **Create**.

Click **Cancel** to return to the Virtual Servers page without saving the changes.



Note Virtual server traffic is subject to firewall rules. You must set up a firewall rule to allow the traffic for the desired services through the firewall. To allow incoming traffic, use the IP address, or the zone containing the IP address, of the LAN device as the destination address of the firewall rule.

Configuring PAT

Normally, a service uses its default port number, but PAT or NAPT (Network Address Port Translation) allows a user to translate this to a different port number. This would allow, for example, the LAN server to run multiple instances of a Web server.

- STEP 1** Set up one-to-one NAT, but make sure you select the one service you require. (You cannot select PAT while **All Services** is highlighted.)
- STEP 2** Check **PAT** and type the port number to which the service will be mapped.
- STEP 3** Set up a firewall policy using the local IP addresses and service corresponding to the local TCP/UDP port to allow the traffic for this mapped service through the firewall.


Web Content Filtering

The options on the **Web Filtering** menu let you view and change Web filter profiles. Web content filtering (sometimes known as content filtering) lets you control access to Web sites from the device. Each profile can be configured for different levels of Web content filtering. You can assign Web profiles to firewall rules to filter based on IP address, IP address groups, security zones, or schedules. You can also use Web content filtering with user authentication and directory services such as Microsoft Active Directory, Novell eDirectory, OpenLDAP, or iPlanet. Users in different groups can receive different Web content filtering settings based on settings returned from these directory services.

The device supports filtering using both the **Web Content Filtering Service** and **custom filtering**:

- The **Web Content Filtering Service** is a subscription service that provides filtering based on classifications of Web sites. Web sites are classified into Core Categories or Productivity Categories. Core Categories are blocked by default; Productivity Categories are permitted by default. You can further control Web site access by adjusting defaults on a per-category basis.
- **Custom filtering** lets you permit or block access to different Web sites based on their URLs, domain names, or IP addresses; through pattern matching; or through keyword matching. No content categorization is used to determine whether a Web site may be accessed or not.

If you apply both types of filtering, custom filters takes precedence over Web Content Filtering Service category filters. Therefore, you can use a custom filter to override the Web Content Filtering Service for a particular Web site.

 **Note** For the device to use Web content filtering, you must set up a Permit firewall rule with the appropriate service or service group selected and the “Enable Web-Filter” option checked. This rule must be positioned in the firewall rule table to ensure it matches the Web traffic before any other rule (for example, a “permit LAN==>WAN ANY” rule) that would allow the same Web traffic.

User authentication is a method of verifying the identity of a user and associating that user with privilege rights configured on the device. User authentication can be implemented in conjunction with firewall rules to define groups of users whose activities bypass Web content filtering (more permissive) or are subject to Web content filtering (more restrictive). For example, you could allow a certain group of users unrestricted access to all Web sites, while restricting access to another group of users.


Setting Up Web Content Filtering

The following steps provide an overview of the Web content filter configuration process:

1. Configure a Web filter profile. You can modify the default profile or create a new one.
2. In the profile, configure general Web content filtering settings. These settings determine the device’s response to Web requests when the profile is enabled. For details, see [“Web Filtering Page” on page 85](#).
3. If you are using the Web Content Filtering Service, configure the Web Content Filtering Service settings. For details, see [“Web Filtering Page” on page 85](#).
4. If you are using the custom filter list, configure the Permit and Block URL lists.
5. Configure a firewall rule to apply Web content filtering. For details, see [“Configuring Firewall Rule Components” on page 68](#).

If you create a custom filter list, you can select the **Create default firewall rule** option to automatically generate the Web filtering firewall rule.

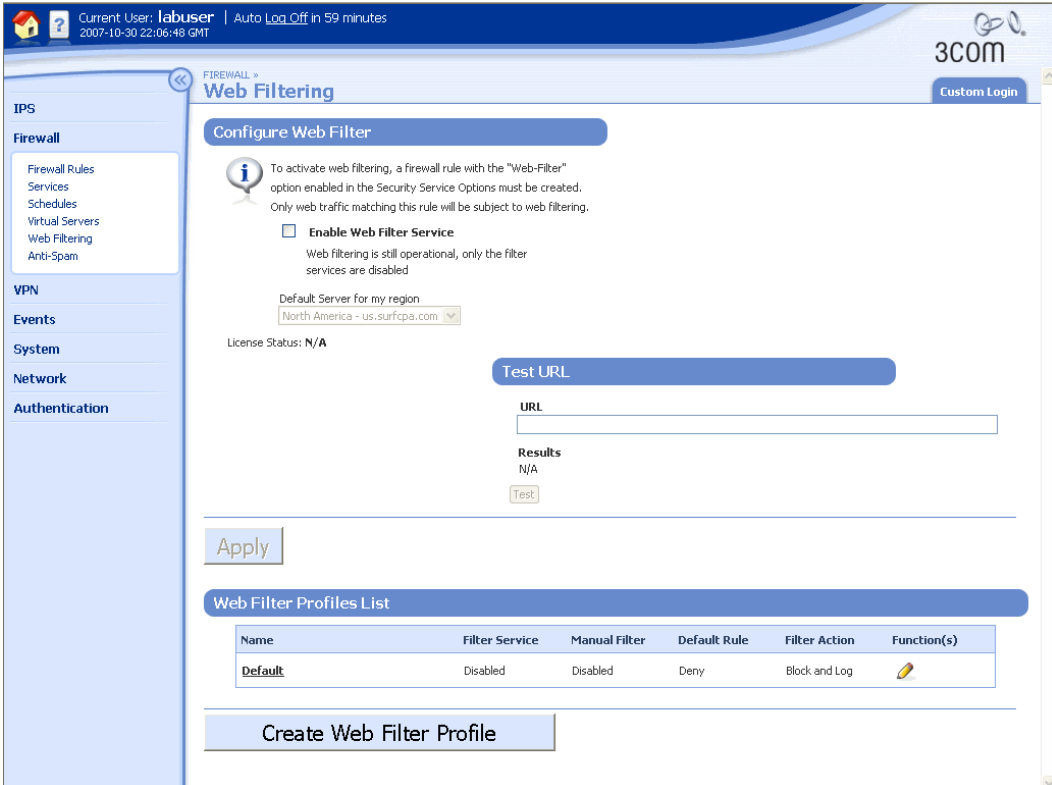
6. Reposition the firewall rule to the top of the firewall rule table.
7. Create a privilege group that includes the firewall rule and assign users to it. (Optionally, if you want to permit certain users unrestricted Web access, configure a privilege group to bypass Web filtering and assign those users to it.) For details, see [“Creating or editing a privilege group” on page 279](#).

 **Note** Existing Web content filtering rules from previous releases are converted to a Permit rule with Web filtering enabled.


Web Filtering Page

Use the Web Filtering menu page (**Firewall > Web Filtering**) to enable, configure, and manage the Web Filter functions. The following figure shows the Web Filtering page:

Figure 4–4: Web Filtering Page



The screenshot displays the 'Web Filtering' configuration page. The left sidebar contains navigation links for IPS, Firewall, VPN, Events, System, Network, and Authentication. The main content area is titled 'Configure Web Filter' and includes an information icon with the following text: 'To activate web filtering, a firewall rule with the "Web-Filter" option enabled in the Security Service Options must be created. Only web traffic matching this rule will be subject to web filtering.' Below this is a checkbox for 'Enable Web Filter Service' which is currently unchecked, with a note that 'Web filtering is still operational, only the filter services are disabled'. A dropdown menu for 'Default Server for my region' is set to 'North America - us.surfcpa.com', and the license status is 'N/A'. There is a 'Test URL' section with a text input field for the URL and a 'Test' button. Below the configuration options is an 'Apply' button. At the bottom, there is a 'Web Filter Profiles List' table and a 'Create Web Filter Profile' button.

Name	Filter Service	Manual Filter	Default Rule	Filter Action	Function(s)
Default	Disabled	Disabled	Deny	Block and Log	



You can complete the following tasks from the Web Filtering page:

- Enabling or disabling the Web Content Filtering Service.
- Creating or editing Web filter profiles.
- Deleting a Web filter profile.
- Checking the category of a URL.
- Creating a custom block page.

Web Filtering General Configuration Parameters

The following table describes the general configuration parameters to enable and configure the Web Filter functions. In addition to these parameters, you must also make sure that the device has the following items configured: a valid DNS server and default gateway (**Network > Configuration**), and Web filter firewall rules (**Firewall > Firewall Rules**).

Table 4–12: Web Filtering General Configuration Parameters

Parameter	Description
Configure Web Filter	Determines whether the Web Content Filtering Service is enabled or disabled. If the service is enabled, specify the Default Server for my region . The License Status field indicates the status of the license for the Web Content Filtering Service: <ul style="list-style-type: none"> • Licensed • Unlicensed or Cannot Connect • Timeout on connect • Not available
Web Filter Profiles List	Determines the system response to Web requests blocked by filters in the Web Content Filtering Service or the custom filters list.
Function(s)	The functions available for the Web filter profiles: <ul style="list-style-type: none">  • Edit a profile. (Click the linked profile name to edit the profile.)  • Delete a profile. (You cannot delete the default profile.)

Enabling or disabling the Web Content Filtering Service

STEP 1 From the navigation pane, select **Firewall Rules > Web Filtering**.

The Web Filtering page opens.

STEP 2 Do one of the following:

STEP A To enable the Web Content Filtering Service, check **Enable Web Filter Service**.

In the **Default Server for my region** drop-down list, select the appropriate regional server.

STEP B To disable the Web Content Filtering Service, clear the checkbox **Enable Web Filter Service**. Web filtering is still operational; only the Web Content Filtering Service is disabled.

STEP 3 When you finish, click **Apply**.

Web Filter Profiles

The following figure shows the Create Web Filtering Profile page:

Figure 4–5: Create Web Filtering Profile Page

The screenshot displays the 'Create Web Filtering Profile: New' page. At the top, it shows the current user 'labuser' and an auto-logout timer. The page is divided into a left sidebar with navigation options (IPS, Firewall, VPN, Events, System, Network, Authentication) and a main content area. The main area includes a 'Profile Name' field with 'New' entered. Below this are two sections: 'General Configuration' with checkboxes for 'Enable Web Filter Service' and 'Enable Manual URL Filtering', and 'Filtering Action' with radio buttons for 'Block Only', 'Log Only', and 'Block and Log'. A 'Default Rule' section has radio buttons for 'Permit unclassified or unknown sites' (selected) and 'Block unclassified or unknown sites'. A 'Core Categories' section allows selecting categories to be allowed, with options like 'Adult/Sexually Explicit', 'Criminal Skills', 'Drugs, Alcohol & Tobacco', 'Gambling', 'Hacking', 'Hate Speech', 'Violence', and 'Weapons'. There are also expandable sections for 'Productivity Categories', 'Block Page', and 'Custom Filter List'. At the bottom, there are 'Save' and 'Cancel' buttons.

You can complete the following tasks from the Create/Edit Web Filtering Profile page:

- Configuring the default filtering action for block events.
- Configuring the default behavior (known as the Default Rule) for managing Web requests for sites that are not included in either the filters defined by the Web Content Filtering Service filters or the

URL lists defined in the Custom Filter List, or if the Web Content Filtering Service is unavailable or unlicensed.

- Defining a custom response page to display when a Web request is blocked. This page is returned to the Web browser that made the request.
- Creating Permit/Block Lists.
- Deleting a URL from the Permit/Block List.
- Importing the Permit and Block List from another device.
- Exporting the Permit and Block List from the current device to a file.

For details, see the following topics:

- [“Web Filter Profile General Configuration Parameters” on page 88](#)
- [“Creating or editing a Web filter profile” on page 89](#)

Web Filter Profile General Configuration Parameters

The following table describes the general configuration parameters to enable and configure Web filter profile functions:

Table 4-13: Web Filter Profile General Configuration Parameters

Parameter	Description
Profile Name	Name of the Web filter profile.
General Configuration	Configures the scope of the profile: <ul style="list-style-type: none"> • Enable Web Filter Service • Enable Manual URL Filtering
Filtering Action	Determines the device’s treatment of intercepted Web requests: <ul style="list-style-type: none"> • Block Only • Log Only • Block and Log
Default Rule	Determines the device’s treatment of Web requests for sites not otherwise covered by filters: <ul style="list-style-type: none"> • Permit unclassified or unknown sites • Block unclassified or unknown sites
Core Categories	Web sites that contain offensive, potentially dangerous, or criminal content. By default, the Web Content Filtering Service blocks URLs that are included in any Core category.
Productivity Categories	Web sites that could impair productivity when used in the work environment. By default, the Web Content Filtering Service allows URLs that are included in any Productivity category.

Table 4–13: Web Filter Profile General Configuration Parameters (Continued)

Parameter	Description
Block Page (custom response page)	<p>Specifies a custom message added to the standard “access blocked” Web page displayed when a Web request is blocked by a Web content filter. You can use the following custom tags in the message:</p> <ul style="list-style-type: none"> • %url% to display the URL of the blocked page • %category% to display the category the blocked page falls under
Custom Filter Lists	<p>Permit or Block lists consisting of URL name patterns representing domain names, URLs, IP addresses, simple keywords, or regular expressions.</p> <p>The Import function lets you upload a URL list to the device.</p> <p>The Export function lets you download the current Permit and Block Pattern lists for export to another device.</p>

Creating or editing a Web filter profile

When you create a Web filter profile, you can specify the Web Content Filtering Service, manual filtering, or both, but not neither.

STEP 1 From the navigation pane, select **Firewall > Web Filtering**.

The **Web Filtering** page opens.

STEP 2 Click Create Web Filter Profile to create a new profile, or click the name or the **Edit** icon for an existing profile.

The **Create** or **Edit Web Filtering Profile** page opens.

STEP 3 Type the **Profile Name**. Use alphanumeric characters, hyphens (-), or underscores (_) only.

STEP 4 Select the **General Configuration** parameters:

STEP A To use the core and productivity categories to control access to Web sites, click **Enable Web Filter Service**.

STEP B To use the custom Permit/Block lists to control access to Web sites, click **Enable Manual URL Filtering**.

STEP 5 By default, core categories are blocked. To allow access to a category, check the check box next to its name.

STEP 6 To configure Productivity Categories filters:

STEP A Click **Productivity Categories**.


The categories appear. By default, productivity categories are allowed.

STEP B To block access to a category, clear the check box next to its name.

STEP 7 To configure a custom response page to display to users in place of a blocked request:

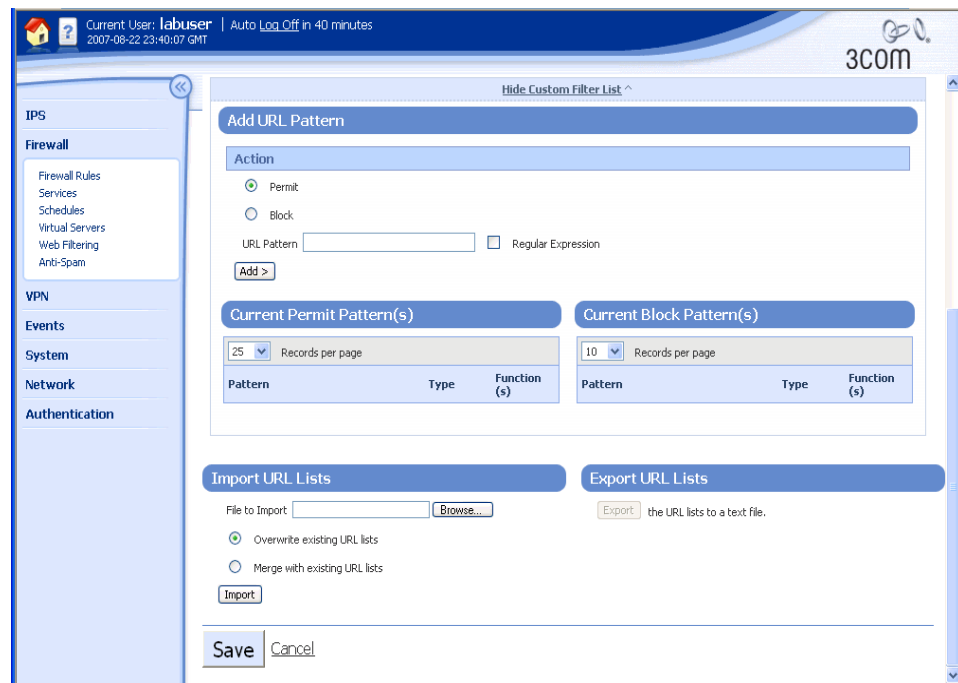
STEP A Click **Block Page**.

The **Custom Response Page** section appears.

STEP B Type the text and HTML code of the custom page.**STEP C** To preview the page, click the **Preview** icon ().**STEP 8** To configure the custom filter list:**STEP A** Click **Custom Filter List**.

Additional options appear. The following figure shows the Custom Filter List section:

Figure 4-6: Configuring Custom Filter List



STEP B In the **Add URL Pattern** section, select the action to take when a Web request matches the pattern: **Permit** or **Block**. Type or edit the **URL Pattern** you want to match. If you are using a regular expression, check the **Regular Expression** check box. (For details on creating regular expressions, see [“Configuring URL Patterns” on page 91](#).) Click **Add**; the pattern is added to the **Current Pattern(s)** table for the selected action (permit or block). Repeat for each URL pattern you need to define.

STEP C To import a list of URLs, in the **Import URL Lists** section, type the filename and path for the file to import, or click **Browse** and navigate to the file. Choose the operation you want to perform when importing the list: either **Overwrite existing URL lists** to delete the existing URL list and replace it with the imported list, or **Merge with existing URL lists** to add the imported URLs to the existing list. Click **Import** to import the list.

STEP D To export the current URL list, in the **Export URL Lists** section, click **Export** to save the URL list to a file. Then, save the resulting Custom Filter list text file.

STEP 9 When you finish, click **Save**.

Deleting a Web filter profile

You can delete any Web filter profile except the Default profile.

STEP 1 From the navigation pane, select **Firewall > Web Filtering**.

The **Web Filtering** page opens.

STEP 2 Click the **Delete** icon for an existing profile.

The system prompts: “Are you sure you wish to delete ‘*profile-name*?’”

STEP 3 Click **OK**.

The profile is deleted.

Configuring URL Patterns

Requests for access to Web sites can be permitted or blocked depending on whether the requested URL matches a pre-set pattern. A pattern can be a domain name, a URL, an IP address, a simple keyword, or a regular expression.

Keyword blocking is the simplest use of pattern matching. Any URL containing a keyword will be blocked regardless of its categorization. In addition, the asterisk (*) is interpreted as a wildcard, matching any number of any characters. Examples of patterns are:

http://www.Acme.com — URL, to match the protocol.

www.Acme.com — keyword to match the Acme site only.

www.Acme.com/* — pattern and wildcard, matching any page on the Acme.com site.

Acme — keyword and wildcards, matching www.Acme.com, ads.Acme.com, www.Acme.co.uk, and so forth.

Regular expression pattern matching enables you to enter regular expressions into the Permit/Block lists to identify URLs. URL patterns that match these expressions are either permitted or blocked.

A valid regular expression must be between 3 and 64 characters in length and conform to the full regular expression syntax. The following table shows examples of regular expression patterns:

Table 4-14: URL Pattern Regular Expression Syntax

Value	Description
x	Matches the character x.
.	Matches any character.
^	Specifies beginning of line.
\$	Specifies end of line.
[xyz]	A character class. This pattern matches either x, y, or z.
[abj-oZ]	A character class with a range. This pattern matches a, b, any letter from j through o, or Z.

Table 4-14: URL Pattern Regular Expression Syntax (Continued)

Value	Description
[^A-Z]	A negated character class. This pattern matches any character except those in the class.
r*	Zero or more r's, where r is any regular expression.
r+	One or more r's, where r is any regular expression.
r?	Zero or one r, where r is any regular expression.
.*	Matches any number of any characters.
r{2,5}	From two to five r's, where r is any regular expression.
r{2,}	Two or more r's, where r is any regular expression.
r{4}	Exactly 4 r's, where r is any regular expression.
"[xyz]"images"	The literal string [xyz]"images".
\x	If x is a, b, f, n, r, t, or v, then the ANSI-C interpretation of \x; Otherwise, a literal X. Used to escape operators such as *.
\0	A NULL character.
\123	The character with octal value 123.
\x2a	The character with hexadecimal value 2a.
(r)	Matches r, where r is any regular expression. Use parentheses to override precedence.
Rs	The regular expression r, followed by the regular expression s.
r s	Either an r or an s.
#<n>#	Inserts an end node causing regular expression matching to stop when reached. The value n is returned.

Examples of patterns are:

www.Acme.com/* — pattern to match any page on the Acme site.

.*Acme.* — pattern to match www.Acme.com, ads.Acme.com, www.Acme.co.uk, and so forth.



Note You can use the wildcard (*) character anywhere in your entries into the URL Permit and Block lists. The wildcard character is allowed with or without the Regular Expression checkbox ticked. Wildcards are not implicitly added to the front and end of the string, thus allowing you to specify an absolute URL or a wildcard URL. All matches are case insensitive.

Checking the category of a URL

You can determine if a given URL is covered by one of the Web Content Filtering Service category filters.



Note This lookup does not take account of any Web filter profiles; it only indicates the category of the URL in the Web Content Filtering Service database.

STEP 1 From the navigation pane, select **Firewall > Web Filtering**.

The **Web Filtering** page opens.

STEP 2 Ensure that the Web Content Filtering Service is running.

STEP 3 In the **Test URL** section, type the URL you want to check into the **URL** field.

STEP 4 Click **Test**.

One of the following messages appears:

- A message showing the category for the URL; for example:
`www.bbc.co.uk belongs to category News Productivity`
- A message showing that the URL is not categorized; for example:
`www.Q1I8Y6R.biz belongs to category Unknown`
- A message showing that the device cannot contact the server selected on the Web Filtering page; one of the following:
`Error. Unable to contact categorization server`
`Device cannot contact Web Filter Service`
 To resolve the error:
 - Verify the DNS configuration specified on the device.
 - Check general Internet connectivity.
 - Verify that the DNS configuration settings (**Network > Configuration > DNS**) on the external (WAN) virtual interface.
- A message showing that the Web Content Filtering Service subscription is not active:
`Error. Device is not licensed to use the 3Com web-filter service.`
 Purchase or renew the subscription for the Web Filter Service.

Anti-Spam

The options on the **Anti-Spam** menu let you view and change anti-spam settings. Spam filtering monitors incoming SMTP traffic (TCP port 25) based on the IP address of the sender. You assign spam filters as part of firewall rules.



Note For the device to use anti-spam filtering, you must set up a Permit firewall rule with the TCP service selected and the option **Enable Anti-Spam** checked. For more information about firewall rules, see [“Creating or editing a firewall rule” on page 70](#).

- [“Configuring Firewall Rule Components” on page 68](#)
- [“Anti-Spam Page” on page 95](#)
- [“Setting Up Anti-Spam Filtering” on page 96](#)

Anti-Spam Page

Use the Anti-Spam page (**Firewall > Anti-Spam**) to enable, configure, and manage the spam filtering functions. The following figure shows the Anti-Spam page:

Figure 4–7: Anti-Spam Page

Current User: labuser | Auto Log Off in 59 minutes
2007-10-31 18:17:47 GMT

3COM IP Address Test

FIREWALL » Anti-Spam

Configure Anti-Spam

To activate the Anti-Spam filtering a firewall rule with the Anti-Spam security service must be enabled
Only traffic matching this rule on TCP port 25 (SMTP) will be subject to Anti-Spam protection.

IP-Reputation

Enable Anti-Spam IP-Reputation Service

Server IP address: [pd%id.3com.ctmail]

License Status: N/A

Switch to Advanced Settings ▾

Block if risk exceeds: 75 percent

Manual Settings

Enable manual Anti-Spam filtering

Permit

No IP Addresses

IP Address Group: DHCP-Pool ▾

IP Subnet: [] Mask: []

IP Range: [] to []

IP Host: []

Block

No IP Addresses

IP Address Group: DHCP-Pool ▾

IP Subnet: [] Mask: []

IP Range: [] to []

IP Host: []

Global Settings

Filtering Action

Block Only

Log Only

Block and Log

Default Rule

Allow unclassified or unknown senders

Filter unclassified or unknown senders

Apply

You can complete the following tasks from the Anti-Spam page:

- Enabling or disabling the Anti-Spam IP Reputation service and configuring global settings that apply to both the Anti-Spam Service and manual filtering.
- Tuning the anti-spam service.
- Defining manual anti-spam settings.
- Testing an IP address.

Setting Up Anti-Spam Filtering

The following steps provide an overview of the spam filter configuration process:

1. If you are using the Anti-Spam IP Reputation Service, configure the threshold setting if necessary. For details, see [“Tuning the Anti-Spam Service” on page 96](#).
2. If you are using the manual spam filter list, configure the Permit and Block IP address lists. For details, see [“Defining manual anti-spam settings” on page 97](#).
3. Configure the highest Permit firewall rule that matches the SMTP service to apply spam filtering. For details, see [“Configuring Firewall Rule Components” on page 68](#).

Enabling or disabling the Anti-Spam Service

STEP 1 From the navigation pane, select **Firewall > Anti-Spam**.

The Anti-Spam page opens.

STEP 2 To enable the Anti-Spam Service, check **Enable Anti-Spam IP-Reputation Service**. To disable the Web Content Filtering Service, clear the checkbox .

STEP 3 In the Global Settings section, do the following:

STEP A Define a global filtering action that applies to all filtered IP addresses:

- **Block and Log** (the default)
- **Block Only**
- **Log Only**

STEP B Define the default rule:

- **Allow unclassified or unknown senders** (the default)
- **Block unclassified or unknown senders**

STEP 4 When you finish, click **Apply**.

Tuning the Anti-Spam Service

3Com recommends leaving the Anti-Spam Service settings at their default values; however, you can adjust the spam filter, either to reduce the amount of unfiltered spam or to reduce the amount of legitimate email (if any) filtered out.

STEP 1 From the navigation pane, select **Firewall > Anti-Spam**.

The Anti-Spam page opens.

STEP 2 Ensure that **Enable Anti-Spam IP-Reputation Service** is checked.

STEP 3 In the **Block if risk exceeds** field, type a percentage between 0 and 100. Email from senders with a risk threshold greater than this value is blocked. The default is 89%.

STEP 4 Click on **Switch to Advanced Settings**.

Additional options appear.

STEP 5 In the Threshold Settings section, define the following:

- STEP A** Select a Priority to specify the action taken if the risk and class response from the service conflict: **Use risk threshold only** (the default), **Use class thresholds only**, **Permitted by either class or risk thresholds**, or **Blocked by either class or risk thresholds**.
- STEP B** Class: Type a **High Volume** value from 0 to 9 (the default is 8); increasing this value accepts email from larger-volume senders. Type a **Transient** value from 0 to 5 (the default is 4); increasing this value accepts email from senders identified by the service for a longer time as spam sources. Select a **White list** action (Permit or Block); selecting Permit accepts email from senders listed by the service as non-spam sources. Select a **Black list** action (Block or Permit); selecting Block rejects email from senders listed by the service as spam sources. Select a **Private** action (Permit or Block) for email received from a private range of IP addresses.
- STEP 6** In the Cache Settings section, define the following:
- STEP A** Type the **Number of records**, from 1000 to 1000000 (the default is 100000). The cache records known spam addresses and the number of hits from each.
- STEP B** Type the **Record lifetime** in minutes, from 0 to 1440 (the default is 60 minutes).
- STEP 7** When you finish, click **Apply**.

Defining manual anti-spam settings

Manual anti-spam settings let you define a white list (a list of IP addresses from which email is always permitted) or black list (a list of IP addresses from which email is always blocked). A manual entry always takes precedence over the results from the service. If a sender (IP address) appears on both the manual white list and manual black list, the connection is permitted.

- STEP 1** From the navigation pane, select **Firewall > Anti-Spam**.
- The Anti-Spam page opens.
- STEP 2** To enable manual filtering, check **Enable manual Anti-Spam filtering**.
- STEP 3** To create a white list, select one of the following in the **Permit** section:
- **No IP Addresses** — List is empty (the default)
 - **IP Address Group**— select an existing group
 - **IP Subnet**— type a subnet and a mask
 - **IP Range**— type a starting and ending IP address
 - **IP Host**— type a single IP address
- STEP 4** To create a black list, select one of the following in the **Block** section:
- **No IP Addresses** — List is empty (the default)
 - **IP Address Group**— select an existing group
 - **IP Subnet**— type a subnet and a mask
 - **IP Range**— type a starting and ending IP address
 - **IP Host**— type a single IP address
- STEP 5** When you finish, click **Apply**.

Testing an IP Address

You can use the IP Address Test page to determine if an IP address is covered by either the Anti-Spam Service or the manual spam filter.

Checking an IP address

- STEP 1** From the navigation pane, select **Firewall > Anti-Spam**.
The **Anti-Spam** page opens.
- STEP 2** Select the IP Address Test tab.
The IP Address Test page opens.
- STEP 3** Type the IP address you want to check into the **Test IP** field and click **Test** to display the result.

5

Events: Logs, Traffic Streams, and Reports

The Events section describes the logs, views, and reports available to monitor system performance and traffic-related events triggered by firewall rules, Web content filters, IPS filters, and traffic threshold policies. In this section, you will review the information presented in the Events pages and learn how to manage the logs and reports. Only users with Super-user access may view all of the logs and reports available.

Overview

The Events menu pages let you monitor system performance and review traffic-related events. The menu provides the following options:

- **Logs** — View information on system events and traffic-related events triggered by firewall, IPS, and traffic threshold security policies.
- **Managed Streams** — Review and manage traffic streams that have been blocked, rate-limited, or quarantined by IPS policies. You can also manually quarantine or release a quarantined IP address.
- **Health** — Review the current status and network performance of the X family device. Information includes memory and disk usage statistics, status of the Threat Suppression Engine and Ethernet ports, and throughput performance.
- **Reports** — View graphs showing information on traffic flow, traffic-related events, and statistics on firewall top sites, top services, top clients, rule hit counts, and triggered filters (attack, rate limit, traffic threshold, quarantine, and adaptive filter).

For details, see the following sections:

- [“Logs” on page 100](#)
- [“Managed Streams” on page 111](#)
- [“Health” on page 117](#)
- [“Reports” on page 122](#)

Logs

The Logs menu pages provide information on system events and traffic-related events triggered by firewall, IPS, and traffic threshold security policies. Each menu page also provides functions to manage the log files.

When you review logs, you may also see the following type of administrator user levels. These users denote the type of account according to the interface they used in the device:

- **SMS** — Indicates the administrator used the SMS when saving messages to the logs
- **LSM** — Indicates the administrator used the LSM when saving messages to the logs
- **CLI** — Indicates the administrator used the CLI when saving messages to the logs



Note Users with any access level can view and print the system log, but only Administrator and Super-user level users can reset this log.

The X family device maintains two files for each log, a historical log file and a current log file. When the current log file reaches the default size (4 MB), the log is deactivated and saved as the historical file, and a new log file is started as the current log. If a historical file already exists, that file is deleted. When the log is rolled over, the device generates a message in the Audit log. To save log all data and create a backup, configure the device to offload log messages to a remote system log.

You can reset a log from its menu page, or use the Reset  function available on the System Summary page.

For details, see the following sections:

- [“Alert Log” on page 100](#)
- [“Audit Log” on page 101](#)
- [“IPS Block Log” on page 102](#)
- [“Firewall Block Log” on page 103](#)
- [“Firewall Session Log” on page 104](#)
- [“VPN Log” on page 105](#)
- [“System Log” on page 106](#)
- [“Configuring Remote System Logs” on page 107](#)
- [“Managing Logs” on page 108](#)

Alert Log

The Alert log contains information about network traffic that triggers IPS filters configured with a Permit + Notify or Permit+Notify+Trace action set. Any user can view the log, but only administrator and super-user level users can print the log.

To maintain a complete history of entries and provide a backup, you can configure the device to send Alert Log entries to a remote syslog server from the Notification Contacts page. For details, see [“Notification Contacts” on page 49](#).

An Alert log entry contains the following fields:

Table 5-1: Alert Log Field Descriptions

Column	Description
Log ID	A system-assigned ID number.
Date/Time	A date and time stamp in the format <i>yyyy-mm-dd hh:mm:ss</i> .
Severity	Indicates the severity of the triggered filter. Possible values include: Critical, Major, Minor, and Low.
Filter Name	The name of the IPS filter that was triggered.
Protocol	The name of the protocol that the action affects.
Security Zone (pair)	The security zone pair where the alert occurred (for example, LAN -WAN).
Source Address	The source address of the triggering traffic.
Dest Address	The destination address of the triggering traffic.
Packet Trace	Details if a packet trace is available.
Hit Count	Details how many packets have been detected.

Audit Log

The audit log tracks user activity that may have security implications, including user attempts (successful and unsuccessful) to do the following:

- Change user information
- Change IPS, firewall, routing, high availability, or network configuration
- Gain access to controlled areas (including the audit log)
- Update system software and attack protection filter packages
- Change filter settings



Note Only users with Super-user access level can view, print, reset, and download the audit log.

To maintain a complete history of entries and provide a backup, you can configure the device to send Audit Block Log entries to a remote syslog server from the Syslog Servers page. For details, see the [“Syslog Servers” on page 267](#).

An Audit log entry contains the following fields:

Table 5-2: Audit Log Field Descriptions

Column	Description
Log ID	A system-assigned Log ID number.
Date and Time	A date and time stamp in the format <i>yyyy-mm-dd hh:mm:ss</i> .
Username	The login name of the user performing the action. The user listed for an event may include SMS, SYS, HA, and CLI. These entries are automatically generated when one of these applications performs an action.
Access Level	The access-level of the user performing the action.
IP Address	The IP address from which the user connected to perform the action.
Interface	The interface with which the user logged in (either WEB for the LSM or CLI for the Command Line Interface).
Component	The area in which the user perform an action (LOGIN, LOGOUT, and Launch Bar Tabs).
Result	The action performed or the result of a LOGIN or LOGOUT attempt.
Action	The action performed as a result (for example, Log Files Reset).

IPS Block Log

The IPS Block log contains information about packets that have triggered an IPS filter configured with a Block + Notify action set.

To maintain a complete history of entries and provide a backup, you can configure the device to send IPS Block Log entries to a remote syslog server from the Notification Contacts page. For details, see [“Notification Contacts” on page 49](#).

An IPS Block log entry contains the following fields:

Table 5-3: IPS Block Log Field Descriptions

Column	Description
Log ID	A system-assigned ID number.
Date/Time	A date and time stamp in the format <i>yyyy-mm-dd hh:mm:ss</i> .
Severity	Indicates the severity of the triggered filter. Possible values include: Low = 1 Minor = 2 Major=3 Critical=4 Note When the log is downloaded, the Severity value is reported using the numerical value.

Table 5-3: IPS Block Log Field Descriptions (Continued)

Column	Description
Filter Name	The name of the filter that was triggered.
Protocol	The name of the protocol that the action affects.
Security Zone (pair)	The security zone pair where the alert occurred (for example, LAN to WAN).
Source Address	The source address of the triggering traffic.
Dest Address	The destination address of the triggering traffic.
Packet Trace	Details if a packet trace is available.
Hit Count	Details how many packets have been detected.

Firewall Block Log

The Firewall Block Log captures information about events that have triggered a firewall rule that blocks matching traffic and has logging enabled.

A log entry is generated for each of the following events:

- Block Web request event — occurs when the device blocks a Web request due to Web content filtering
- Block event — occurs when a firewall rule with Block action is triggered

To maintain a complete history of entries and provide a backup, you can configure the device to send Firewall Block Log entries to a remote syslog server from the Notification Contacts page. For details, see [“Notification Contacts” on page 49](#).

Each log entry is tab-delimited. The log fields are populated based on the type of event being logged. If a field is not used, a tab is inserted to properly position the data in the next field.

A Firewall Block log entry contains the following fields:

Table 5-4: Firewall Block Field Descriptions

Column	Description
Log ID	A system-assigned ID number.
Date/Time	A date and time stamp in the format <i>yyyy-mm-dd hh:mm:ss</i> .
Severity	Indicates the severity of the triggered filter. Possible values include: Critical, Major, Minor, and Low.
Firewall Rule	The name of the firewall rule that was triggered. In the LSM, the firewall rule is linked to let you edit/view the rule that triggered the event.
Protocol	The name of the protocol that the action affects.
Source Zone	The security zone where the traffic originated.

Table 5–4: Firewall Block Field Descriptions (Continued)

Column	Description
Dst Zone	The security zone where traffic was sent.
SourceIP: Port Dest	The source address and port where the triggering traffic originates.
Dest IP: Port	The destination address and port of the triggering traffic.
Category	For Web requests blocked by the Web Content Filtering Service, this represents the filter category triggered by the URL (examples: Gambling, Entertainment, or Violence).
URL	For Web requests events only, the target URL. This field is populated regardless of whether the request was filtered by the Web Content Filtering Service.

Firewall Session Log

For firewall and Web content filter Permit rules with logging enabled, this log captures information on session creation and termination, including the time the session started and the URL being accessed (for Web requests). When a session terminates the Firewall Session Log shows how many bytes were transferred through the session.

A log entry is generated for each of the following events if the firewall rule had logging enabled:

- Web Request event — device permits a Web request to pass through
- Session Started event — firewall rule is triggered
- Session Close event — network connection is ended or closed due to inactivity

To maintain a complete history of entries and provide a backup, you can configure the device to send Firewall Session Log entries to a syslog server from the Syslog Servers page. For details, see [“Syslog Servers” on page 267](#).

Each log entry is tab delimited. The log fields are populated based on the type of event being logged. If a field is not used, a tab is inserted to properly position the data in the next field.

A Firewall Session log entry contains the following fields:

Table 5–5: Firewall Session Log Field Descriptions

Column	Description
Log ID	A system-assigned ID number.
Date/Time	A date and time stamp in the format <i>yyyy-mm-dd hh:mm:ss</i> .
Rule	The ID of the firewall rule triggered.
Protocol	The name of the protocol associated with the session in the format $x(y)$, where x =protocol name and y =protocol number.
Src Zone	Name of the source security zone for the firewall rule.

Table 5–5: Firewall Session Log Field Descriptions (Continued)

Column	Description
Dst Zone	Name of the destination security zone for the firewall rule.
SourceIP: Port	The source IP address and port from which the session was started.
DestIP: Port	The destination IP address and port that is the target of the session.
Category	For Web requests filtered by the Web Content Filtering Service, this represents the filter category triggered by the URL (examples: Gambling, Entertainment, or Violence).
URL	For Web requests blocked by a Web conter filter firewall rule with logging enabled, this field specifies the target URL. This field is populated regardless of whether the request was filtered by the Web Content Filtering Service.
Session Duration(s)	For Session End events only, this field contains the duration of the session based on the session start time. The duration is displayed in the format <i>DD:HH:MM:SS</i> .
Bytes	For Session End events, this field contains the number of bytes transferred during each session. For web request events, this field indicates the number of bytes downloaded from the HTTP GET.
Message	Message text associated with the firewall session event: Web request — no message Session start — Regular session start, Secondary session start Session end — Session ended because of inactivity, Session ended because of inactivity

VPN Log

The VPN log captures diagnostic messages relating to VPN tunnels to help troubleshoot and monitor VPN configurations. Each log entry is tab-delimited. The log fields are populated based on the type of event being logged. If a field is not used, a tab is inserted to properly position the data in the next field.

To maintain a complete history of entries and provide a backup, you can configure the device to send VPN Log entries to a syslog server from the Syslog Servers page. For details, see [“Syslog Servers” on page 267](#).

A VPN log entry contains the following fields:

Table 5–6: VPN Log Field Descriptions

Column	Description
Log ID	A system-assigned ID number.
Log Entry Time	A date and time stamp in the format <i>yyyy-mm-dd hh:mm:ss</i> .
Severity	The severity of the event, which is INFO.

Table 5–6: VPN Log Field Descriptions (Continued)

Column	Description
Src IP:Port	Source address — the IP address and port for the event. This is a string and the value may be <i>this-device</i> , indicating that the device sent the message itself.
Dest IP:Port	Destination IP address and port for the event.
Message	Free-form text with error messages or notification about a VPN tunnel.

Configuration

The logging level for the VPN log can be configured to provide more detailed or less detailed information by configuring the **Enable Verbose** messages in the VPN Log option, available on the IPSec Configuration page.

System Log

The System Log contains information about the software processes that control the X family device, including startup routines, run levels, and maintenance routines. System log entries can provide useful troubleshooting information if you encounter problems with the device.

To maintain a complete history of entries and provide a backup, you can configure the device to send System Log entries to a syslog server from the Syslog Servers page. For details, see [“Syslog Servers” on page 267](#).



Note Users with any access level can view and print the system log, but only Administrator and Super-user level users can reset this log.

For information on Adaptive Filter messages, see [“Adaptive Filter Configuration” on page 56](#).

System Log entries are only sent to the syslog server after the device has fully booted. During the boot sequence, entries cannot be sent because network ports are not yet enabled. When the boot sequence completes, the device sends a startup message to the syslog server.

A System log entry contains the following fields:

Table 5–7: System Log Field Descriptions

Column	Description
Log ID	A system-assigned ID number.
Log Entry Time	A date and time stamp in the format <i>yyyy-mm-dd hh:mm:ss</i> .
Severity Level	The severity level of a message indicates whether the log entry is simply informational (INFO) or whether it indicates an error condition (ERR or CRIT).
Component	An abbreviation indicating which software component sent the message to the log.
Message	The text of the log entry.

Configuring Remote System Logs

All information logged by the LSM can be offloaded to a remote syslog server. Options to configure logging behavior for traffic-related events are available from the Edit Action Sets page (**IPS > Action Sets > Edit**) and the Edit Firewall Rule page. To use remote logging options, you must configure the contact information for the remote syslog servers.

For details on configuring the Remote System Log contact for the Alert, IPS Block, and Firewall Block log messages, see [“Configuring the remote system log contact” on page 50](#).

For details on configuring the Syslog Server contact for the System, Audit, VPN, and Firewall Session log, see [“Configuring remote syslog for the System, Audit, VPN, and Firewall Session logs” on page 107](#).



CAUTION Remote syslog, in adherence to RFC 3164, sends clear-text log messages using the UDP protocol with no additional security protections. Therefore, you should only use remote syslog on a secure, trusted network to prevent syslog messages from being intercepted, altered, or spoofed by a third party.

Configuring remote syslog for the System, Audit, VPN, and Firewall Session logs

STEP 1 From the navigation pane, select **System > Configuration > Syslog Servers**.




The Syslog Servers page opens.

STEP 2 For each log type you want to offload, click the check box and specify the IP address for the syslog server.

Managing Logs

On each log page, the functions available for the log are displayed at the top of the page. You can also access the log functions from the System Summary page. The following table describes these functions:

Table 5–8: Log Functions

Function	Icon/Field	Description
View		<p>To view a log from the LSM, select Events > Logs. Then, click the name of the desired log.</p> <p>To customize the display, specify the desired value in the Records per page field.</p> <p>To page through log entries, use the Navigation functions in the upper and lower left corners:</p> <p><< Go to first page < Go to previous page > Go to next page >> Go to last page</p>
Download		<p>Click the Download icon to download an electronic copy of the log or report. When you click the icon, the Download Log page displays to specify filter criteria for the log entries to be included in the downloaded log.</p> <p>When you download some logs, the downloaded log file contains additional information that is not displayed in the LSM interface. See Chapter B, “Log Formats” for details.</p>
Search		<p>Click the Search icon to search for an entry in the log or report. The Logs page displays a search page according to the selected log or report.</p>
Reset		<p>Use the Reset icon to clear a log of all current entries. The log will then begin compiling new information.</p>

For additional details, see the following topics:

- [“Viewing Logs” on page 109](#)
- [“Downloading a Log” on page 109](#)
- [“Resetting a Log” on page 110](#)
- [“Searching a Log” on page 110](#)

Viewing Logs

Logs can be viewed from the Events menu.

Viewing a log file

- STEP 1** From the LSM **Events** menu, click the name of the log you want to view.
- STEP 2** Click the desired log. The LSM updates to display the log page for the selected item.
- For details on managing the logs from the log page, see [“Managing Logs” on page 108](#).

Downloading a Log

To save log data, use the download function.

In the LSM, the log view displays both current and historical log entries. When you download a log file, you have the option to download all the entries, or only the entries in the current log file.

The download function provides the following options:

- Download the entire log, or selected entries based on the following user-specified filter criteria:
 - **All** — Downloads all entries in the current and historical log files
 - **Current** — Downloads only the entries in the current log file
 - **Time Range** — Specifies the dates and times (optional) for compiling entries
 - **ID Range** — Range of ID numbers for logged entries
- View the log in a Web browser
- Export the downloaded information to a comma-separated values (CSV) text file.



Note Downloaded logs provided more detailed information on each event than what is displayed in the LSM interface. See [Chapter B, “Log Formats”](#) for more information.

In the downloaded log, file entries are in a tab-delimited format with a line feed character terminating each line. Use WordPad or a spreadsheet application to view downloaded log files on a Windows workstation.

Downloading a log

- STEP 1** On the log page in the **Log Functions** section, click the Download icon.



Note If the log is empty, the download link will be disabled or grayed out.

- STEP 2** Verify that the **Log Type** dropdown list box has the correct log selected.

- STEP 3** In the **Log Entry** section, specify one of the following criteria for the log entries to be included in the downloaded file:
- Select **All** to download all entries.
 - Select **Current** to download all current entries.
 - Enter a **Time Range**, including the date (required) in *yyyy-mm-dd* format and time (optional) in *hh:mm:ss* format.
 - Enter an **ID Range** for entries in the **From** and **To** fields.
- STEP 4** In the **Options** section, select one or both boxes for file format options: **Comma delimited format (csv)** or **Open in Internet Explorer**.
- STEP 5** Click **Download**.

Resetting a Log

When you reset a log, the LSM starts a new log file beginning with the current date and time based on the system time. All previous information is permanently deleted. For record keeping, you may want to download the log before performing a reset. (For details, see [“Downloading a Log” on page 109](#)).

Resetting a log

- STEP 1** On a the log page in the Log Functions section, click **Reset**.
- STEP 2** A confirmation message displays, prompting if you want to reset the log.
- STEP 3** Click **OK**.

Searching a Log

Some logs provide a search function to help locate specific entries. This feature is available on the Alert, Audit, IPS Block Log, Firewall Block Log. To locate an entry within a log file, use the Search function available on each log page. You can search for entries by specifying one or more of the following criteria:

- **Date Range** — Search all log entries or specify a date range. You can also enter a time range.
- **Severity** — The severity includes low, minor, major, and critical events. You can select any severity you want to search.
- **Filter Name** — You can search for logged entries based on the filter that triggered them.
- **Protocol** — You can search by name of the protocol that the action affects.
- **Source Address** — You can search for a source address of the triggering traffic.
- **Destination Address** — You can search for a destination address of the triggering traffic.

Searching a log

- STEP 1** Open the log view. Then, in the Log Functions section, click [Search](#).
- The Search System Log page opens.

- STEP 2** Specify the search criteria. For the **Log Entry Time**, choose one of the following search options:
- Choose **All** to search all log entries.
 - Enter a date range for log entries. You can enter a date and time for the range, using the format *yyyy-mm-dd* (required) and *hh:mm:ss* (optional).
- STEP 3** Check the box next to each **Severity** of the alerts you wish to retrieve (optional).
- STEP 4** Enter the name of the **Filter Name** whose alerts you would like to find (optional).
- STEP 5** Enter the name of the **Protocol** whose alerts you would like to find (optional).
- STEP 6** Enter the **Source Address** for alerts you would like to find (optional).
- STEP 7** Enter the **Destination Address** for the alerts you would like to find (optional).
- STEP 8** Choose the **# of Results to Display** from the drop-down box (optional).
- STEP 9** Click **Search**.



TIP In Step 4 through Step 7, you can enter the first part of the item you want to search for. For example, you can enter the first few letters or numbers in a filter name, or the first few numbers of an IP address.

Managed Streams

The Managed Streams menu pages provide options to review and manage traffic streams that have been blocked, rate-limited, or quarantined by IPS policies. These events are captured by the Threat Suppression Engine, which uses a blend of ASICs and network processors to detect threats and anomalies in network traffic.

The traffic streams include the following:

- **Blocked streams**— Traffic streams detected and blocked based on filters configured with a Block action set.
- **Rate-Limited streams** — Traffic streams detected and rate limited based on filters configured with a Rate-Limit action set.
- **Quarantined streams** — Traffic streams detected and blocked based on filters configured with a Quarantine action set, or quarantined manually.

For details, see the following topics:

- [“Action Sets” on page 42](#)
- [“Blocked Streams Page” on page 112](#)
- [“Rate Limited Streams Page” on page 114](#)
- [“Quarantined Addresses Page” on page 115](#)

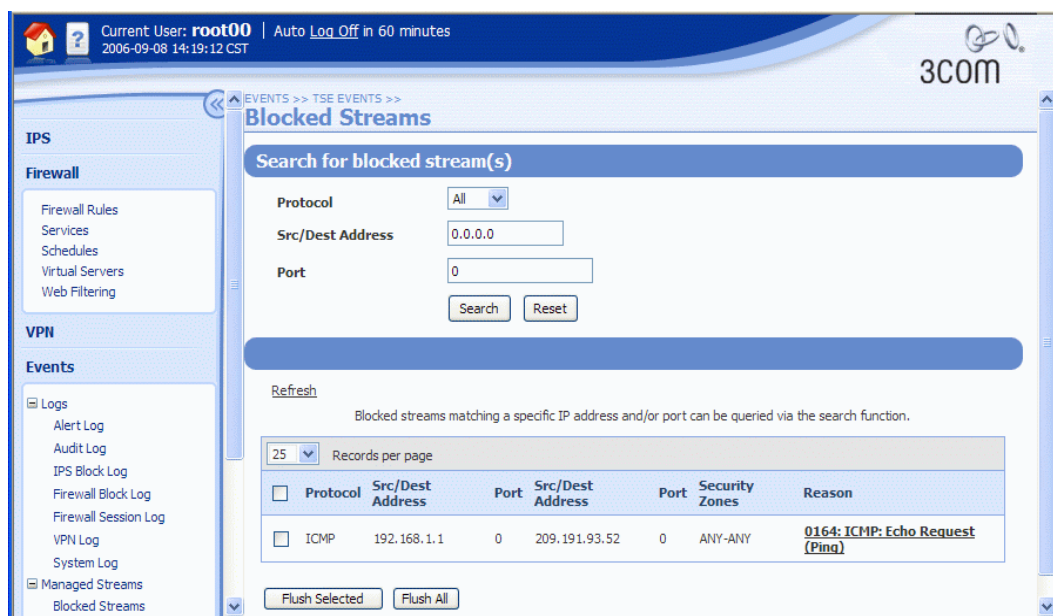
Blocked Streams Page

When traffic triggers an IPS filter that has been configured with a Block or Block+Notify action, traffic from the source IP address and port is blocked and an entry is added to the Blocked Streams page, based on the contact configuration in the action set. From the Blocked Streams page, you can:

- View and search for information on blocked streams
- Manually terminate all or selected blocked stream connections

The following figure shows the Blocked Streams page:

Figure 5–1: Blocked Streams Page



The Blocked Log Entries table displays up to 50 entries. Entries are added when the block event occurs. Entries are automatically removed when the connection times out based on the **Connection Table timeout** setting configured from the IPS Preferences page. The default timeout settings is 1800 seconds (30 minutes). You can manually remove an entry by terminating the connection using the **Flush** functions.

For each blocked traffic stream, the Blocked Streams page provides the following information:

Table 5–9: Blocked Streams Table

Field	Description
Protocol	Protocol used by the blocked connection.
Src/Dest Address	Source or destination IP address of the connection.
Port	Port of the connection.
Src/Dest Address	Source or destination IP address of the connection.
Port	Port of the connection.
Security Zones	The security zones where traffic was blocked or rate-limited.

Table 5–9: Blocked Streams Table (Continued)

Field	Description
Reason	The filter link that details why the traffic connection stream was blocked. Click the link to display and manage the filter.

Searching for blocked streams

STEP 1 From the navigation pane, select **Events > Managed Streams > Blocked Streams**.

The Blocked Streams page opens.

STEP 2 Enter search criteria for any of the following:

- Protocol — The protocol for the connection: All, TCP, UDP, ICMP
- Source or Destination Address — The traffic source or destination IP address
- Source or Destination Port — The traffic source or destination IP port

Entering “0” or “0.0.0.0” in the fields you do not want to specify lets you search on any of the four fields (combination or single). This value acts as the value “any.”

STEP 3 Click **Search**.

To reset the search, click **Reset**.

Flushing blocked streams

You can manually drop the connection for all or selected streams using the Flush functions available on the Blocked Streams page. A connection is automatically dropped when the connection table timeout period expires.

STEP 1 From the navigation pane, select **Events > Managed Streams > Blocked Streams**.

The Blocked Streams page opens.

STEP 2 To drop all the connections, scroll to the bottom of the page and click **Flush All**.

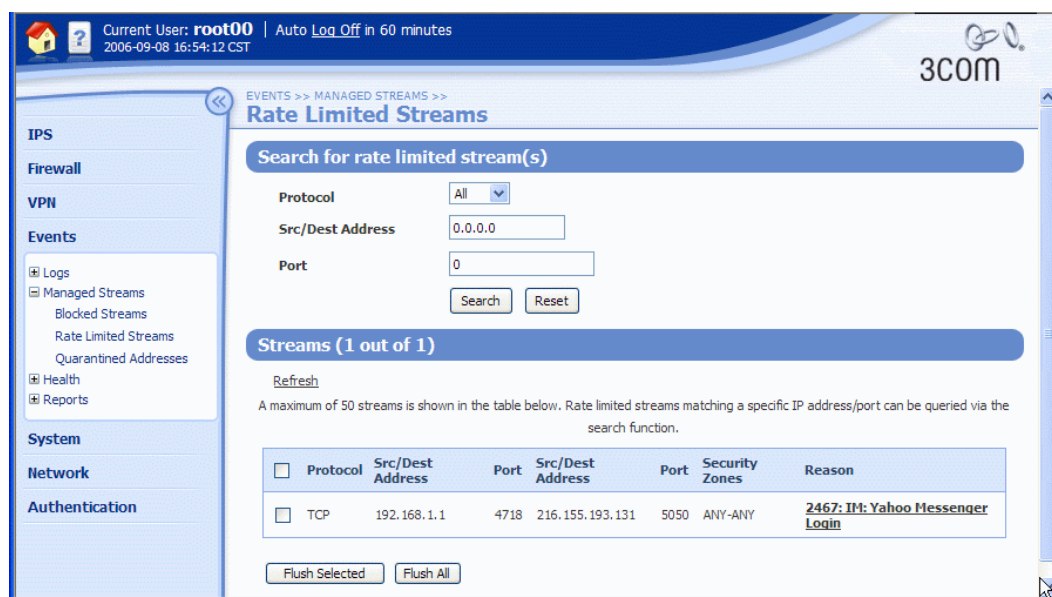
To drop selected connections, use the check box next to an entry to select it. Then, scroll to the bottom of the page and click **Flush**.

Rate Limited Streams Page

When traffic triggers an IPS filter configured with a Rate Limit action set, traffic from the source IP and port is limited based on the rate limit settings in the action set. Traffic from the source IP address and port to the destination IP address and port remains rate limited until the connection timeout period expires or the connection is manually terminated from the LSM.

The following figure shows the Rate Limited Streams page:

Figure 5–2: Rate Limited Streams Page



From the Rate Limited Streams page, you can:

- View and search for information on rate-limited streams
- Manually terminate all or selected rate-limited stream connections

The Rate Limited Streams table displays up to 50 entries. Entries are added when the rate-limit event occurs. Entries are automatically removed when the connection times out based on the **Connection Table timeout** setting configured from the IPS Preferences page (**IPS > IPS Preferences**). The default timeout setting is 1800 seconds (30 minutes). You can manually remove an entry by terminating the connection using the **Flush** functions.

For each rate-limited stream, the **Rate Limited Streams** table provides the following information:

Table 5–10: Rate Limited Streams Table

Column	Definition
Protocol	Protocol used by the blocked connection.
Src/Dest Address	Source or destination IP address of the connection.
Port	Port of the connection.
Src/Dest Address	Source or destination IP address of the connection.
Port	Port of the connection.

Table 5–10: Rate Limited Streams Table (Continued)

Column	Definition
Security Zone (pair)	The security zone pair where the stream is rate limited (for example, LAN -WAN).
Reason	The filter link that details why the traffic connection stream was blocked. Click the link to display and manage the filter.

Searching for rate-limited streams

STEP 1 From the navigation pane, select **Events > Managed Streams > Rate Limited Streams**.

The Rate Limited Streams page opens.

STEP 2 Enter search criteria for any of the following:

- Protocol — The protocol for the connection: All, TCP, UDP, ICMP
- Source or Destination Address — The traffic source or destination IP address
- Source or Destination Port — The traffic source or destination IP port

Entering “0” or “0.0.0.0” in the fields you do not want to specify lets you search on any of the four fields (combination or single).

STEP 3 Click **Search**.

To reset the search, click **Reset**.

Flushing rate-limited streams

You can manually drop the connection for all or selected streams using the Flush functions available on the Rate Limited Streams page. A connection is automatically dropped when the connection table timeout period expires.

STEP 1 From the navigation pane, select **Events > Managed Streams > Rate Limited Streams**.

The Rate Limited Streams page opens.

STEP 2 To drop all the connections, scroll to the bottom of the page and click **Flush All**.

To drop selected connections, use the check box next to an entry to select it. Then, scroll to the bottom of the page and click **Flush**.

Quarantined Addresses Page

When traffic triggers an IPS filter configured with a Quarantine action set, the IP address of the host is quarantined. The host remains in quarantine with limited or no network access based on the settings configured in the quarantine action set, or until the address is manually removed from quarantine via the Quarantined Addresses page in the LSM, or until the global quarantine timeout (**IPS > Preferences**) expires.

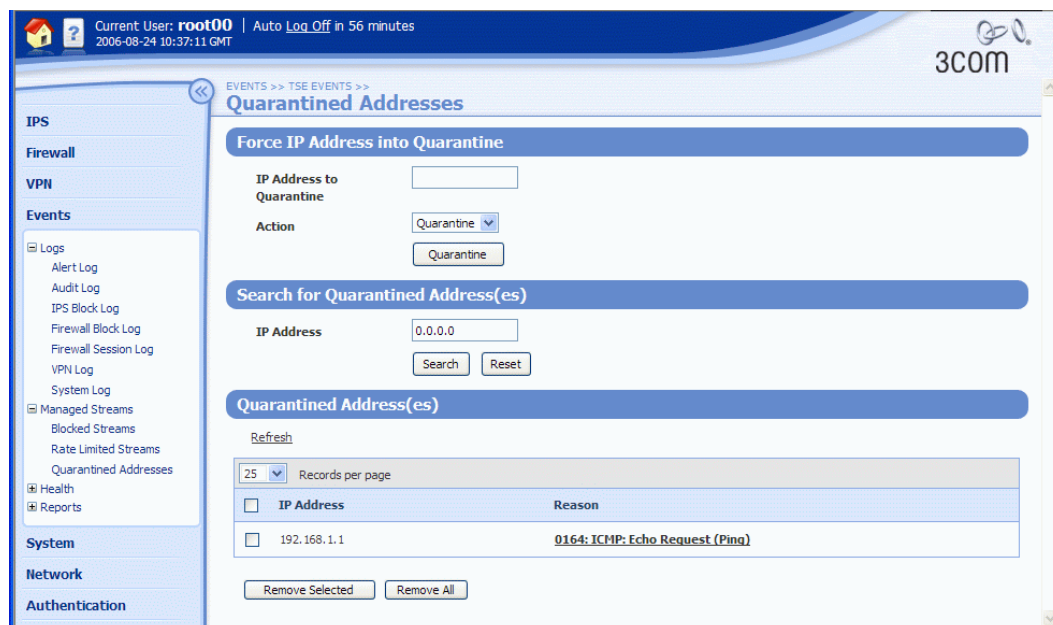
Entries are added to the Quarantined Addresses page when the quarantine event occurs. Entries are automatically removed when the address is removed from quarantine either automatically based on the quarantine threshold settings for the action set, manually using the **Remove** function, or when the quarantine timeout expires.

From the Quarantined Addresses page, you can perform the following tasks:

- Viewing and searching for information on quarantined addresses
- Forcing an address into quarantine
- Removing all or selected addresses from quarantine

The following figure shows the Quarantine Addresses page:

Figure 5–3: Quarantined Addresses Page



For each quarantined address, the Quarantined Addresses page provides the following information:

Table 5–11: Quarantined Address Table

Column	Description
IP address	The IP address of the host in quarantine.
Reason	Identifies the IPS filter that triggered the quarantine. Click the filter link to display and manage the filter.

Searching for quarantined addresses

STEP 1 From the navigation pane, select **Events > Managed Streams > Quarantined Addresses**.

The Quarantined Addresses page opens.

STEP 2 Enter a valid IP address for the quarantined host.

To view all quarantined addresses, the IP Address field must contain the value 0.0.0.0. This value is equivalent to the value *any*.

STEP 3 Click **Search**.

The Quarantined Addresses table updates with addresses matching the search criteria.

To reset the search field and update the Quarantined Addresses table to display all entries, click **Reset**.

Forcing IP address into quarantine

To manually quarantine a host, you must first configure a Quarantine action set which determines the behavior when the host attempts to access the network. As soon as you force the quarantine, the host immediately has limited or no network access based on the Quarantine action set configuration. For example, if the action set is configured to display a quarantine page, any requests from the host are redirected to the specified page.

STEP 1 From the navigation pane, select **Events > Managed Streams > Quarantined Addresses**.

The Quarantined Addresses page opens.

STEP 2 Click **Quarantine**.

The Quarantined Addresses table updates to display the IP address of the quarantined host. Use the **Remove** function to manually remove the host from quarantine.

Removing IP addresses from quarantine

You can manually remove all or selected IP addresses using the Remove functions available on the Quarantined Addresses page. An address may be automatically removed based on the quarantine threshold configuration for the Quarantine action set.

STEP 1 From the navigation pane, select **Events > Managed Streams > Quarantined Addresses**.

The Quarantined Addresses page opens.

STEP 2 To remove all connections from quarantine, scroll to the bottom of the page. Then, click **Remove All**.

To remove selected addresses, use the check box next to an entry to select it. Then, scroll to the bottom of the page and click **Remove**.

Health

The Health menu pages show the current status and network performance of the X family device. From the Health menu you can review:

- Device health indicated by memory and disk usage statistics
- Module health, including the Threat Suppression Engine and Ethernet ports
- Performance/Throughput

To access the Monitor page, select **Events > Health > Monitor**, or click **Health** on the System Summary page.

For details on each type of Health information, see the following:

- [“Device Health” on page 118](#)
- [“Module Health” on page 119](#)
- [“Performance/Throughput” on page 121](#)
- [“Port Health” on page 121](#)

Device Health

The Device Health section of the Monitor page displays the current status of a variety of chassis components, including power modules, fans, temperature, and memory and disk space usage.

Table 5-12: Device Health

Column	Description
Component	The component or resource being monitored. These components include the following: <ul style="list-style-type: none"> • Memory — the amount of memory used • Disk/000 — the amount of disk space available
State	The current operating status of the component or resource being monitored. The state can be one of the following: <ul style="list-style-type: none"> • Normal — usage is at normal levels • Major — usage has reached the major threshold setting specified for the device • Critical — usage has reach the critical threshold setting specified for the device To set the thresholds that trigger the Major and Critical states for memory and disk usage, select System > Configuration > Thresholds .
Graph	A representation of the current usage level of the component or resource being monitored.
Details	The units being measured in the graph. For example, for the memory component, this field index the percentage of total memory being used.

Memory and Disk Usage

The Memory Usage statistic displays usage averaged over the last refresh period. These values fluctuate fairly frequently. If Memory Usage percentages seem consistently high, check your log for Memory Fault messages.



Note If device health is consistently showing yellow or red warnings about Disk or Memory Usage, but the log does not show any hardware fault messages, your usage is spiking, but is not remaining consistently high.

If Memory Usage percentages are consistently high, you may need to adjust some IPS filter or Firewall Rule settings. Filters that require notification actions require more resources than filters that do not

require notification, but this difference only comes into play when network traffic matches or nearly matches these filters. Firewall rules with logging enabled also consume more memory.



TIP To reduce memory and disk usage, make the following filter adjustments:

- Reduce the number of IPS filters that use alerts.
- Reduce usage of packet trace and email notification on action sets.
- Increase aggregation periods for action sets that include alerts.
- Use more global filters and fewer filter overrides.
- Deactivate filters that do not apply to your network (for example: IIS filters are not relevant if you only have Apache servers).
- Reset logs from the System Summary page or use the CLI `clear log` command. The clear log command will clear all log entries from all log files. For record keeping, you may want to download existing log files before resetting a log, or configure a remote syslog server to offload the logs.
- Delete previously installed TOS version images from the System Update page.
- Reduce the number of Firewall rules with logging enabled.
- Reduce the inactivity timeout on Firewall rules. This allows the firewall to discard inactive sessions more quickly.

Module Health

The Module Health section of the Monitor page displays the current status of the modules that are inside the chassis of the device. The following information is provided.

Table 5–13: Module Health

Column	Description
Module	<p>A brief description of the type of module. Possible values:</p> <ul style="list-style-type: none"> • Management Processor — The central processing and control system for the device. • Threat Suppression Engine — The TSE provides full threat detection and suppression. Receives data from the Ethernet ports, performs deep packet inspection on the data, and permits or blocks the data based on configuration of security profiles and traffic threshold policy. When you click the link, it displays the IPS Preferences page. See “Configuring the Threat Suppression Engine” on page 55. • Ethernet Ports— The Ethernet ports on the device. When you click the link, it displays the Port Health page with detailed information on each port. See “Port Health” on page 121.
Configuration	<p>A description of the configuration of the module:</p> <ul style="list-style-type: none"> • Simplex — A communications channel that can carry a signal in one direction • Duplex — A communications channel that can carry signals in both directions

Table 5-13: Module Health (Continued)

Column	Description
Module State	A description of the current operation state of the module: <ul style="list-style-type: none"> • Active — The module is active without errors • Active with Faults — The module is active but has errors • Stand-by — The module is waiting for traffic or usage in a stand-by mode • Out-of-service — The module is not working or disabled • Diagnostic — The module is running a diagnostic
Qualifier-1	A description of any reasons for an other-than-active state of the module.
Qualifier-2	Additional description of any reasons for an other-than-active state of the module.
Port State	A description of the current port state. Possible values: <ul style="list-style-type: none"> • Active — The port is active normally without errors • Active with Faults — The port is active with errors • Not Initialized — The port is not out of service but the device has not initialized the hardware • Stand-by — The port is waiting for traffic or usage in a stand-by mode • Out-of-service — The port is not working or disabled due to errors • Diagnostic — The port is running a system check diagnostic applications or being repaired

Performance/Throughput

To view the current throughput performance of the device, select **Events > Monitor > Performance**. If the device is experiencing performance problems, the following information is provided.

Table 5-14: Performance/Throughput

Column	Description
Component	The component or resource being monitored. On this page, the component is device throughput performance.
State	The current operating status of the component or resource being monitored. The state can be one of the following: <ul style="list-style-type: none"> • Normal — The device is active without errors • Major — The device is active but has errors • Critical — The device is waiting for traffic or usage in a stand-by mode • Out-of-service — The device is not working or disabled • Diagnostic — The device is running a diagnostic
Graph	A representation of the current status of the component or resource being monitored.
Details	Percentage of throughput used.
System Performance Messages	This table provides information about current system performance. If the device is experiencing problems, the table displays messages indicating the cause of the problem along with suggested remedies.

Port Health

To view Port Health information for each Ethernet port on the device, select **Events > Health > Port**. The following information is provided:

Table 5-15: Port Health

Column	Description
Port	The number of the port on the device.
Speed	The speed of the port.
Duplex	Indicates if the port is set to full or half duplex.
State	A description of the current operation state of the module. Possible values: <ul style="list-style-type: none"> • Active — The module is active without errors • Active with Faults — The module is active but has errors • Stand-by — The module is waiting for traffic or usage in a stand-by mode • Out-of-service — The module is not working or disabled • Diagnostic — The module is running a diagnostic

Table 5-15: Port Health (Continued)

Column	Description
Qual-1	A description of any reasons for an other-than-active state of the module.
Qual-2	Additional description of any reasons for an other-than-active state of the module.
Media	The type of media of the port, such as copper or fiber.
Type	The type of the port, such as Ethernet.

Reports

The **Reports** menu provides access to detailed information about the LSM system alert and traffic activity. Data for each report is gathered in real time. You can use the **Refresh** option on each report page to get the most current report information.

The following Reports menu options are available:

- **Attacks** — Displays data on traffic that has been filtered by the device based on the IPS filter and firewall rule configuration in a security profile.
- **Rate Limits** — Displays a bar graph showing the percentage of rate limit bandwidth used for each action set configured with a rate limit.
- **Traffic** — Displays traffic flow data categorized by transmission type, protocol, frame size, and port.
- **Traffic Thresholds** — Displays a bar graph of traffic that has triggered a traffic threshold filter. The report graphs the amount of incoming traffic as a function of time.
- **Quarantine** — Displays a bar graph showing quarantine activity as a function of time.
- **Adaptive Filter Events** — Displays the global Adaptive Filter settings and a list of the ten most recent filters impacted by adaptive filtering. You can also edit the Adaptive Filter settings from this report page.
- **Firewall** — Displays a bar graph showing the hit counts for each firewall rule as a percentage of total traffic based on firewall sessions.

For additional information, see the following:

- [“Viewing a report” on page 123](#)
- [“Attack Reports” on page 123](#)
- [“Rate Limit Reports” on page 124](#)
- [“Traffic Reports” on page 124](#)
- [“Traffic Threshold Report” on page 124](#)
- [“Quarantine Report” on page 125](#)
- [“Configure Adaptive Filter Events Report Page” on page 125](#)
- [“Disabling Adaptive Filter settings for a filter” on page 126](#)
- [“Firewall Reports” on page 126](#)

Viewing a report

- STEP 1** From the Reports menu (**Events > Reports**), click the desired Report menu option.
- The selected Reports page opens.
- STEP 2** Click any available view options to update the report data.
- STEP 3** To update the report data, use the **Refresh** option. On some reports, an **Animate Charts** option is available to update the data in real time.

Attack Reports

The Attack Reports page lets you view data on traffic that has been filtered by the device based on the IPS filter and firewall rule configuration. Firewall rules display as filter IDs in the 7400 to 7410 range. For example, filter ID 7400 is the default DENY ANY ANY rule that is implicitly added to the end of the Firewall Rule table.

Traffic data is reported based on the view options you select:

- **Top Ten Filters** — Displays a bar graph of the top ten attack filters which includes a packet counter, and the percentage of total traffic affected by the filter.
- **Severity** — Displays the number of attacks categorized as Low, Minor, Major, and Critical. The graph also shows the percentage of total traffic for each severity level. The severity levels are assigned by the TippingPoint Digital Vaccine team and are included as part of the filter definition.
- **Action** — Displays the actions taken on filtered traffic: traffic can be dropped (Invalid), blocked, or permitted. The report includes the number of packets processed by each action and the percentage of total traffic the number represents.
- **Protocol** — Displays attack traffic categorized by protocol. The report includes the number of filtered packets for each protocol and the percentage of total traffic the number represents. Protocols include: ICMP, UDP, TCP, and IP-Other.
- **By Port: All** — Displays amount of all attack traffic reported by the security zone where the traffic was filtered; number of packets is reported as a percentage of total traffic.
- **By Port: Permit** — Displays amount of attack traffic permitted reported by security zone. Number of packets is reported as a percentage of total traffic.
- **By Port: Block** — Displays amount of attack traffic blocked reported by security zone. Number of packets is reported as a percentage of total traffic.

Updating report data

To update the traffic statistics in real time information, select the **Animate Charts** option. If this option is not selected, click the **Refresh Data** link to view the most current information.



Note Additional information on attack filter events is available in the LSM logs. For details, see [“Logs” on page 100](#).

Rate Limit Reports

In the LSM, you can configure a rate limit action set to define the maximum amount of bandwidth available for traffic matching IPS filters that have a rate limit action set assigned. If two or more IPS filters use the same rate limit action set, then all packets matching these filters share the bandwidth. For each rate limit action set, the Rate Limit Reports page lets you view the percentage of bandwidth consumed by rate-limited traffic graphed as a function of time.

Data is reported based on the view options you select in the Rate Limit Reports page:

- **Rate Limit Action Set Name** — The list of available rate limit action sets is provided at the top of the rate limit table. To view the percentage of rate-limited bandwidth used for an action set, click on the action set name to update the report.
- **Reporting time interval** — Select the time interval for the reporting period: **Last 24 hours**, **Last 60 Minutes**, or **Last 60 seconds**.



Note The Rate Limit report is only available if an action set has been configured with the Rate Limit action.

For additional information on rate limit action sets, see [“Action Sets” on page 42](#). For details on rate-limited traffic streams, see [“Rate Limited Streams Page” on page 114](#).

Traffic Reports

The traffic report provides profile data on the packets flowing through the device (permitted packets only).

Traffic data is reported based on the view option you select on the Traffic Reports page:

- **Transmission Types** — Graphs the number of packets transmitted for each of the following transmission categories: Unicast, Broadcast, MultiCast, MAC control, FCS Errors, and Align Errors.
- **Protocol** — Graphs the number of packets transmitted by ICMP, UDP, TCP, IP-other, ARP, and Ethernet-Other.
- **Frame size** — Traffic profile by framesize, by specified byte ranges.
- **By Port** — Traffic profile by port, includes all security zones/ports.

Updating report data

To update the traffic statistics with real-time information, select the **Animate Charts** option. If this option is not selected, click the **Refresh Data** link to view the most current information.

Traffic Threshold Report

Traffic threshold filters track statistical changes in network traffic patterns. You can specify the amount of traffic that triggers a Traffic Threshold filter from the Traffic Threshold Reports page. The units used in the report (packets/hour, bytes/minute, connections/second, and so forth) are determined by the units configured in the Traffic Threshold filter.



Note The Traffic Threshold report is only available if an IPS Traffic Threshold filter has been configured for the device.

Traffic data is reported based on the viewing options you select on the Traffic Threshold Reports page:

- **Traffic Threshold filter name** — In the dropdown list under the Traffic Thresholds table heading, select the filter name to generate the traffic data for that filter.
- **Reporting time interval** — Click the time interval for the reporting period: **Last 35 Days**, **Last 24 hours**, **Last 60 Minutes**, or **Last 60 seconds**.

For additional information, see [“Traffic Threshold Filters” on page 37](#).

Quarantine Report

You can configure a filter with a quarantine action set. When a host computer triggers the filter, the host is quarantined according to the settings configured in the action set. You can monitor quarantine activity from the Quarantine Reports page.

Quarantine data is reported based on the viewing options you select on the Quarantine Reports page:

- **Total Hosts** — Displays the total number of quarantined hosts as a function of time.
- **Packets Blocked** — Displays the total number of packets blocked as a function of time.
- **Src Pages** — Displays the number of LSM quarantine pages served to quarantined hosts as a function of time. The quarantine source pages are generated based on the configuration specified in the Quarantine action set.
- **Redirect Pages** — Displays the number of times hosts have been redirected as a result of a quarantine action as a function of time.
- **Reporting time interval** — Click the time interval for the reporting period: **Days** (last 35), **Hours** (last 24), **Minutes** (last 60), or **Seconds** (last 60).



Note More detailed information on quarantined hosts is available from the Quarantined Addresses page. For details, see [“Quarantined Addresses Page” on page 115](#).

Configure Adaptive Filter Events Report Page

From the Configure Adaptive Filter Events Report page, you can:

- Review and modify the global Adaptive Filter configuration
- View a list of the ten most recent filters managed by adaptive filtering
- Disable adaptive filter settings for an individual filter

The Configure Adaptive Filter Events report page provides the following information:

Table 5–16: TSE Adaptive Filter Configuration Details

Column	Definition
Settings	The Settings table lets you change the global system configuration for the Adaptive Filter function. For details, see “Adaptive Filter Configuration” on page 56 .
Ten Most Recent:	Table that displays the ten most recent filters managed by adaptive filtering.

Table 5–16: TSE Adaptive Filter Configuration Details

Column	Definition
Filter Name	The linked name of the filter being managed by the Adaptive Filter function. To disable Adaptive Filter Configuration for a filter, click the linked name. On the Edit Filter page, select Do not apply adaptive configuration settings to this filter. Then, click Apply to save the setting.
Filter State	Indicates the current state of the filter. <ul style="list-style-type: none"> • Enabled — Displays Enabled if the filter is enabled and running. • Disabled — Displays an empty value if the filter is disabled. To enable, edit the filter.
Adaptive Filter State	Indicates the adaptive state of the filter. If it displays Enabled , the filter is being managed by the Adaptive Filter configuration. If the Adaptive Filter configuration is set to Auto , the filter is automatically disabled. If the configuration is set to Manual , a message is generated in the system log, but the filter has not been disabled.
Functions	Icon representing functions to perform. These options can include resetting the filter and saving the packet trace.

For additional information on the Adaptive Filters, see [“Adaptive Filter Configuration” on page 56](#).

Disabling Adaptive Filter settings for a filter

- STEP 1** From the navigation pane, select **Events > Reports > Adaptive Filter**.
- STEP 2** In the **Ten Most Recent** table, click the **Filter Name**.
- STEP 3** On the Edit Filter page in the **Adaptive Filter Configuration State** table, click **Do not apply adaptive configuration settings to this filter**.
- STEP 4** Click **Apply**.

After the setting is changed, the filter can no longer be managed by the Adaptive Filter function.

Firewall Reports

The Firewall Reports page provides links to data about the network as seen by the firewall (that is, traffic crossing security zones). The report timespan is the preceding 24 hours, or since the last reboot, whichever is more recent. Data is added when the firewall session is closed; therefore, a large file transfer in progress, for example, will not be tabulated until after it finishes.

Data is presented as one of the following graphs:

- **Top Web sites** — The 25 most visited external Web sites by bandwidth. You must create a firewall rule to match with the “web-filter” action between zones that you wish to monitor. You do not need to enable either of the Web content filtering options (manual-filter or filter-service). Only connections

to or from TCP port 80 are displayed. The Web site name is extracted from the HTTP request headers; for requests that do not provide a host name or only an IP address, the IP is displayed. Sites with multiple domains or that host images and other data on different Web servers appear as multiple entries.

- **Firewall rule hits** — The 25 most triggered firewall rules. The “hit count” is the number of firewall sessions that have matched that rule in the table. The top ten rules are assigned colors. Unlike the other tables, which are sorted by bandwidth, entries in this table are displayed in order of precedence; rules outside of the first ten are listed as “other” even if they have larger hit counts.
- **Top clients** — The 25 protocols generating the most traffic to and from internal IP addresses by bandwidth. An internal address is one which is on an internal security zone; that is, one that is part of any internal virtual interface. Generally the only IP addresses not considered internal are those reached via a route out of the external virtual interface. Machines reached via PPTP, L2TP, and IPSec tunnels that terminate on an internal security zone are considered as internal addresses and can appear as clients.
- **Top services** — The 25 services consuming the most bandwidth. For TCP and UDP, the service name is determined from the IP protocol and destination port. Traffic for which there is no known service is shown as a generic name tcp(port), udp(port) or ip(protocol), such as “tcp(1234),” “udp(5001),” or “ip(100).” FTP connections are aggregated, but services such as p2p that use different port numbers appear as multiple entries and cannot be aggregated.

Updating report data

To update the traffic statistics in real time information, select the **Animate Charts** option. If this option is not selected, click the **Refresh Data** link to view the most current information.

6 Network

The Network section describes IP interfaces, security zones, DHCP functions, failover and load balancing, routing, and IP address groups, and explains how to enable, disable, and modify their various features. The network tools provided by the LSM are also described.

Overview

The Network menu pages in the LSM let you set up the X family device to work within your network environment. The following menu options are available:

- **Network Ports** — Manage port configuration (auto-negotiation and line speed), disable, enable, or restart a port.
- **Security zones** — Create and manage security zones that logically segment your network by ports and VLANs, so you can apply firewall rules and IPS filters to traffic passing between sections.
- **IP interfaces** — Manage and configure the internal and external IP interfaces the device uses to make the network connections for your environment. Each security zone must be associated with an IP interface.
- **IP address groups** — Create and manage groups of IP address group by host, subnet, or address range. You can use these IP address group to simplify device configuration.
- **DNS** — Configure the global DNS servers and search domains for the device, or choose to use the DNS configuration obtained from the WAN connection.
- **Default Gateway** — If you have configured an external interface with a static IP address, use this option to manually configure the default IP address that the device uses to route packets when it has no other route to a given IP address.
- **Dynamic DNS** — Supports third-party organizations that offer dynamic DNS addressing. This allows the device to have a changing IP address but a static Internet domain name.
- **WAN Failover and Load Balancing** — Failover configures the secondary external interface for use as a backup link in case the primary link fails. Load balancing between the external interfaces also lets the device use both interfaces simultaneously to route traffic.
- **Routing** — Configure the static and dynamic routing for the device and enable/global options for unicast (OSPF or RIP) and multicast (IGMP and PIM-DM) routing.

- **DHCP Server** — Enable the device to act as a DHCP server and configure the server settings.
- **Tools** — Access tools to look up DNS names, find the physical interface/security zone that the device would use to reach a given location, capture traffic on the device for analysis, ping devices on the network, and trace the network hops traffic takes from the device to another device in the network.

For additional information, see the following topics:

- [“Configuration Overview” on page 130](#)
- [“Deployment Modes” on page 131](#)
- [“Network Ports Page” on page 133](#)
- [“Security Zone Configuration” on page 135](#)
- [“IP Interfaces” on page 141](#)
- [“IP Address Groups Page” on page 156](#)
- [“DNS Page” on page 159](#)
- [“Default Gateway Page” on page 159](#)
- [“Dynamic DNS Page” on page 160](#)
- [“WAN Failover and Load Balancing Page” on page 164](#)
- [“Routing” on page 167](#)
- [“Multicast Routing \(IGMP and PIM-DM\)” on page 180](#)
- [“DHCP Server” on page 185](#)
- [“Network Tools” on page 193](#)

Configuration Overview

The X family device has a default configuration so that the device can pass traffic in most network environments after it has been installed and configured using the Setup Wizard. However, you may need to customize the configuration for your network. The following provides a list of common configuration steps.

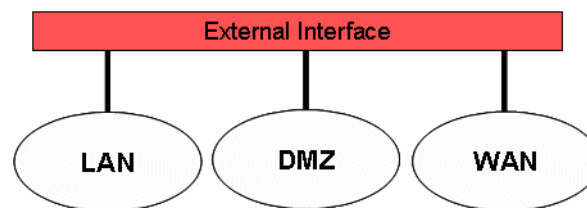
1. Select the deployment mode: Full Transparent, Transparent DMZ - NAT Routed LAN, full routed/ NAT deployment.
2. Configure IP Address Groups to use when creating security zones and configuring the DHCP server (optional).
3. Define IP Interfaces.
4. If you configure an external IP interface to use a static IP address, define the default gateway.
5. Create security zones.
6. Configure Firewall Rules (see [“Firewall” on page 59](#)).
7. Configure DNS servers.
8. Define routing static, unicast, and multicast routing for your network.
9. Configure the default gateway (or route).
10. Configure DHCP Server (optional).

Deployment Modes

The deployment mode you select determines how to configure the IP interfaces and routing on the device. You have the following ways to implement security zones, depending on your current network deployment:

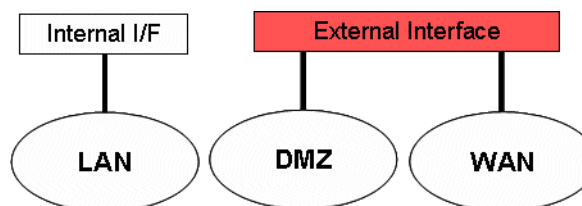
- **Transparent** — In this mode, the device behaves like a layer 2 switch, except that you can still enforce security policy (firewall rules, Web content filtering, IPS filtering, and so forth) between security zones. All devices share the same IP address, which means that you only have one IP interface for all security zones in the same transparent group. All security zones are in the same broadcast domain.

Figure 6–1: X Family Transparent Deployment Mode



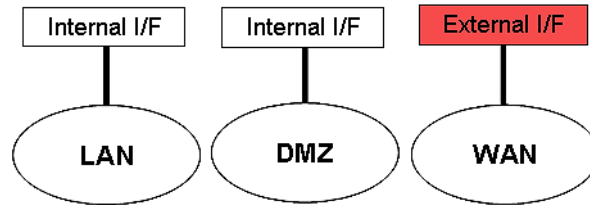
- **Transparent DMZ — NAT/Routed LAN** — In this mode, the network is divided into multiple IP subnets. Each security zone has a unique IP interface, so that the devices within each zone have a unique IP address space. For example, hosts in the LAN zone use a private (RFC 1918) IP address range, while hosts in the WAN and DMZ zones use another IP address range. Private IP addresses originating in the LAN zone and going to the WAN zone are mapped to one or more public IP addresses using NAT. The internal and external IP interfaces are configured with private and public IP addresses, respectively. The LAN security zone is in one broadcast domain, while the DMZ and WAN zones are in another.

Figure 6–2: X Family Transparent DMZ — NAT/Routed LAN Deployment Mode



- **Full routed/NAT** — In this mode, all security zones have unique IP addresses, and addresses going to the WAN zone are subject to NAT. Each security zone is in a separate broadcast domain.

Figure 6–3: X Family Full Routed/NAT Deployment Mode



- **Bridge** — In this mode, the device acts as a bridge to transparently connect security zones assigned to the same virtual interface. You do not have to configure IP routes to bridge traffic. When in bridge mode, the device learns MAC addresses on ports, and forwards traffic within the transparent virtual interface by destination MAC address to the appropriate port. If the address is unknown, the device forwards the packet to all ports. The device does not forward spanning tree packets. It still operates normally as a router and VPN terminator.

For more detailed information and examples of deployment modes, refer to the *Concepts Guide*.

Network Ports Page

Use the Network Ports page to configure and manage the ports on the device. From this page you can complete the following tasks:

- Editing port configuration
- Restarting a port
- Disabling a port



TIP You can view the current status and port configuration from the Port Health page (**Events > Health > Port Health**).

The following figure shows the Network Ports page:

Figure 6–4: Network Ports Page

The screenshot shows the Network Ports page in a web interface. The page title is "Network Ports" under "CONFIGURATION". The page contains a table of port configurations and an "Apply" button.

Port	Auto Negotiation	Line Speed	Duplex Setting	Media	Port Enabled	Restart
1	<input checked="" type="checkbox"/>	100 Mbps	Full	Copper	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	100 Mbps	Full	Copper	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	100 Mbps	Full	Copper	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>	100 Mbps	Full	Copper	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	<input checked="" type="checkbox"/>	100 Mbps	Full	Copper	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6	<input checked="" type="checkbox"/>	100 Mbps	Full	Copper	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The Network Ports page provides the following information:

Column	Description
Port	The port number on the device.
Auto Negotiation	Indicates whether the port auto-negotiates line speed based on the Line Speed setting. If Auto Negotiation is enabled, the device automatically selects the correct line speed and duplex setting based on the device port it is connected to. If Auto Negotiation is disabled, the port will negotiate between the available line speeds.
Line Speed	Indicates the line speed setting for the port: 10 or 100 Mbs.

Column	Description
Duplex Setting	Indicates whether the port is set to full or half duplex.
Media	Indicates whether the port is Copper or Fiber.
Port Enabled	Indicates whether the port is currently enabled or disabled.
Restart	If selected, the port is restarted when you click Apply .

From the Network Ports page you can perform the following tasks:

- Editing port configuration
- Disabling a port
- Restarting a port
- Correcting a port link-down error

Editing port configuration

STEP 1 From the navigation pane, select **Network > Configuration > Network Ports**.

The Network Ports page opens.

STEP 2 Clear the **Auto Negotiation** checkbox for the port you want to configure.

The page updates to show configuration fields for Line Speed and Duplex Setting.

STEP 3 Select the **Line Speed** setting from the drop-down menu.

STEP 4 Select the **Duplex** setting: **Full** or **Half**.

STEP 5 Check the **Restart** checkbox.

STEP 6 Click **Apply**.

The configuration is saved and the port restarts.

Disabling a port

STEP 1 From the navigation pane, select **Network > Configuration > Network Ports**.

The Network Ports page opens.

STEP 2 Clear the **Port Enabled** checkbox.

STEP 3 Check the **Restart** checkbox.

STEP 4 Click **Apply**.

The configuration is saved and the port restarts.

Restarting a port

STEP 1 From the navigation pane, select **Network > Configuration > Network Ports**.

The Network Ports page opens.

STEP 2 Check the **Restart** checkbox.

STEP 3 Click **Apply**.

The configuration is saved and the port restarts.

Troubleshooting Port Link-Down Errors

If the device indicates that the ports are unable to establish a link, check the connections on the device. If you use a copper-fiber translator (such as Netgear) and it is disconnected or loose, the device driver will attempt to re-initialize the port several times before timing out and placing the port in an Out-of-Service mode.

Netgear does not support auto-negotiation. When you remove the copper cable or the cable is loose, Netgear does not attempt to auto-negotiate with the device.

Correcting a port link-down error

STEP 1 From the navigation pane, select **Network > Configuration > Network Ports**.

The Network Ports page opens.

STEP 2 Clear the **Auto Negotiation** checkbox for the port that is not working.

STEP 3 Check the **Restart** checkbox.

STEP 4 Click **Apply**.

The configuration is saved and the port restarts.

Security Zone Configuration

A security zone is a section of the network that is associated with a port, a VLAN, or the termination of a VPN. If you need to control the traffic between devices, the devices must be in separate security zones. You can add, edit, or delete security zones. For further information on security zones, refer to the *Concepts Guide*.

Devices in your network that communicate freely and do not require restricted access between them should be placed in the same zone.

You can view and manage security zones from the Security Zone page (**Network > Configuration > Security Zones**). From this page you can complete the following tasks:

- Viewing a summary of current configuration for all security zones
- Creating a security zone
- Editing the configuration for a security zone
- Deleting a security zone

The following figure shows the Security Zones page:

Figure 6–5: Network: Security Zones Page



The Security Zones page provides the following information about each zone:

Column	Description
Zone	The name of the security zone. Initially, the device is configured with LAN, VPN, and WAN default zones.
VLAN ID	Identifies the VLAN associated with the security zone (if applicable).
Untagged Port(s)	The ports on the device that have been assigned to each zone.
VLAN Tagged Port(s)	The physical ports that have been allocated to the VLAN (if applicable).
Bandwidth Mgmt	Whether bandwidth rate limiting has been applied, and the access speeds in Kbps for outbound (upload) traffic and inbound (download) traffic across the device. Applying bandwidth limitation physically limits the rate of traffic flow.
IP Addr Restrictions	The IP addresses for this security zone, either an IP Address Group , IP subnet , or IP range .
Function(s)	The functions available to manage the security zones: <ul style="list-style-type: none"> • Edit a security zone • Delete a security zone

Creating, Editing, and Configuring Security Zones

Each device is configured with the following default security zones:

Table 6–1: Default Security Zones

Preconfigured Zones	Ports
LAN	Port 1 (or “LAN”)
WAN	Port 6 (or “WAN”)
VPN	VLAN ID = 4

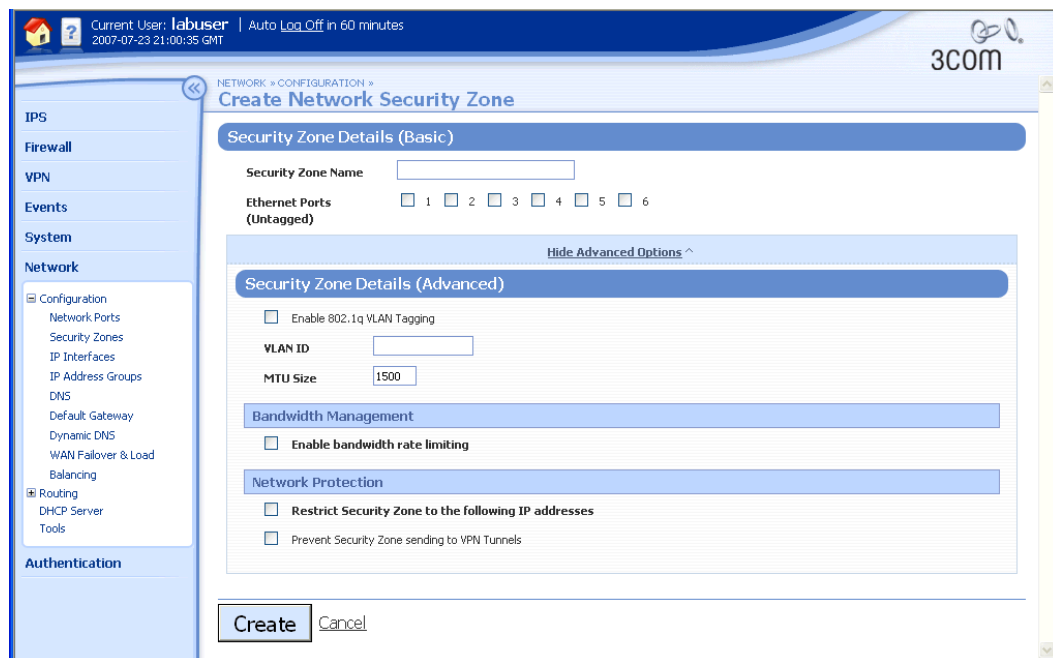
Although the device is preconfigured with default security zones, you can modify these or create your own security zones, with associated security policies and traffic shaping rules, based on your network environment and user requirements.

Setting up security zones involves the following:

1. Create a security zone for each section of the network you want to protect. If you need firewalling between ports, create a security zone for each port so that you can define the firewall policies to monitor the traffic between the zones. You do not need to assign ports to a zone if you are using the zone solely for a VPN tunnel.
2. To use the security zone to monitor traffic, you must assign the zone to an IP interface. For details, see the online help.
3. After creating security zones, configure firewall policies to monitor the traffic entering and leaving the zones.
4. For zones that will send or receive traffic using VPN, add the security zone association to the VPN connection configuration.

You can create and edit security zones from the Create/Edit Security Zone page:

Figure 6–6: Create/Edit Security Zone Page



The following table lists the security zone configuration parameters:

Table 6–2: Security Zone Configuration Parameters

Parameter	Description
Security Zone Name	Type a name for the security zone.
Ethernet Ports (Untagged)	Select one or more ports on the device to be assigned to the zone. If you select a port that is already assigned to another zone, the port will be reassigned to this zone.
Advanced Options	
Enable 802.1q VLAN Tagging	Option to enable VLAN tagging on the port(s) assigned to the security zone. Note With tagged ports, you can have as many security zones sharing a port as you require. Each zone must be associated with an IP interface.
VLAN Tagged Ethernet Ports	If Enable 802.1q VLAN Tagging is enabled, select the physical ports that have been allocated to the VLAN.
VLAN ID	Identifies the VLAN associated with the security zone (if applicable).
MTU Size	Maximum transmission unit (MTU) size in bytes; enter a decimal number from 100 to 1500.

Table 6-2: Security Zone Configuration Parameters (Continued)

Parameter	Description
Bandwidth Management	
Enable bandwidth rate limiting	Select this option to specify bandwidth rate limiting for the access speed for outbound (upload) traffic and inbound (download) traffic across the device. Applying bandwidth limitation physically limits the rate of traffic flow. You can define separate limits for outbound and inbound traffic in Kbps. Note Bandwidth management is typically used to prevent packet queuing on a WAN device to provide lower end-to-end latency on latency-sensitive traffic such as VoIP.
Network Protection If you configure Network Protection options, verify that all IP hosts that use the zone are within the IP addresses specified. Hosts may include: <ul style="list-style-type: none"> • Directly attached hosts connected to the zone via the Ethernet ports associated with the zone • Remote IP subnets connected via routers in the zone • IP address pools specified for any PPTP or L2TP server where the VPNs terminate in the security zone This option is commonly used for transparent deployments to ensure that an IP address can appear in only one security zone.	
Restrict Security Zone to the following IP addresses	The IP addresses for this security zone: IP Address Group , IP Subnet , or IP Range .
Prevent Security Zone sending to VPN Tunnels	Determines whether traffic is allowed from this security zone to an IPSec VPN tunnel.

Creating or editing a security zone

STEP 1 From the navigation pane, select **Network > Security Zones**.

The Security Zones page opens.

STEP 2 Click **Create Security Zone** or click the **Edit** icon for the zone you want to modify.

The Create Network Security Zone or Edit Network Security Zone page opens.

STEP 3 Configure the zone as required.

For more information, refer to [“Configuring a security zone” on page 139](#).

Configuring a security zone

STEP 1 From the navigation pane, select **Network > Security Zones**.

The Security Zones page opens.

STEP 2 Click **Create Security Zone** or click the **Edit** icon for the zone you want to modify.

The Create Network Security Zone or Edit Network Security Zone page opens.

STEP 3 Type the **Security Zone Name** for the new zone.

You can only edit the security zone name when you are creating the zone.

STEP 4 Check the **Ethernet Ports** that you want to add to the zone.

If you select a port that is already assigned to another zone, the port will be reassigned to this zone.

You do not need to assign ports to a zone if you are using the zone solely for a VPN tunnel.



Note You cannot configure firewall rules or IPS filters between ports in the same security zone.

STEP 5 If you want to enable VLAN tagging on the port(s) assigned to the security zone, check the **Enable 802.1q VLAN Tagging** option and enter a VLAN ID.



Note Each security zone must be associated with an interface.

STEP 6 To set the maximum transmission unit (MTU) size, enter a decimal number from 100 to 1500 in the **MTU Size** field.

The default for Ethernet is 1500 bytes. Reducing the MTU ensures that packets sent over networks with smaller MTUs than Ethernet are not fragmented.

STEP 7 To apply **Bandwidth Management**, check **Enable bandwidth rate limiting**, and enter the required limits in Kbps (any decimal number from 1 to 100000) for **outbound traffic** and **inbound traffic** in the appropriate fields.

Bandwidth Management is typically used to prevent packet queuing on a WAN device to provide lower end-to-end latency on latency-sensitive traffic such as VoIP.

STEP 8 To restrict the IP addresses of clients in the security zone, check **Restrict Security Zone to the following IP addresses**. Then, select one of the following:

- **IP Address Group** — Select the name of the group from the drop-down list. (To configure IP address groups, navigate to **Network > Configuration > IP Address Groups**.)
- **IP Subnet** — Type the IP network address and subnet mask.
- **IP Range** — Type a range of IP addresses within the IP interface subnet.

STEP 9 To prevent traffic going from this security zone to an IPSec VPN tunnel, check **Prevent Security Zone sending to VPN Tunnels**.

STEP 10 Click **Create** or **Save**, or **Cancel** to return to the Security Zones page without saving the changes.

IP Interfaces

Configuration Overview

IP interfaces provide the X family device with the interfaces to make the network connections required for your environment. An IP interface is the Layer 3 configuration for the device, that is, the IP configuration for its set of security zones (and hence Ethernet ports within the security zones). Before configuring the IP interfaces for the device, you need to determine the deployment mode that best meets network requirements: transparent, transparent DMZ (NAT/Routed LAN), or full-routed/NAT. For a description of these deployment modes, see [“Deployment Modes” on page 131](#).

The device lets you configure three types of IP interfaces: external, internal, and GRE. You can configure up to two external interfaces; see [Appendix C, “Device Maximum Values”](#) for device maximum configurable values.

Setting up the IP interfaces for a device is a three-step process:

1. For each IP interface, configure the IP address information. An interface is required for every IP subnet that is directly connected to the device. For example, you need one for an Internet connection (external interface) and one for every directly connected network subnet (internal interfaces).
2. For each IP interface, select the security zones that will use the configuration. Each security zone must be associated with an internal or external IP interface.
3. If necessary, configure the interface to perform routing using the advanced configuration options.

For additional information, see the following topics:

- [“IP Interfaces Page” on page 142](#)
- [“IP Addresses: Configuration Overview” on page 143](#)
- [“Configuring a GRE Tunnel” on page 149](#)
- [“Managing Security Zones for IP Interfaces” on page 150](#)
- [“Configuring Routing for IP Interfaces” on page 151](#)

IP Interfaces Page

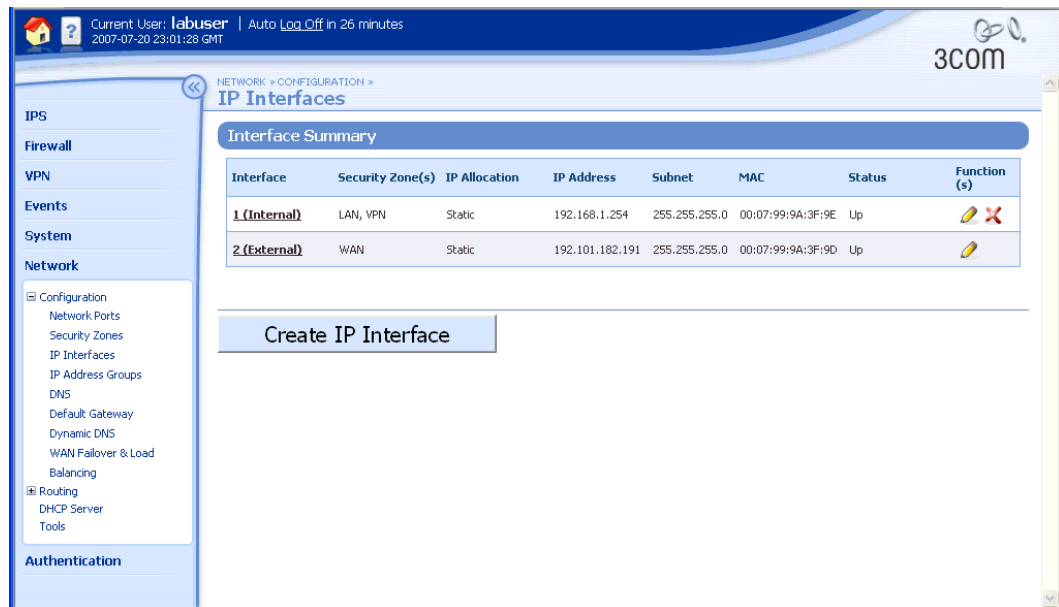
The IP Interfaces page (**Network > Configuration > IP Interfaces**) shows the IP interfaces that are currently configured on the device. From this page you can create, edit, or delete IP interfaces.



Note You can also configure IP interfaces using the device Setup Wizard. For details, see [“Setup Wizard” on page 268](#).



The following figure shows the IP Interfaces page:

Figure 6–7: IP Interfaces Page



The IP Interfaces page provides the following information about each interface:

Column	Description
Interface	The number of the interface, and the type of interface, either GRE , Internal or External . For device maximum configurable values, see Appendix C, “Device Maximum Values” .
Security Zone(s)	The security zones assigned to the interface.
IP Allocation	The allocation method and configuration for the interface.
IP Address	The IP address of the interface.
Subnet	The subnet mask for the interface.
MAC	The MAC address for the internal or external interface. (A GRE interface does not have a MAC address.)

Column	Description
Status	The status of the interface, either Up or Down (with brief details why if the interface is down).
Function(s) The functions available to manage the IP Interfaces: <ul style="list-style-type: none">  • Delete an interface  • Edit the IP interface configuration 	

Managing IP interfaces

STEP 1 From the navigation pane, select **Network > Configuration > IP Interfaces**.

The IP Interfaces page opens.

STEP 2 To edit or delete an interface, click the appropriate icon.

STEP 3 To create an IP interface, click **Create IP Interface**. The Create IP Interfaces page opens. Then, specify the configuration options.

For more information on configuring IP Interfaces, see [“IP Addresses: Configuration Overview” on page 143](#).

IP Addresses: Configuration Overview

For each IP interface required, select the IP address allocation method and configure the required parameters from the IP Interfaces Create or Edit page.

The following allocation methods are available, depending on whether you are configuring an internal or an external interface:

- **Internal (LAN) Interfaces** — The only addressing method available on an internal IP interface is **Static IP Address**.
- **External (WAN) Interface** — Typically this is the interface that the device uses to connect to your Internet Service Provider (ISP). Select one of the following allocation methods:
 - **Static IP Address** — If are using a public static IP address, or if your ISP has allocated you a public static IP address.
 - **DHCP** — If your ISP has told you to use DHCP, or you are connecting to a device that provides IP configuration using DHCP. DHCP is the default IP allocation method for an external interface.
 - **PPTP** — If your ISP is using PPTP to provide your IP configuration.
 - **L2TP** — If your ISP is using L2TP to provide your IP configuration.
 - **PPPoE** — If your ISP is using PPPoE to provide your IP configuration.

For details on configuring the IP address for each type of interface, see the following topics:

- [“Internal Interface: Static IP Address” on page 144](#)
- [“Setting up one-to-many NAT” on page 144](#)
- [“External Interface: Static IP Address Configuration” on page 145](#)
- [“External Interface: DHCP Configuration” on page 146](#)
- [“External Interface: PPTP Client Configuration” on page 146](#)
- [“External Interface: L2TP Client Configuration” on page 147](#)
- [“External Interface: PPPoE Client Configuration” on page 148](#)

After you have configured the basic options for the internal IP interface, you can manage the security zones associated with the interface, or configure routing in the **Advanced Options** section. For details, see the following topics:

- [“Managing Security Zones for IP Interfaces” on page 150](#)
- [“Configuring Routing for IP Interfaces” on page 151](#)

Internal Interface: Static IP Address

The **Internal (LAN) Interfaces** on the X family device use static IP addressing.

Configuring a static IP address on an internal interface

- STEP 1** From the navigation pane, select **Network > Configuration > IP Interfaces**.
- The IP Interfaces page opens.
- STEP 2** Click **Create IP Interface** or the **Edit** icon for the interface that you want to edit.
- The Create IP Interface page or Edit IP Interface page opens.
- STEP 3** In the Interface Type section, select **Internal**.
- STEP 4** In the **Internal Interface Configuration** section, enter information in the appropriate fields:
- **IP Address** — The address on the IP subnet that you have allocated for this interface
 - **Subnet Mask** — The subnet mask associated with the IP subnet
- STEP 5** To allow all the computers on your network to share one IP address, check **Enable NAT**. Then, for the **Public NAT Address**, select one of the following:
- **Use External Interface IP Address**
 - **Manually Enter** and enter a public IP address allocated by your ISP that is on the same subnet as the external interface
- STEP 6** Click **Create** or **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

Setting up one-to-many NAT

When configuring Static IP addressing on the internal interfaces, you can allow the device to perform Network Address Translation (NAT), which allows all the computers on your network to share one IP address. The procedure for setting up one-to-many NAT is described below; see [“Configure a virtual server and provide one-to-one NAT” on page 82](#) for the procedure for setting up one-to-one NAT.

- STEP 1** From the navigation pane, select **Network > Configuration > IP Interfaces**.
The IP Interfaces page opens.
- STEP 2** Select an internal interface and click the Edit icon.
The Edit IP Interface page opens.
- STEP 3** In the **Internal Interface Configuration** section, check **Enable NAT**.
- STEP 4** Either provide one of your unused public IP addresses of the external interface, or select **Use External Interface IP Address** to use the public IP address that X family device is using.
- STEP 5** Click **Save**.
- STEP 6** Configure firewall rules to allow the internal clients to access the required external services.
See [“Creating or editing a firewall rule” on page 70](#) for more information.

External Interface: Static IP Address Configuration

When configuring an external IP interface, select **Static IP Address** if are using a public static IP address or if your ISP has allocated you a public static IP address.



Note After configuring an external interface as a static IP address, you need to configure the default gateway for the device from the Default Gateway page (**Network > Configuration > Default Gateway**). For details, see [“Default Gateway Page” on page 159](#).

Configuring a static IP address on an external IP interface

- STEP 1** Go to **Network > Configuration > IP Interfaces**.
The IP Interfaces page opens.
- STEP 2** Click **Create IP Interface** or the **Edit** icon for the interface that you want to edit.
The Create IP Interface page or Edit IP Interface page opens.
- STEP 3** In the Interface Type section, select **External**.
- STEP 4** In the **External Interface Configuration** section, in the **External Interface Type** drop-down list field, select **Static**.
- STEP 5** In the **External Interface Configuration** section, enter information in the appropriate fields:
- **IP Address** — The public static IP address that you are using or that has been allocated to you by your ISP for this connection



Note If you have been allocated a range of IP addresses, enter one of the addresses in the range.

- **Subnet Mask** — The subnet mask allocated by your ISP for this connection
- STEP 6** Click **Create** or **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

After you have configured the basic options for an external IP interface, you can manage the security zones associated with the interface, or configure routing in the **Advanced Options** section. For details, see the following topics:

- [“Managing Security Zones for IP Interfaces” on page 150](#)
- [“Configuring Routing for IP Interfaces” on page 151](#)

External Interface: DHCP Configuration

When configuring an external IP interface, if your ISP has told you to use DHCP, or you are connecting to a device that provides the IP configuration for the device using DHCP, select **DHCP**. With DHCP, you can confirm the configuration settings by requesting a DHCP lease. If the interface is down, DHCP attempts to auto-connect until the connection is established.

Configuring DHCP on an external IP interface

- STEP 1** From the navigation pane, select **Network > Configuration > IP Interfaces**.
The IP Interfaces page opens.
- STEP 2** Click **Create IP Interface** or select the **Edit** icon for the interface that you want to edit.
The Create IP Interface page or Edit IP Interface page opens.
- STEP 3** In the Interface Type section, select **External**.
- STEP 4** In the **External Interface Configuration** section, in the **External Interface Type** drop-down list field, select **DHCP**.
- STEP 5** Click **Create** or **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

After you have configured the basic options for the internal IP interface, you can manage the security zones associated with the interface, or configure routing in the **Advanced Options** section. For details, see the following topics:

- [“Managing Security Zones for IP Interfaces” on page 150](#)
- [“Configuring Routing for IP Interfaces” on page 151](#)

External Interface: PPTP Client Configuration

When configuring an external IP interface, if your ISP is using PPTP to provide the IP configuration for the device, or you wish to use a PPTP tunnel for all WAN traffic (for example, to connect back to the main office site), select **PPTP**. After configuring the PPTP client, you can confirm the settings by using the **Connect** icon on the IP Interfaces page (**Network > Configuration > IP Interfaces**).



Note Use of a PPTP client requires the device to have a valid IP configuration for an external virtual interface on the local network. This IP configuration can be provided by DHCP or specified via the "Local IP" parameters as shown in step 6 of the following procedure.

Configuring PPTP client on an external IP interface

- STEP 1** From the navigation pane, select **Network > Configuration > IP Interfaces**.
- The IP Interfaces page opens.
- STEP 2** Click **Create IP Interface** or select the **Edit** icon for the interface that you want to edit.
- The Create IP Interface page or Edit IP Interface page opens.
- STEP 3** In the Interface Type section, select **External**.
- STEP 4** In the **External Interface Configuration** section, in the **External Interface Type** drop-down list field, select **PPTP**.
- Additional fields appear.
- STEP 5** In the **External Interface Configuration** section, enter information in the appropriate fields:
- **PPTP/L2TP Server** — The IP address of the PPTP server provided by your ISP.
 - **Username** — The user name allocated by your ISP for this connection.
 - **Password** — The password allocated by your ISP for this connection.
 - **Idle-Disconnect** — Select the amount of time that a connection can be inactive before the user is logged out. Refer to your ISP for disconnection guidelines.
- STEP 6** To set the local IP address on an external virtual interface allowing the device access to the IP network, select one of the following:
- **Local IP - Use DHCP** to use the local IP address allocated by the DHCP server
 - **Local IP - IP Address** and enter the following information to configure the connection manually:
 - IP Address** — The local WAN IP address of the device
 - Subnet Mask** — The subnet mask of the WAN IP subnet
 - Local Gateway** — The local gateway IP address for the WAN IP subnet
- STEP 7** Click **Create** or **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

After you have configured the basic options for an external IP interface, you can manage the security zones associated with the interface, or configure routing in the **Advanced Options** section. For details, see the following topics:

- [“Managing Security Zones for IP Interfaces” on page 150](#)
- [“Configuring Routing for IP Interfaces” on page 151](#)

External Interface: L2TP Client Configuration

When configuring an external IP interface, if your ISP is using L2TP to provide the IP configuration for the device, or you wish to use an L2TP tunnel for all WAN traffic (for example, to connect back to an HQ site), select **L2TP**. After configuring the L2TP client, you can confirm the settings by using the **Connect** button.

Configuring L2TP client on an external IP interface

- STEP 1** From the navigation pane, select **Network > Configuration > IP Interfaces**.
- The IP Interfaces page opens.
- STEP 2** Click **Create IP Interface** or select the **Edit** icon for the interface that you want to edit.
- The Create IP Interface page or Edit IP Interface page opens.
- STEP 3** In the Interface Type section, select **External**.
- STEP 4** In the **External Interface Configuration** section, in the **External Interface Type** drop-down list field, select **L2TP**.
- Additional fields appear.
- STEP 5** In the **External Interface Configuration** section, enter information in the appropriate fields:
- **PPTP/L2TP Server** — The IP address of the L2TP server provided by your ISP.
 - **Username** — The user name allocated by your ISP for this connection.
 - **Password** — The password allocated by your ISP for this connection.
 - **Idle-Disconnect** — Select the amount of time that a connection can be inactive before the user is logged out. Refer to your ISP for disconnection guidelines.
- STEP 6** To set the local IP address on an external virtual interface allowing the device access to the IP network, select one of the following:
- **Local IP - Use DHCP** to use the local IP address allocated by the DHCP server.
 - **Local IP - IP Address** and enter the following information to configure the connection manually:
 - IP address** — The local WAN IP address of the device
 - Subnet Mask** — The subnet mask of the WAN IP subnet
 - Local Gateway** — The local gateway IP address for the WAN IP subnet
- STEP 7** Click **Create** or **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

After you have configured the basic options for an external IP interface, you can manage the security zones associated with the interface, or configure routing in the **Advanced Options** section. For details, see the following topics:

- [“Managing Security Zones for IP Interfaces” on page 150](#)
- [“Configuring Routing for IP Interfaces” on page 151](#)

External Interface: PPPoE Client Configuration

When configuring an external IP interface, if your ISP is using PPPoE to provide the IP configuration for the device, select **PPPoE**. After configuring the PPPoE client, you can confirm the settings by using the **Connect** button.

Configuring PPPoE client on an external IP interface

- STEP 1** From the navigation pane, select **Network > Configuration > IP Interfaces**.
- The IP Interfaces page opens.
- STEP 2** Click **Create IP Interface** or select the **Edit** icon for the interface that you want to edit.
- The Create IP Interface page or Edit IP Interface page opens.
- STEP 3** In the Interface Type section, select **External**.
- STEP 4** In the **External Interface Configuration** section, in the **External Interface Type** drop-down list field, select **PPPoE**.
- Additional fields appear.
- STEP 5** In the **External Interface Configuration** section, enter information in the appropriate fields:
- **Username** — The user name allocated by your ISP for this connection.
 - **Password** — The password allocated by your ISP for this connection.
 - **Idle-Disconnect** — Select the amount of time that a connection can be inactive before the user is logged out. Refer to your ISP for disconnection guidelines.
- STEP 6** Click **Create** or **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

After you have configured the basic options for an external IP interface, you can manage the security zones associated with the interface, or configure routing in the **Advanced Options** section. For details, see the following topics:

- [“Managing Security Zones for IP Interfaces” on page 150](#)
- [“Configuring Routing for IP Interfaces” on page 151](#)

Configuring a GRE Tunnel

An IP Security (IPSec) tunnel can only carry unicast IP traffic. **Generic Route Encapsulation (GRE)** can be used to allow transfer of dynamic routing (RIP), Open Shortest Path First (OSPF), and multicast traffic between two GRE end points (a GRE tunnel). This GRE tunnel can then be secured by further encapsulation within an IPSec tunnel. Note that GRE tunnels cannot encapsulate non-IP traffic.

For secure GRE connections, you must configure an IPSec security association (IPSec SA) before you configure GRE tunnels. You can configure an IPSec SA from the IPSec Status page (**VPN > IPSec Status**).

Secure GRE connections are required if either side of the GRE tunnel has a dynamic address, since the remote tunnel endpoint can change.

A GRE tunnel requires a security zone; however, GRE tunnels can share security zones. This eliminates the need to create a security zone for each GRE tunnel.

Configuring a secure GRE tunnel to a remote device

STEP 1 From the navigation pane, select **Network > Configuration > IP Interfaces**.

The IP Interfaces page opens.

STEP 2 Click **Create IP Interface** or select the **Edit** icon for the interface that you want to edit.

The Create IP Interface page or Edit IP Interface page opens.

STEP 3 In the Interface Type section, select **GRE Tunnel secured by IPSec SA**.

STEP 4 In the **GRE Interface Configuration** section, in the **IPSec SA** drop-down list field, select the security association from the drop-down list.



CAUTION 3Com recommends that you select **Unsecured** only if you do not intend to use IPSec and if the network that the GRE tunnel traverses is secure.

STEP 5 Enter information in the remaining fields:

STEP A If you selected **Unsecured**, the **Remote Tunnel Endpoint** field becomes available.

Type the IP address or hostname for the remote device on the public network.

STEP B In the **IP Address** field, enter the IP address of the tunnel on the local network on the external virtual interface. Choose an unused IP address that is routable through your network.

STEP C In the **Peer IP Address** field, type the IP address for the peer. This is the IP address entered in the IP Address field on the remote device.

STEP 6 In the Security Zones section, configure the security zones assigned to the tunnel. For details, see [“Managing Security Zones for IP Interfaces” on page 150](#).

STEP 7 Click **Create** or **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

After you have configured the basic options for the GRE tunnel, you can manage the security zones associated with the interface, or configure routing in the **Advanced Options** section. For details, see the following topics:

- [“Managing Security Zones for IP Interfaces” on page 150](#)
- [“Configuring Routing for IP Interfaces” on page 151](#)


Managing Security Zones for IP Interfaces

Security zones can be configured to control traffic across the network. Each security zone is associated with an IP interface.

The IP Interfaces page lists the zones that are assigned to each interface. All firewall and IPS filtering can be applied between any two security zones even if they are on the same IP interface.

You can manage (add or remove) the security zone configuration for an IP interface from the Create or Edit IP Interface pages.

Managing (adding or removing) security zones for IP interfaces

- STEP 1** From the navigation pane, select **Network > Configuration > IP Interfaces**.
- The IP Interfaces page opens.
- STEP 2** Click **Create IP Interface** or select the **Edit** icon for the interface that you want to edit.
- The Create IP Interface page or Edit IP Interface page opens.
- STEP 3** Scroll down to the **Security Zones** section.
- STEP 4** From the **Security Zone** drop-down list, select the zone you want to add to the IP interface. Then, click **Add to table below**.
- STEP 5** Add as many zones as needed.
- STEP 6** To delete a zone, in the **Function(s)** column for the zone, click  .
- STEP 7** Click **Create** or **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

Configuring Routing for IP Interfaces

You can configure IP interfaces to perform dynamic unicast or multicast routing if required. You can modify routing information from the Create IP Interfaces or Edit IP Interfaces pages (**Network > Configuration > IP Interfaces**). For details, see the following topics:

- [“Bridge Mode for IP Interfaces” on page 151](#)
- [“OSPF for IP Interfaces” on page 152](#)
- [“RIP for IP Interfaces” on page 153](#)
- [“Multicast Routing for IP Interfaces” on page 155](#)

Bridge Mode for IP Interfaces

In bridge mode, the X family device implements a software bridge to transparently connect security zones assigned to the same virtual interface. Using bridge mode, you do not have to configure IP routes to bridge traffic.



Note The High Availability feature is not available if bridge mode is enabled.

Enabling bridge mode on an IP interface

- STEP 1** From the navigation pane, select **Network > Configuration > IP Interfaces**.
- The IP Interfaces page opens.
- STEP 2** Click **Create IP Interface** or select the **Edit** icon for the interface that you want to edit.
- The Create IP Interface page or Edit IP Interface page opens.
- STEP 3** Near the bottom of the page, click **Show Advanced Options**.
- The **IP Interface Details (Advanced)** section opens.

- STEP 4** Select **Enable bridge mode**.
- STEP 5** Click **Create** or **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

OSPF for IP Interfaces

OSPF (Open Shortest Path First, RFC 2328) is an interior gateway protocol used within larger autonomous system networks. For more information on OSPF, see the *Concepts Guide*.

The X family device supports redistribution of routing information between the RIP and OSPF routing stacks.



Note Before using OSPF on an IP interface, you must enable it globally from the OSPF Setup page (**Network > Routing > OSPF**).

Enabling and configuring OSPF on an IP interface

- STEP 1** From the navigation pane, select **Network > Configuration > IP Interfaces**.
The IP Interfaces page opens.
- STEP 2** Click **Create IP Interface** or select the **Edit** icon for the interface that you want to edit.
The Create IP Interface page or Edit IP Interface page opens.
- STEP 3** Near the bottom of the page, click **Show Advanced Options**.
The **IP Interface Details (Advanced)** section opens.
- STEP 4** In the **OSPF** section, select **Enable OSPF**.
Additional fields appear.
- STEP 5** To prevent this interface from being advertised by RIP throughout the network, select **Disable OSPF Advertisement of this interface on other interfaces**.
3Com recommends enabling this option on every external IP interface.
- STEP 6** Enter configuration information in the remaining fields:
 - STEP A** In the **OSPF Area ID** field, type the area number (in IP address format). The area identifies a hierarchical set of routers that exchanges link state advertisements (LSAs). The area must exist before you can assign a virtual interface to it. (Area 0.0.0.0 always exists.)
 - STEP B** In the **OSPF Router Priority** field, type the device's priority. Router priority is only used on multi-access networks such as LANs. The router with the highest priority becomes the Designated Router (DR) for the LAN. A router with a priority of 0 is not eligible to become DR. At least one router on a LAN must have a priority greater than 0, since there must be a DR; if all routers have the same priority, they negotiate with each other for the DR election. The default priority is 1. The best practice is to assign the least busy router on a LAN as the DR, to reduce processing overhead on busier routers.

- STEP C** In the **OSPF Output Cost** field, type the cost. The default is 1. The lower the cost, the more the path is given preference.
- STEP D** In the **Hello Interval** field, type the Hello Interval (1 to 8192 seconds; the default is 10 seconds). This is the interval at which the device sends out hello (“keep-alive”) packets, which signal to routers that the device is up. This value must be identical to the value on its neighbors. The smaller the hello interval, the faster the network converges, but the more network resources are consumed.
- STEP E** In the **OSPF Router Dead Interval** field, type the device’s dead interval in seconds. If the device does not receive a hello packet within this time, it assumes its neighbor is down. This interval is normally about four times the Hello Interval. The default is 40 seconds.



Note The Hello Interval and Router Dead Interval must match for each connected router or the routers will not be able to communicate. If you change the defaults, you must change them on all attached routers.

- STEP F** In the **OSPF Retransmit Interval** field, type the retransmit interval in seconds; the default is 30 seconds. After sending an LSA, the device waits for an acknowledgement packet. If it receives no acknowledgement within the retransmit interval, it retransmits the LSA.
- STEP G** In the **OSPF Transmit Delay** field, type the transmit delay in seconds; the default is 30 seconds.
- STEP H** Select the **OSPF v2 Authentication** type:
Null (no authentication used).
Simple (plain-text password). Type an authorization key. The authentication key is a password (up to 8 characters) which can be assigned on a per-interface basis. The authentication key must match that of each router on the interface
Crypto (encrypted password). Type an authorization key. The authentication key is a password (up to 8 characters) which can be assigned on a per-interface basis. The authentication key must match that of each router on the interface. Type the **OSPF Key ID** (the default is 1). **Crypto** is the recommended authentication type.

- STEP 7** Click **Create** or **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

RIP for IP Interfaces

RIP (Routing Information Protocol, RFC 2453) is used for exchanging unicast routing information between routers and hosts.

The X family device listens for RIP advertisements from routers and combines them with its static route and configured interface information, then calculates the shortest route to any destination.

Using RIP, the device determines the route for network packets based on the fewest number of hops between the source and the destination. RIP regularly broadcasts routing information to other devices on the network.

RIPv1 Configuration Settings

RIPv1 is a simple distance vector protocol where the longest path cannot exceed 15 hops and static metrics are used to compare routes. RIPv1 should only be used to communicate routing information with legacy devices that cannot support RIPv2. Because the protocol does not send subnet mask information, it is considered technically obsolete and can cause routing problems in classless networks. RIPv1 should only be used when all of the consequences of its use are well understood by the network administrator.

RIPv2 Configuration Settings

RIP version 2 is the current version of the RIP protocol. It adds support subnetted CIDR networks and authentication of routing updates. The preferred method for sending RIPv2 advertisements is multicast. This also reduces the interrupt load on other network devices that are not interested in routing updates. Broadcast should only be used for compatibility with legacy RIPv1 devices. RIPv2 MD5 authentication is highly recommended to prevent the device from accepting bogus routing information.



Note Before using RIP on an IP interface, you must enable it globally from the RIP Setup page (**Network > Routing > RIP**).

Enabling and configuring RIP on an IP interface

- STEP 1** From the navigation pane, select **Network > Configuration > IP Interfaces**.
The IP Interfaces page opens.
- STEP 2** Click **Create IP Interface** or select the **Edit** icon for the interface that you want to edit.
The Create IP Interface page or Edit IP Interface page opens.
- STEP 3** Near the bottom of the page, click **Show Advanced Options**.
The **IP Interface Details (Advanced)** section opens.
- STEP 4** In the **RIP** section, select **Enable RIP**.
Additional fields appear.
- STEP 5** To prevent this interface from being advertised by RIP throughout the network, select **Disable RIP Advertisement of this interface on other interfaces**.
3Com recommends enabling this option on every external IP interface.
- STEP 6** Select one of the following from the **Send Mode** drop-down list:
- **Do not send updates** — Passive mode
 - **RIP v1** — Send route advertisements as RIPv1
 - **RIP v2 Multicast** — Send route advertisements using IP multicast address 224.0.0.9
 - **RIP v2 Broadcast** — Send route advertisements using IP broadcast address

- STEP 7** Select one of the following from the **Receive Mode** drop-down list:
- **Do not receive updates** — Ignore all route advertisements received on this interface
 - **RIP v1 only** — Accept only v1 advertisements received on this interface
 - **RIP v2 only**— Accept only v2 advertisements received on this interface
 - **RIP v1 or v2**— Accept any RIP advertisements received on this interface
- STEP 8** For **RIP v2 Authentication**, select one of the following authentication methods:
- **None** — Use no authentication of RIP communication on the interface.
 - **Simple** — Use clear-text password authentication. Enter a password of between 1 and 32 characters (over 8 characters is recommended).
 - **MD5** — Use Message Digest version 5 (MD5) authentication. Enter a password of between 1 and 32 characters (over 8 characters is recommended). MD5 is the recommended authentication mechanism.
- STEP 9** Select **Enable Split Horizon** to prevent the device from advertising networks in the direction from which those networks were learned. Split Horizon reduces convergence time. The announcements only include networks in the opposite direction. This also reduces loops.
- STEP 10** If **Enable Split Horizon** is enabled, check **Enable Poison Reverse** to further ensure that routes learned from a neighbor are not advertised back.
- Routes learned from a neighbor are advertised back to it with metric 16 (unreachable). Enabling Poison Reverse has a similar effect as split horizon, and is also called split horizon with poison reverse. In a single-path network this has no advantage over split horizon. However, in multi-path networks this greatly reduces loops.
- STEP 11** Select **Enable RIP Redistribution of OSPF routes** to enable redistribution of OSPF routes by the RIP protocol on this interface.
- STEP 12** Click **Create** or **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

Multicast Routing for IP Interfaces

The X family device can be configured to function as a multicast router on the network. The device supports two multicast protocols; you can configure an IP interface with either or both:

- **IGMP** — **Internet Group Management Protocol**, used by hosts to define multicast group membership. Multicast groups are identified by special IP addresses.
IGMP must be enabled on all IP interfaces that are directly connected to clients using multicast traffic.
- **PIM-DM** — **Protocol Independent Multicast-Dense Mode** routing protocol, used for multicast routing between remote sites. PIM-DM is also used to support site-to-site NBX conference calls.
PIM-DM must be enabled on all IP interfaces that multicast data will travel through to or from the multicast clients. This includes the GRE and IP interfaces.



Note Firewall rules must be established to allow PIM-DM and IGMP to be passed through the firewall between each set of security zone pairs that the multicast traffic must traverse. This includes between virtual zones such as a VPN zone and this-device.

Enabling multicasting on an IP interface

- STEP 1** From the navigation pane, select **Network > Configuration > IP Interfaces**.
- The IP Interfaces page opens.
- STEP 2** Click **Create IP Interface** or select the **Edit** icon for the interface that you want to edit.
- The Create IP Interface page or Edit IP Interface page opens.
- STEP 3** Near the bottom of the page, click **Show Advanced Options**.
- The **IP Interface Details (Advanced)** section opens.
- STEP 4** In the **IGMP/PIM-DM** section, select **Enable IGMP** and/or **Enable PIM-DM** to enable multicast routing.
- STEP 5** If you select **Enable IGMP**, additional fields appear. Enter configuration information in the remaining fields:
- STEP A** In the **Host Query Interval** field, type the interval at which host membership queries are sent. The default is 125 seconds.
- STEP B** In the **Max Query Response Time** field, type the maximum response time. The default is 10 seconds.
- STEP C** In the **Query Timeout** field, type the longest interval that a group will remain in the local group database without receiving a Host Membership Report. The default is 250 seconds.
- STEP 6** Click **Create** or **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.
- STEP 7** Enable firewall rules to allow PIM-DM and/or IGMP to/from *this-device* for the relevant zones.

After configuring the multicast routing options, verify that the IGMP and/or PIM-DM options have been enabled globally. For details, see the following topics:

- [“IGMP Setup Page” on page 181](#)
- [“PIM-DM Setup Page” on page 183](#)

IP Address Groups Page

IP address groups let you associate a selection of IP addresses with a name that can be used in place of the specific IP addresses. IP address groups save time when configuring the X family device because you can apply the same parameters to all IP addresses in the group rather than configuring each address separately.

IP address groups can be used when configuring the following features:

- Firewall rules
- DHCP server address pool
- IPSec local and destination subnets

- PPTP pool
- L2TP pool
- Security zones
- Anti-Spam

You can manage IP address groups from the IP Address Groups page (**Network > Configuration > IP Address Groups**). From this page you can complete the following tasks:



- Creating an IP address group
- Editing an existing group to add or remove addresses
- Deleting an IP address group

The following figure shows the IP Address Groups page:

Figure 6–8: IP Address Groups Page



The screenshot shows the IP Address Groups page in a 3COM network management interface. The page title is "IP Address Groups" under the "NETWORK > CONFIGURATION" menu. The interface includes a left-hand navigation menu with categories: IPS, Firewall, VPN, Events, System, Network, and Authentication. The "Network" category is expanded, showing sub-items: Configuration (Network Ports, Security Zones, IP Interfaces, IP Address Groups, DNS, Default Gateway, Dynamic DNS, WAN Failover & Load, Balancing), Routing (DHCP Server, Tools), and Authentication.

The main content area displays a table of IP Address Groups. The table has three columns: Name, IP Addresses, and Function(s). There is a "Records per page" dropdown set to 25. Below the table is a "Create Address Group" button.

Name	IP Addresses	Function(s)
DHCP-Pool	192.168.1.1 - 192.168.1.20	 

The IP Address Groups page provides the following information about existing groups:

Table 6–3: IP Address Group Details

Column	Description
Name	The name of the IP address group.
IP Addresses	The IP addresses belonging to the group. These can include IP hosts, IP ranges, and IP subnets.
<p>Function(s) The functions available to manage each IP address group listed in the table:</p> <ul style="list-style-type: none">  • Delete an IP address group  • Edit the IP address group to add or remove IP addresses 	

Creating or editing IP address groups

- STEP 1** From the navigation pane, select **Network > Configuration > IP Address Groups**.
The IP Address Groups page opens.
- STEP 2** Click **Create Address Group** to add an IP Address Group, or click the Edit button for the group you want to edit.
The Create/Edit IP Address Group page opens.
- STEP 3** Type a **Group Name**.
- STEP 4** Select the type of IP address you want to add to the group, either:
- **IP Host** — A host IP address.
 - **IP Subnet** — A subnet IP address/mask.
 - **IP Range** — A range of IP addresses.
- STEP 5** Click **Add to table below** to add the address to the group and update the table.
- STEP 6** To remove an address, click the Delete icon in the **Function(s)** column of the address table.
- STEP 7** Click **Save**.

DNS Page

You can configure the global DNS settings for the device from the DNS page (**Network > Configuration > DNS**). You can configure up to three DNS servers and search domains, or use the DNS configuration obtained from the WAN connection. The device uses global DNS settings for its own DNS lookups or when it functions as a DNS relay.

Manually configuring global DNS servers

- STEP 1** From the navigation pane, select **Network > DNS**.
The DNS page opens.
- STEP 2** Select **Manually configure DNS servers and search domains**.
- STEP 3** Type the **DNS Server** IP address and **DNS Search Domain** for up to three DNS servers.
- STEP 4** Click **Apply**.

Obtaining the DNS configuration from the WAN connection

- STEP 1** From the navigation pane, select **Network > DNS**.
The DNS page opens.
- STEP 2** Select **Use DNS configuration obtained from WAN connection**.
The DNS server configuration returned from the ISP is used. Alternatively, the DNS servers can be explicitly set using the manual configuration option.
- STEP 3** Click **Apply**.



Note If you have enabled and configured the DHCP server option for the device, you can override the DNS settings returned to DHCP clients if necessary. For details, see [“Configuring the DHCP Server” on page 187](#). If you do not override these settings, DHCP clients will receive the DNS server settings used by the device itself.

Default Gateway Page

The device uses the default IP gateway to route packets when it has no other route to a given IP address. You can configure the default gateway from within the IP interface settings for an external interface or by using the Default Gateway page (**Network > Configuration > Default Gateway**). If you are not using the WAN Load Balancing feature with two external interfaces, you normally configure a single Default Gateway. This can be on your LAN or (more normally) an address provided by your ISP.

- If you have configured an external interface to use a static IP address, then you must manually configure the default gateway.
- If you are using L2TP, PPTP, PPPoE, or DHCP, then the default route will be automatically configured by your ISP and you cannot configure it yourself.

- If you are using WAN ISP failover or load balancing, then the default gateway should only be configured by editing the settings of the external IP interface.
- If you are using two external interfaces with WAN load balancing, then configure the default gateways for each on the external interfaces themselves. The Default Gateway screen only shows the default gateway of the primary external interface.

Configuring the default route for a single external interface

STEP 1 From the navigation pane, select **Network > Configuration > Default Gateway**.

The Default Gateway page opens.

STEP 2 Select **Manually configure Default Gateway** and type the **IP Address** for the default gateway.

Enter the IP address of the next router on the WAN side of the device into the **Default Gateway** field. Your ISP will provide you with this information.

Dynamic DNS Page

The X family device supports selected third-party dynamic DNS providers. Dynamic DNS lets the device use a dynamic IP address allocated by the Internet Service Provider (ISP) while retaining a static Internet domain name. The device sends the provider its initial IP address, refreshes that information according to the provider's schedule, and notifies the provider when the address changes. (The last address and notification time is stored to prevent multiple notifications if the device is restarted.)

Dynamic DNS integrates with virtual servers and simplifies VPN configuration. Virtual servers can be accessed by a stable DNS name rather than a volatile IP address. You can configure VPNs to connect to a peer device specified by DNS name, making it easier to configure site-to-site connections between small offices with dynamic IP addresses.

Dynamic DNS enables the following services:

- A public (WWW) Internet server with a dynamic IP address.
- Site-to-site VPN with dynamic WAN interface addresses.
- Failover support. The DNS name for the device is updated should its IP address change. For example, this can occur if the ISP suffers an Internet service outage and the device fails over to an alternative ISP.

The following table lists the supported dynamic DNS providers:

Table 6-4: Supported Dynamic DNS Providers

Provider	URL
ChangeIP	www.changeip.com
DHS International	www.dhs.org
DynDNS	www.dyndns.com

Table 6–4: Supported Dynamic DNS Providers (Continued)

Provider	URL
DyNS	www.dyns.cx
easyDNS	www.easydns.com
easyDNS-PARTNER	www.easydns.com
No-IP	www.no-ip.com
ODS	www.ods.org
TZO	www.tzo.com
ZoneEdit	www.zoneedit.com

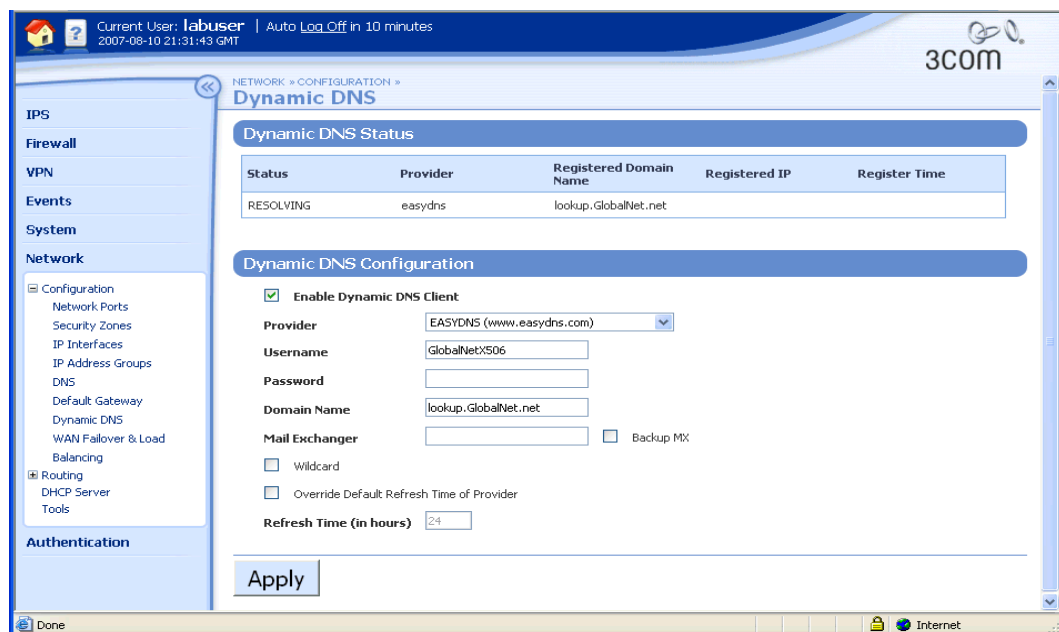
You can manage dynamic DNS from the Dynamic DNS page (**Network > Configuration > Dynamic DNS**). From this page you can complete the following tasks:

- Enabling or disabling dynamic DNS
- Checking dynamic DNS status

For additional information, see the following:

- [“Enabling dynamic DNS” on page 163](#)

The following figure shows the Dynamic DNS page:

Figure 6–9: Dynamic DNS Page

The Dynamic DNS page provides the following information:

Column	Description
Dynamic DNS Status	
Status	One of the following: RESOLVING — Resolving IP address of server CONNECTING — Connecting to server REGISTERING — Registering with server REGISTERED — Registered with server STOPPED — DDNS thread stopped
Provider	Name of the dynamic DNS provider.
Registered Domain Name	Registered domain name
Registered IP	Current IP address.
Register Time	Time of the last notification.
Dynamic DNS Configuration	
Enable Dynamic DNS Client	Select to enable dynamic DNS.
Provider	Select a provider from the drop-down list.
Username	User name registered with provider.
Password	Password registered with provider.
Domain Name	Domain name portion of fully qualified domain name.
DYNDNS Host Type	The type of service registered (DYNDNS only) <ul style="list-style-type: none"> • Dynamic (the default) • Static • Custom
Mail Exchanger	Indicates mail server for the domain name registered with the dynamic DNS provider. Sent in replies to DNS queries.
Backup MX	When selected, use smtp.easydns.com as a backup mail exchanger with a lower priority (easyDNS only).
EASYDNS Partner Name	Partner name (easyDNS-PARTNER only). For example, for <code>http://bell.easydns.ca/</code> the partner name is <code>bellnet</code> .
Wildcard	ON or OFF (easyDNS-PARTNER only). This allows all fully qualified domain names <code>*.domain.com</code> to resolve to the same address as <code>domain.com</code> .
Override Default Refresh Time of Provider	Select to override the default refresh time of the selected provider.

Column	Description
Refresh Time (in hours)	Enter the time interval between refreshes of DNS records with the provider. The default is the provider's default.

Enabling dynamic DNS

Before configuring dynamic DNS on the device, choose one of the supported dynamic DNS providers and register an account with them, making note of the registered user name and password.

STEP 1 From the navigational pane, select **Network > Configuration > Dynamic DNS**.

The Dynamic DNS page opens.

STEP 2 Select **Enable Dynamic DNS Client**.

Additional configuration options appear:

STEP A Select the **Provider** from the drop-down list.

STEP B Type the **Username** registered with the dynamic DNS provider.

STEP C Type the **Password** registered with the dynamic DNS provider.

STEP D Type the **Domain Name** portion of the fully qualified domain name registered with the dynamic DNS provider.

STEP E For DYNDNS only, select a **DYNDNS Host-type** : **Dynamic**, **Static**, or **Custom**.

STEP F For EasyDNS-PARTNER only, type an **EasyDNS Partner** (the EasyDNS reseller or partner that provided your account).

STEP G Type a **Mail Exchanger** that specifies where mail for the registered hostname should go.

STEP H Optionally, select **Backup MX** to allow the dynamic DNS provider to be a backup mail spooler for the domain.

STEP I Optionally, select **Wildcard** to enable wildcards for this host.

STEP J Select **Override Default Refresh Time of Provider** and enter a Refresh Time in hours. (The default is the provider's default; 3Com recommends not changing the default value, lest the provider disable or terminate your account.)

STEP 3 Click **Apply**.

STEP 4 3Com recommends testing the DNS name from the Internet.

You can now use the DNS name for features such as virtual servers, remote management of the device, and VPN configuration.

WAN Failover and Load Balancing Page

WAN failover supports a secondary external interface for use as a backup link in case the primary link fails. Load balancing lets the X family device use both external interfaces to route traffic.

You can manage failover and load balancing from the WAN Failover & Load Balancing page (**Network > Configuration > WAN Failover & Load Balancing**). From this page you can complete the following tasks:

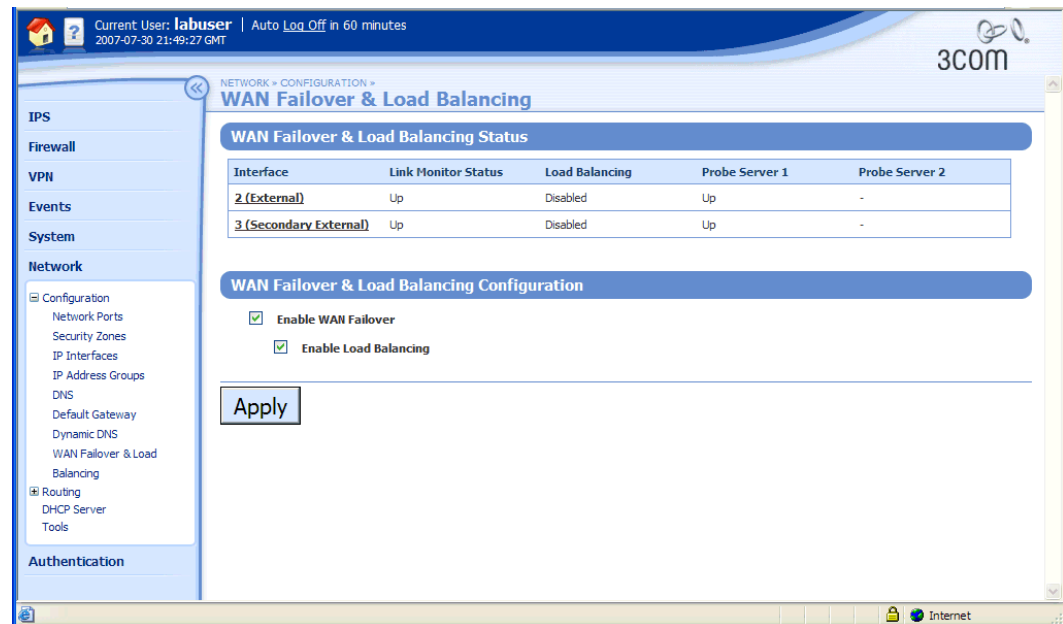
- Enabling or disabling failover
- Enabling or disabling load balancing

For additional information, see the following:

- [“Configuring link monitoring” on page 165](#)
- [“Enabling failover” on page 166](#)
- [“Configuring load balancing” on page 166](#)

The following figure shows the WAN Failover & Load Balancing page:

Figure 6–10: WAN Failover & Load Balancing Page



The WAN Failover & Load Balancing page provides the following information:

Column	Description
Interface	Lists the interfaces defined.
Link Monitor Status	Status of link: Up or Down .

Column	Description
Load Balancing	Status of load balancing: Enabled or Disabled .
Probe Server 1	Primary ping server.
Probe Server 2	Backup ping server.

Link Monitoring

The X family device probes the link to the ISP either by using ICMP pings or by trying to form a TCP connection to the default gateway or to a user-defined IP address on that external interface. The device periodically probes the specified servers to determine if the link is up. If a reply is seen then the link is considered good. If no reply is received after a configurable number of tries, the device switches the link to the secondary external interface. You can configure the device to fall back to the primary interface after a configurable number of successful tries.



Note For the ICMP (ping) probe, the server must be configured to respond to pings.

Configuring link monitoring

Link monitoring is configured as part of defining or editing an external interface.

STEP 1 From either the Create IP Interface or Edit IP Interface page for an external interface, click **Show Advanced Options**.

The Show Advanced Options section opens.

STEP 2 Select **Enable Link Monitor**.

Additional configuration options appear:

STEP A Select the **Fail Condition: Primary fail, Both fail, or Any fail**. This defines what the result of the probe needs to be before the link is considered to have failed.

STEP B For **Probe Server 1**, select the probe type, either **ICMP** or **TCP**, and the address, either **Default Gateway** or **IP Address**. If you select IP Address, type an IP address and port number.

STEP C For **Probe Server 2**, select the probe type, either **ICMP** or **TCP**, and the address, either **Default Gateway** or **IP Address**. If you select IP Address, type an IP address and port number.

STEP D Type a **Probe Interval** in seconds (the default is five seconds).

STEP E Type a **Fail after** number of probes (the default is 3 probes).

STEP F Type a **Succeed after** number of probes (the default is 3 probes).

STEP 3 Click **Create** or **Save**.

Failover

The failover function switches routes from the primary to the secondary link if it detects that the primary link is down. Once the primary link is back up, it switches the routes back.

You can configure the time interval for sending pings, the number of unsuccessful pings before failover, and the number of successful pings before falling back to the primary interface when you define the external interface. For more information, see [“IP Addresses: Configuration Overview” on page 143](#).

You must configure the second external interface before you can configure failover. For details, see [“IP Addresses: Configuration Overview” on page 143](#). If applicable, you must add firewall rules manually for the backup link. For details, see [“Creating or editing a firewall rule” on page 70](#).

Enabling failover

STEP 1 From the navigation pane, select **Network > WAN Failover & Load Balancing**.

The WAN Failover & Load Balancing page opens.

STEP 2 In the **WAN Failover & Load Balancing Configuration** section, select **Enable WAN Failover**.

STEP 3 Click **Apply**.

Load Balancing

WAN ISP load balancing lets you configure two external interfaces over which traffic can be routed, by using either specific static routes or a simple round-robin algorithm that selects a particular external interface based on source and destination IP address.

When using load balancing, bear in mind the following considerations:

- You must configure failover before you can configure load balancing.
- Transparent mode is not supported.
- The device sends GRE encapsulated traffic only on the primary link.
- The device sends IPsec encrypted traffic only on the primary link unless the link fails, in which case the traffic is switched to the secondary link. You must configure the peer of the IPsec tunnel with an alternate VPN peer address.
- Local device traffic only uses the primary link unless the link fails, in which case the traffic is switched to the secondary link.
- Internal interfaces that do not have NAT enabled, or that have NAT enabled with a specific IP address rather than *external-ip*, are not load balanced; instead, their traffic is always sent using the primary external interface.

Configuring load balancing

STEP 1 From the navigation pane, select **Network > WAN Failover & Load Balancing**.

The WAN Failover & Load Balancing page opens.

- STEP 2** In the **WAN Failover & Load Balancing Configuration** section, select **Enable Load Balancing**.
- STEP 3** Click **Apply**.

Routing

The X family device provides static and dynamic routing which you can manage and configure from the Routing menu pages. The menu provides the following options:

- **Routing Table** — View all current routes on the device. Use the Routing Table to view the routes by IP address and subnet mask.
- **Static Routes** — Review, manage, and create static routes for the device. A static route defines the gateway to use for a particular network.
- **OSPF** — Enable OSPF globally; view and edit IP interfaces configured with OSPF.
- **RIP** — Enable RIP (unicast routing) globally; view and edit IP interfaces configured with RIP.
- **IGMP** — Enable IGMP (multicast routing) globally; view and edit IP interfaces configured with IGMP.
- **PIM-DM** — Enable PIM-DM (multicast routing) globally; view and edit IP interfaces configured with IGMP.



Note If you have configured OSPF, RIP, IGMP, or PIM-DM routing on an IP interface, these options must be enabled globally in order for the routing to be implemented.

For additional information, see the following topics:

- [“Routing Table Page” on page 167](#)
- [“Static Routes Page” on page 169](#)
- [“RIP Setup Page” on page 171](#)
- [“OSPF Setup Page” on page 174](#)

Routing Table Page

Use the Routing Table page (**Network > Routing > Routing Table**) to view all current routes on the device by IP address and subnet mask. The table displays up to 250 routes per page.

From the Routing Table page, you can do the following:

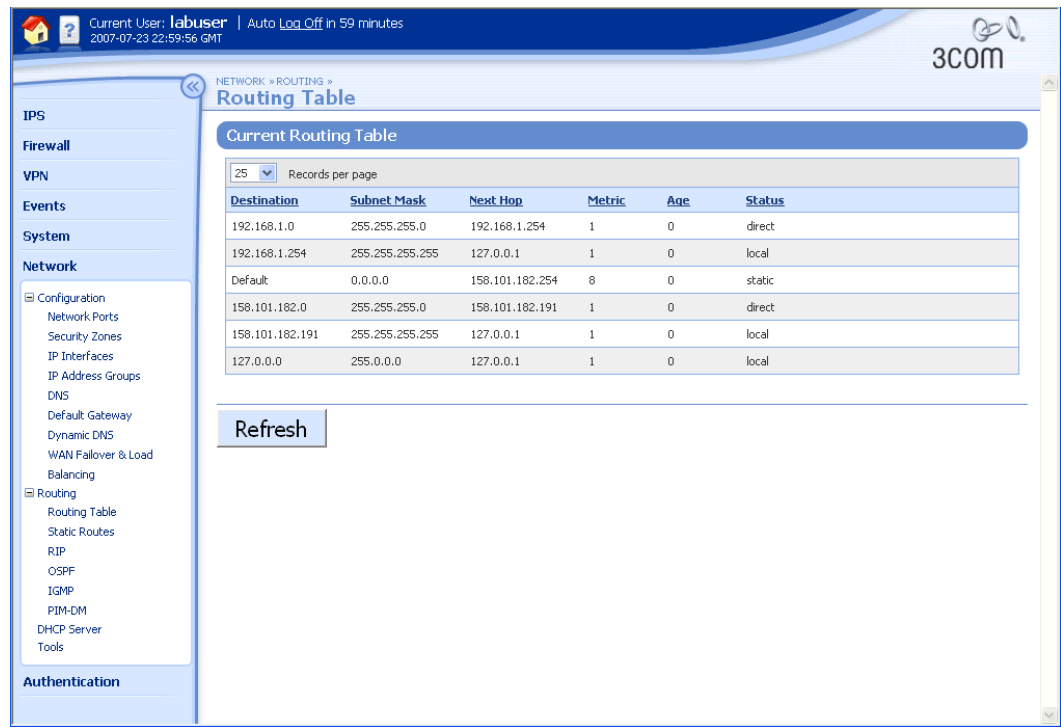
- Click on a column heading to sort the table by the specified parameter: **Destination**, **Subnet Mask**, **Next Hop**, **Metric**, **Age**, or **Status**.
- Select a **Records per page** setting to change the number of routing entries displayed in the table.
- Click **Refresh** to update the table with the most current network information.



Note Routes across a VPN are always the most specific. There is no way to configure a static route, or a route learned via RIP, to override a VPN route.

The following figure shows the Routing Table page:

Figure 6–11: Routing Table Page



The Routing Table page provides the following information:

Column	Description
Destination	The IP address of the destination network.
Subnet Mask	The subnet mask of the destination network.
Next Hop	The IP address of the router that will be used to access a host or subnet.
Metric	The number that is used to determine the order in which the static route will be accessed.

Column	Description
Age	The number of seconds since the route entry appeared in the Routing Table. For permanent routes (local, direct, and static), a hyphen (-) is displayed
Status	One of the following: <ul style="list-style-type: none"> • Static if the route is to the default destination • Local if the route is a device IP address • Direct if the route is directly attached to an IP interface on the subnet

Static Routes Page

A static route defines the gateway to use for a particular network. The device supports the use of static routes to forward traffic:

- Between the device and any external interface. For example, you may need to define a static route so that the device can communicate with the email server used to send event notifications.
- Between the device and any GRE interface.



Note Static routes configured on the device are not used to route traffic to subnets at the other end of an IPSec VPN tunnel. The destination network's configuration in the security association associated with a VPN tunnel is used for this. For more information, see [“Editing the default SA for client-to-site VPN connections using L2TP over IPSec” on page 211](#).

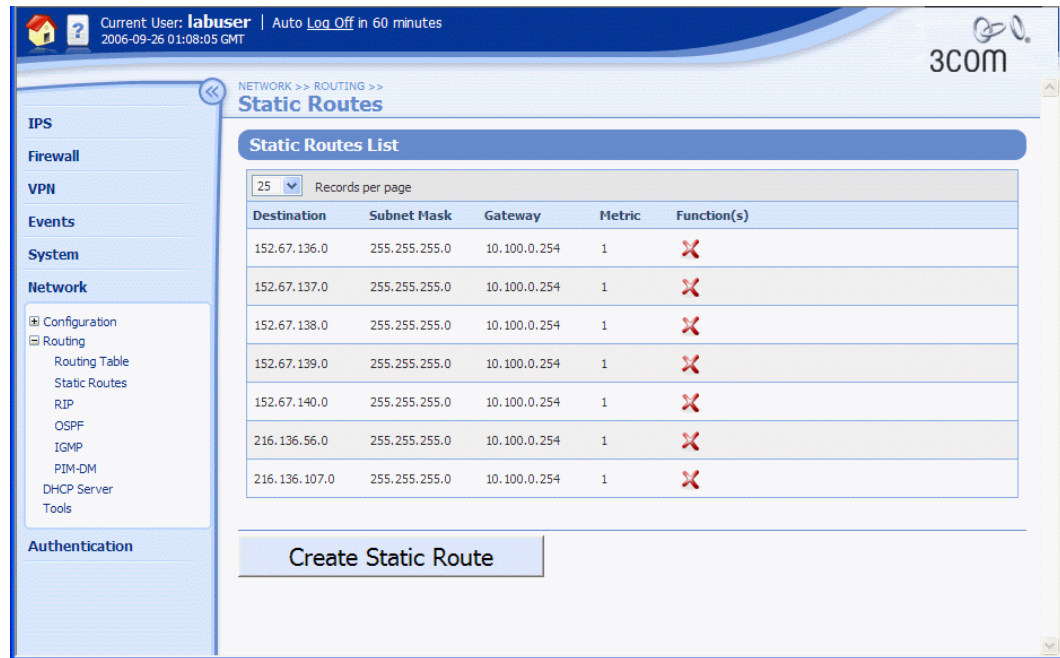
Routes across a VPN are always the most specific. There is no way to configure a static route, or a route learned via RIP, to override a VPN route.

You can view and manage static route from the Static Routes page (**Network > Routing > Static Routes**). From this page you can complete the following tasks:


- Viewing the list of existing routes
- Creating a static route
- Deleting a static route
- Changing the number of static route entries displayed in the table

The following figure shows the Static Routes page:

Figure 6–12: Static Routes Page



The Static Routes page provides the following information:

Column	Description
Destination	The IP address of the destination network for the static route
Subnet Mask	The subnet mask of the destination network
Gateway	The IP address of the device to which the device forwards traffic destined for the destination network
Metric	<p>A number (between 1 and 15) that is used to determine the order in which the static route will be accessed.</p> <p>Note By default, the device will re-distribute any static routes configured on the device into RIP. If you do not want to re-distribute some static routes, configure those with a metric of 15. The other peer routers will receive these routes, increment the metric by one (to 16). RIP routes with a metric of 16 are considered unreachable and will be discarded by the peer router.</p>
Function(s)	<p>The functions available to manage each static route listed in the table:</p> <ul style="list-style-type: none">  Delete a static route

Creating a static route

STEP 1 From the navigation pane, select **Network > Routing > Static Routes**.

The Static Routes page opens.

STEP 2 Click **Create Static Route**.

The Create Static Routes page opens.

STEP 3 Type the **IP Address** of the destination network.



Note Setting this address to 0.0.0.0 is not allowed.

STEP 4 Type the **Subnet Mask** of the destination network.

STEP 5 Type the **Gateway** IP address. (For GRE tunnels, enter the IP address for the tunnel's peer.)

STEP 6 Type the **Metric** for this route. Enter a number between 1 and 15 that represents the priority of this static route, which determines the order in which the route will be accessed. To prevent the static route from being re-distributed when RIP is enabled on the device, enter 15.

STEP 7 Click **Create** to add the static route, or **Cancel** to return to the Static Routes page without saving the changes.

RIP Setup Page

Routing Information Protocol (RIP) is used for exchanging unicast routing information between routers and hosts. Using RIP, the X family device determines a route for network packets based on the fewest number of hops between the source and the destination. RIP regularly broadcasts routing information to other devices on the network.



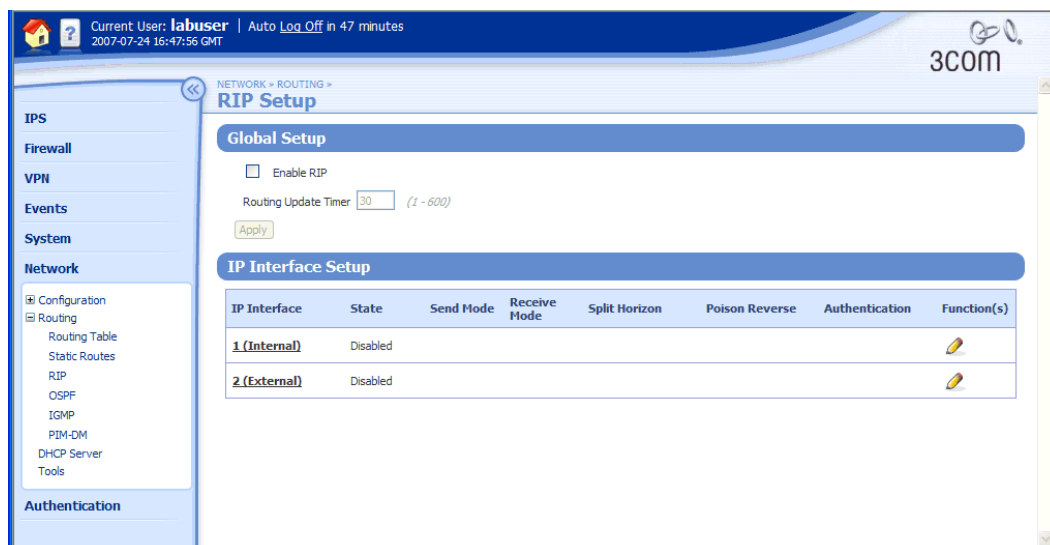
CAUTION When RIP is enabled, the device automatically re-distributes any static routes configured on the device into RIP. If you do not want to re-distribute some static routes, configure those with a metric of 15. The other peer routers will receive these routes, increment the metric by one (to 16). RIP routes with a metric of 16 are considered unreachable and will be discarded by the peer router.

You can manage and configure RIP routing from the RIP Setup page (**Network > Routing > RIP**). From this page you can complete the following tasks:

- Viewing the current RIP configuration for the device and the current state of RIP for each IP interface
- Enabling RIP globally on the device and set the routing timer
- Editing the RIP configuration for an IP interface

This following figure shows the RIP Setup page:

Figure 6–13: RIP Setup Page



On the RIP Setup page, the **IP Interface Setup** table lists the existing interfaces on the device, and provides the following information about the RIP configuration on each interface:

Column	Description
State	Whether RIP is enabled or disabled on the interface. Generally RIP should not be enabled on an external interface.
Send Mode	The mode used for broadcasting the routing information: v1 , v2 Broadcast , v2 Multicast , or Disabled .
Receive Mode	The mode used for receiving the routing information: v1 only , v2 only , v1 or v2 , or Disabled .
Split Horizon	Whether Split Horizon is enabled or disabled on the interface. Split Horizon reduces convergence time by not allowing routers to advertise networks in the direction from which those networks were learned. The announcements only include networks in the opposite direction. This also reduces loops.
Poison Reverse	Whether Poison Reverse is enabled or disabled on the interface. If Poison Reverse is enabled, routes learned from a neighbor are advertised back to it with metric 16 (unreachable). This has a similar effect as split horizon, and is also called split horizon with poison reverse. In a single-path network this has no advantage over split horizon. However, in multi-path networks this greatly reduces loops.
Authentication	The type of authentication used on the interface: none , MD5 , or Simple .
Function(s)	The functions available to manage the IP interface. Edit is the only option available.

For additional information, see the following topics:

- [“Enabling RIP globally” on page 173](#)
- [“Editing the configuration of RIP on an IP interface” on page 173](#)
- [“IP Interfaces Page” on page 142](#)

Enabling RIP globally

STEP 1 From the navigation pane, select **Network > Routing > RIP**.

The RIP Setup page opens.

STEP 2 Check **Enable RIP**. This globally enables RIP such that it can be used on any interface.



Note You must enable RIP globally to run it on any interface. Generally, you should not enable RIP on external IP interfaces.

STEP 3 In the **Routing Update Timer** field, enter a value between 1 and 600 seconds (default 30 seconds) for the interval between updates of RIP routes to neighbors.

STEP 4 Click **Apply** to save the change.

Editing the configuration of RIP on an IP interface

STEP 1 From the navigation pane, select **Network > Routing > RIP**.

The RIP Setup page opens.

STEP 2 Click the **Edit** icon for the interface you want to edit.

The Edit IP Interface page opens.

STEP 3 Near the bottom of the page, click **Show Advanced Options**.

The **IP Interface Details (Advanced)** section opens.

STEP 4 Modify the RIP configuration as required.

STEP 5 Enable Firewall Rules to allow RIP to/from *this-device* for the relevant zones.

STEP 6 Click **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

For more information on configuring interfaces, see [“Enabling bridge mode on an IP interface” on page 151](#).

OSPF Setup Page

OSPF (Open Shortest Path First) is an interior gateway protocol for large, autonomous system networks. See [Appendix C, “Device Maximum Values”](#) for device maximum configurable values.

You can manage and configure OSPF routing from the OSPF Setup page (**Network > Routing > OSPF**). From this page you can complete the following tasks:

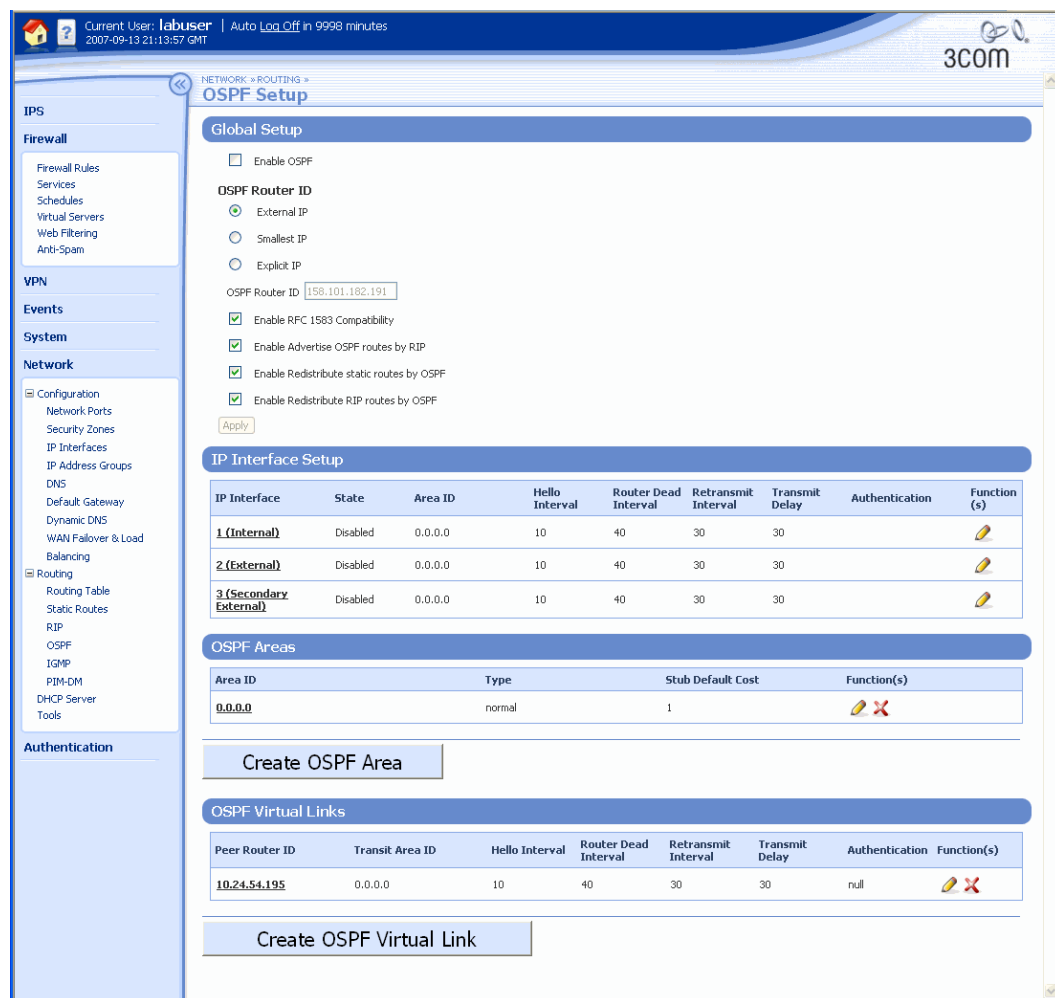
- Viewing the current OSPF configuration for the device and the current state of OSPF for each IP interface, OSPF area, and OSPF virtual link
- Enabling OSPF globally on the device and set the router ID
- Editing the OSPF configuration for an IP interface
- Creating and editing the configuration for an OSPF area
- Creating and editing the configuration for an OSPF virtual link

You must create a firewall rule to permit OSPF protocol traffic to and from the device. See [Chapter 4, “Firewall”](#) for more information.

For information on OSPF diagnostic tools, see the *CLI Reference*.

This following figure shows the OSPF Setup page:

Figure 6–14: OSPF Setup Page



On the OSPF Setup page, the **IP Interface Setup** table lists the existing interfaces on the device, and provides the following information about the OSPF configuration on each interface:

Column	Description
State	Status of the OSPF interface: Enabled or Disabled .
Area ID	The OSPF area the device is a member of.
Hello Interval	The interval (in seconds) at which the device sends out hello (“keep-alive”) packets, which signal to routers that the device is up.
Router Dead Interval	If the device receives no hello packet from its neighbor within this interval (in seconds), the device considers the neighbor down.

Column	Description
Retransmit Interval	After sending an LSA, the device waits for an acknowledgement packet. If it receives no acknowledgement when the retransmit interval elapses, it retransmits the LSA.
Transmit Delay	Transmit delay time.
Authentication	The authentication scheme used: <ul style="list-style-type: none"> • null — no authentication • simple — plain-text password authentication • crypto — encrypted password authentication (MD5)
Function(s)	The functions available to manage the IP interface. Edit is the only option available.

The **OSPF Areas** table lists the existing areas on the device, and provides the following information about the OSPF areas:

Column	Description
Type	Area type: <ul style="list-style-type: none"> • normal — area has no limitations regarding external routes • stub — receives inter-area routes, but does not receive external routes, accept external LSAs, or provide transit • nssa — Not So Stubby Area: can import autonomous system (AS) external routes and send them to the backbone, but cannot receive AS external routes from the backbone or other areas • tsa — Totally Stubby Area: does not allow summary routes or external routes
Stub Default Cost	The cost of the default route advertised to the stub or NSSA area.
Function(s)	The functions available to manage the OSPF area: Edit or Delete .

The **OSPF Virtual Links** table lists the existing virtual links on the device, and provides the following information about the OSPF virtual links on each interface:

Column	Description
Transit Area ID	ID of the area connecting the two area border routers that the virtual link will cross.
Hello Interval	Interval at which the device sends out "keep-alive" packets which signal to routers that the device is up. A value in seconds from 1 to 8192; the default is 10 seconds. This value must be identical to the value on its virtual link neighbor.

Column	Description
Router Dead Interval	If the device receives no hello packet from its neighbor within this interval (in seconds), the device considers the neighbor down.
Retransmit Interval	After sending an LSA, the device waits for an acknowledgement packet. If it receives no acknowledgement when the retransmit interval elapses, it retransmits the LSA.
Transmit Delay	Transmit delay time.
Authentication	The authentication scheme used: <ul style="list-style-type: none"> • null — no authentication • simple — plain-text password authentication • crypto — encrypted password authentication (MD5)
Function(s)	The functions available to manage the IP interface: Edit or Delete .

Enabling OSPF globally

STEP 1 From the navigation pane, select **Network > Routing > OSPF**.

The OSPF Setup page opens.

STEP 2 In the Global Setup section, check **Enable OSPF**. This globally enables OSPF such that it can be used on any interface.



Note You must enable OSPF globally to run it on any interface. Generally, you should not enable OSPF on external IP interfaces.

STEP 3 If all you are doing is enabling OSPF, click **Apply** to save the change; otherwise, continue with the procedure.

STEP 4 Select the OSPF Router ID: **External IP**, **Smallest IP**, or **Explicit IP**. If you select Explicit IP, enter the IP address in the **OSPF Router ID** field.

STEP 5 For an OSPF V2 network, check **Enable RFC 1583 Compatibility**.

STEP 6 To advertise OSPF routes using RIP, check **Enable Advertise OSPF routes by RIP**.

STEP 7 To redistribute static routes using OSPF, check **Enable Redistribute static routes by OSPF**.

STEP 8 To redistribute RIP routes using OSPF, check **Enable Redistribute RIP routes by OSPF**.

STEP 9 Click **Apply** to save the change.

Editing the configuration of OSPF on an IP interface

STEP 1 From the navigation pane, select **Network > Routing > OSPF**.

The OSPF Setup page opens.

STEP 2 Click the **Edit** icon for the interface you want to edit.

The Edit IP Interface page opens.

- STEP 3** Near the bottom of the page, click **Show Advanced Options**.
The **IP Interface Details (Advanced)** section opens.
- STEP 4** Modify the OSPF configuration as required.
- STEP 5** Enable Firewall Rules to allow OSPF to/from *this-device* for the relevant zones.
- STEP 6** Click **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

For more information on configuring the OSPF interface, see [“Enabling and configuring OSPF on an IP interface” on page 152](#).

Creating and editing the configuration for an OSPF area

- STEP 1** From the navigation pane, select **Network > Routing > OSPF**.
The OSPF Setup page opens.
- STEP 2** In the OSPF Areas section, click **Create OSPF Area**, or click the Edit icon for the area to edit.
The **Create/Edit OSPF Area** page opens.
- STEP 3** Type the **Area ID** (in IP address format). The area identifies a hierarchical set of routers that exchanges link state advertisements (LSAs).
- STEP 4** Select the **Area Type**:
- **Normal**: area has no limitations regarding external routes.
 - **Stub**: receives inter-area routes, but does not receive external routes, accept external LSAs, or provide transit. If you select Stub, also type the **Stub Default Cost** (the cost of the default route advertised to the area; the default is 1).
 - **NSSA** — Not So Stubby Area: can import autonomous system (AS) external routes and send them to the backbone, but cannot receive AS external routes from the backbone or other areas. If you select NSSA, also do the following: type the **Stub Default Cost** (the cost of the default route advertised to the area; the default is 1); check or uncheck **Enable Import summary LSAs by NSSA area**; select an NSSA Area Translator Role (**Candidate** or **Always**); and type an **NSSA Translator Stability Interval** (the default is 40 seconds).
 - **TSA**: Totally Stubby Area: does not allow summary routes or external routes. If you select TSA, also type the **Stub Default Cost** (the default is 1).
- STEP 5** In the OSPF Area Address Range Setup section, enter the **IP Subnet** and **Mask** and click **Add to table below**.
- STEP 6** Click **Save** to save the change, or **Cancel** to return to the OSPF Setup page without saving your changes.

Creating and editing the configuration for an OSPF virtual link

- STEP 1** From the navigation pane, select **Network > Routing > OSPF**.
The OSPF Setup page opens.
- STEP 2** In the OSPF Virtual Links section, click **Create OSPF Virtual Link**, or click the Edit icon for the virtual link you want to edit.
The **Create/Edit OSPF Virtual Link** page opens.

- STEP 3** Type the **Peer Router ID** (in IP address format). This is the ID of the neighboring router on the virtual link.
- STEP 4** Type the **Transit Area ID** (in IP address format). This is the ID of the area connecting the two area border routers that the virtual link will cross.
- STEP 5** Type the **Hello Interval** (from 1 to 8192 seconds; the default is 10 seconds). This is the interval at which the device sends out hello (“keep-alive”) packets, which signal to routers that the device is up. This value must be identical to the value on its virtual link neighbor. The smaller the hello interval, the faster the network converges, but the more network resources are consumed.
- STEP 6** Type the **Router Dead Interval** in seconds (the default is 40 seconds). If the device receives no hello packet from its neighbor within this interval, the device considers the neighbor down. The dead interval should be at least four times the hello interval.



Note Any two routers attached to the same segment must have the same dead interval.

- STEP 7** Type the **Retransmit Interval** in seconds (the default is 30 seconds). After sending an LSA, the device waits for an acknowledgement packet. If it receives no acknowledgement within the retransmit interval, it retransmits the LSA. Increase the value for WAN links if the default causes unnecessary retransmissions.
- STEP 8** Type the **Transmit Delay** in seconds; the default is 30 seconds. Increase the value for WAN links if the default causes a problem.
- STEP 9** Select the **OSPF v2 Authentication** type:
- **Null** (no authentication used).
 - If you select **Simple** (plain-text password) or **Crypto** (encrypted password), also type the **OSPF key** (which is not displayed) and the **OSPF Key ID** (which is displayed). The authentication key is a password (up to 8 characters) which can be assigned on an interface basis. The authentication key must match that of each router on the interface.
- STEP 10** Click **Save** to save the change, or **Cancel** to return to the OSPF Setup page without saving your changes.

Troubleshooting OSPF Configurations

The following sections describe some common OSPF configuration problems and how to solve them.

No OSPF Neighbor Relationship Established

Symptom: No OSPF neighbor relationship can be established.

Analysis: If the physical link and lower layer protocols work well, check OSPF parameters configured on the device. Two neighbor routers must have the same parameters, such as the area ID, network segment, mask (a virtual link can have different network segments and masks), Hello Interval, and Router Dead Interval.

Solution:

1. Use the OSPF Setup page (**Network > Routing > OSPF**) to display neighbors and OSPF interface information. (For more information, see [“OSPF Setup Page” on page 174.](#))
2. Ping the neighbor router’s IP address to check connectivity. (For more information, see [“Pinging a device” on page 195.](#))
3. Check OSPF timer configuration. (For more information, see [“Enabling and configuring OSPF on an IP interface” on page 152.](#)) The Router Dead Interval on an interface must be at least four times the Hello Interval.

Incorrect Routing Information

Symptom: OSPF cannot find routes to other areas.

Analysis: The backbone area must maintain connectivity to all other areas. If a router connects to more than one area, at least one area must be connected to the backbone. The backbone cannot be configured as a stub area. In a stub area, all routers cannot receive external routes, and all interfaces connected to the stub area must be associated with the stub area.

Solution:

1. Use the CLI interface to display neighbors and OSPF routing diagnostic information. (For more information, see the *CLI Reference*.) If more than two areas are configured, at least one area must be connected to the backbone.
2. Check the state of the virtual link.

Multicast Routing (IGMP and PIM-DM)

The X family device can act as an IP multicast router, supporting IGMP and PIM-DM multicast protocols.

- **IGMP — Internet Group Management Protocol**, used by hosts to define multicast group membership. Multicast groups are identified by special IP addresses.
IGMP must be enabled on all IP interfaces that are directly connected to clients using multicast traffic.
- **PIM-DM — Protocol Independent Multicast-Dense Mode** routing protocol, used for multicast routing between remote sites. PIM-DM is also used to support site-to-site NBX conference calls.
PIM-DM must be enabled on all IP interfaces that multicast data will travel through to or from the multicast clients. This includes the GRE and IP interfaces.



Note Firewall rules must be established to allow PIM-DM and IGMP to be passed through the firewall between each set of security zone pairs that the multicast traffic must traverse. This includes between virtual zones such as a VPN zone and this-device.

IGMP Setup Page

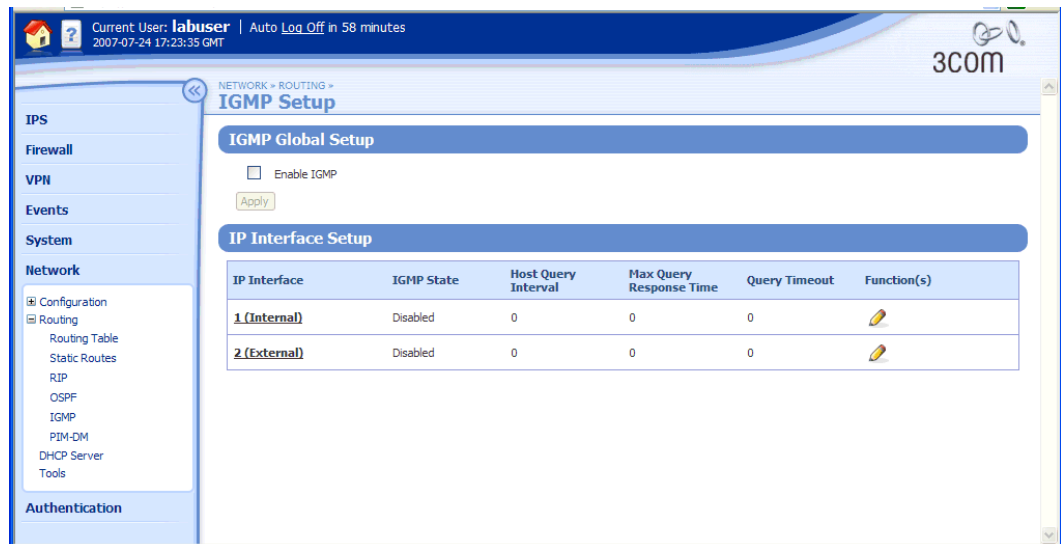
Internet Group Management Protocol (IGMP) is used by hosts to join or leave multicast groups.

You can manage and configure IGMP routing from the IGMP Setup page (**Network > Routing > IGMP**). From this page you can complete the following tasks:

- Viewing the current IGMP configuration for the device and the current state of IGMP for each IP interface
- Configuring the global IGMP setup parameters for the device
- Editing the IGMP configuration for an IP interface

This following figure shows the IGMP Setup page:

Figure 6–15: IGMP Setup Page



On the IGMP Setup page, the **IP Interface Setup** table lists the existing interfaces on the device, and provides the following information about the IGMP configuration on each interface:

Column	Description
IGMP State	Whether IGMP is enabled or disabled on this IP interface.
Host Query Interval	Interval in seconds between queries from the IGMP querier router to multicast groups. Default interval is 125 seconds.
Max Query Response Time	Maximum time that the querier waits for a response from the host.
Query Timeout	Length of time that the interface waits for a query from the host before it becomes the querier. Default is double the Host Query Interval.

Column	Description
Function(s)	The functions available to manage the IP interface. Edit is the only option available.

For additional information, see the following topics:

- [“Enabling IGMP globally” on page 182](#)
- [“Editing the IGMP configuration on an IP interface” on page 182](#)
- [“Enabling PIM-DM globally” on page 183](#)
- [“Editing the PIM-DM configuration on an IP interface” on page 184](#)
- [“Setting up site-to-site multicasting” on page 184](#)
- [“IP Interfaces Page” on page 142](#)

Enabling IGMP globally

STEP 1 From the navigation pane, select **Network > Routing > IGMP**.

The IGMP Setup page opens.

STEP 2 Check **Enable IGMP**.



Note You must enable IGMP globally in order to run it on an interface.

STEP 3 Click **Apply** to save the change.

Editing the IGMP configuration on an IP interface

STEP 1 From the navigation pane, select **Network > Routing > IGMP**.

The IGMP Setup page opens.

STEP 2 In the **IP Interface Setup** table, click the **Edit** icon for the interface you want to edit.

The Edit IP Interface page opens.

STEP 3 Edit the configuration for the interface.

STEP 4 Enable firewall Permit rules to allow IGMP to or from *this-device* for the relevant zones.

STEP 5 Click **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

For more information on configuring interfaces, see [“Enabling multicasting on an IP interface” on page 156](#).

PIM-DM Setup Page

Protocol Independent Multicast-Dense Mode (PIM-DM) is used for multicast routing between remote sites. You can manage and configure PIM-DM routing from the PIM-DM Setup page (**Network > Routing > PIM-DM**). The IP Interfaces Setup table lists the existing IP interfaces on the device, and indicates whether PIM-DM is enabled or disabled on this IP interface. From this page you can complete the following tasks:

- Viewing the current PIM-DM configuration for the device and the current state of PIM-DM for each IP interface.
- Configuring the global PIM-DM setup parameters for the device.
PIM-DM must be enabled on interfaces that are connected to another multicast router that separates the device from clients using multicast traffic.
- Editing the PIM-DM configuration for an IP interface.

This following figure shows the PIM-DM Setup page:

Figure 6–16: PIM-DM Setup Page

The screenshot shows the PIM-DM Setup page in a web interface. The page has a navigation pane on the left with categories like IPS, Firewall, VPN, Events, System, Network, and Authentication. The main content area is titled 'PIM-DM Setup' and is divided into two sections: 'PIM-DM Global Setup' and 'IP Interface Setup'.

PIM-DM Global Setup

- Enable PIM-DM
- Query Interval**: 30 seconds
- Prune Timeout**: 180 seconds
-

IP Interface Setup

IP Interface	PIM-DM State	Function(s)
1 (Internal)	Disabled	
2 (External)	Disabled	

Enabling PIM-DM globally

STEP 1 From the navigation pane, select **Network > Routing > PIM-DM**.

The PIM-DM Setup page opens.

STEP 2 In the PIM-DM Global Setup section, check **Enable PIM-DM**.



Note You must enable PIM-DM globally to run it on an interface.

STEP 3 Enter a value between 1 and 600 seconds (default 30 seconds) in the **Query Interval** field.

- STEP 4** Optionally, enter a value between 1 and 900 seconds (default 180 seconds) in the **Prune Timeout** field.

Prune Timeout alleviates some PIM-DM flood problems. A prune delay is introduced, allowing the first multicast packet to flood to all sites. Subsequent multicast packets to that multicast group are then dropped until most prunes have returned from remote devices, when the multicast stream is released again.

- STEP 5** Click **Apply** to save the change.

Editing the PIM-DM configuration on an IP interface

- STEP 1** From the navigation pane, select **Network > Routing > PIM-DM**.

The PIM-DM Setup page opens.

- STEP 2** In the **IP Interface Setup** table, click the **Edit** icon for the interface you want to edit. Then, configure PIM-DM for the interface.

- STEP 3** Enable firewall Permit rules to allow PIM-DM to/from *this-device* for the relevant zones.

- STEP 4** Click **Save**, or **Cancel** to return to the IP Interfaces page without saving the changes.

Setting up site-to-site multicasting

- STEP 1** From the LSM menu select **Network > Routing > IGMP**.

The IGMP Setup page opens.

- STEP 2** Check **Enable IGMP**.

- STEP 3** Click **Save**.

- STEP 4** From the navigation pane, select **Network > Routing > PIM-DM**.

The PIM-DM Setup page opens.

- STEP 5** Check **Enable IGMP**.

- STEP 6** Click **Save**.

- STEP 7** Create a GRE Interface. (For details, see [“Configuring a secure GRE tunnel to a remote device” on page 150](#).) In the **Advanced Options** section, check **Enable PIM-DM**.

For more information on configuring interfaces, see [“Enabling multicasting on an IP interface” on page 156](#).

DHCP Server

A DHCP server allows computers on your network to obtain an IP address and subnet mask automatically. DHCP assigns a temporary IP address and subnet mask to any PC that requires IP configuration information. When a PC with a DHCP-assigned address disconnects from the network, the address is released and can be reassigned.

You can configure the X family device to act as a DHCP server for devices on its LAN-side interfaces (internal IP interfaces) that require IP configuration. The following pages (**Network > DHCP Server**) are available to manage and configure DHCP settings:

- **DHCP Server** — View the current status of DHCP leases and a list of current DHCP clients.
- **Static Reservations** — Create and manage static mappings on the device. A static mapping is used to assign a specific IP address to a device such as a printer or DNS server.
- **DHCP Relay** — Enable and configure the DHCP Relay option on the device.
- **Configure DHCP** — Enable the DHCP server option and configure the settings.

For additional information, see the following topics:

- [“DHCP Server Page” on page 185](#)
- [“Configuring the DHCP Server” on page 187](#)
- [“DHCP Relay Page” on page 189](#)
- [“Static Reservations Page” on page 191](#)

To use the X family device as your network’s DHCP server:

1. Configure the pool of available IP addresses for DHCP clients — you can specify this as an IP range, an IP subnet, or an IP address group.
2. Configure DNS settings — you can configure the device to override the default DNS settings providing the IP addresses of up to three DNS Servers. If you do not choose to override DNS, the clients will automatically be configured to use the device as the DNS server. The device will then forward DNS requests to the DNS servers that were automatically obtained or configured on the external interface.
3. Optionally, provide the IP addresses of up to two WINS servers for use by the client. If you have a WINS server on your network enter its IP address in the **WINS Server** box. The device will pass this information on to all Windows PCs that obtain an address from its DHCP server.
4. Ensure that the firewall policies configured on the device allow DHCP clients to send DHCP requests to the correct security zone and to receive their IP address by DHCP.

DHCP Server Page

A DHCP server leases IP addresses to DHCP clients. If a lease has not been released normally, you can release it manually. By default, the device DHCP server grants leases for one hour. You can edit the duration of the lease on the Configure DHCP page. If you are running short of addresses in the DHCP pool and know that some computers are unlikely to connect to the network soon, you can release their IP addresses, allowing them to be reallocated to other systems.


DHCP lease assignments are generally stable even if the client (PC) or server (X family device) is rebooted. The client usually gets the same DHCP lease when the server comes back online unless that is prevented for some reason (for example, all the leases are used up or the lease in question is otherwise in use).

Use the DHCP Server page to complete the following tasks:

- Viewing current and available leases
- Viewing a list of current clients with DHCP-allocated addresses
- Releasing a client IP address so that the IP address can be reallocated
- Accessing the functions to manage static reservations, DHCP relay, and DHCP configuration

The **DHCP Client Summary** table provides the following information about the status of current DHCP client leases:

Table 6–5: Network: DHCP Server Details

Column	Description
IP Address	The IP address assigned from the DHCP address pool
Hostname	The host name of the client
MAC Address	The MAC address of the client
Type	<ul style="list-style-type: none"> • Dynamic for a lease from the DHCP Address Pool • Static if Static Mapping has been applied • Dynamic (BOOTP) for a BOOTP client
Function(s) 	The available functions for DHCP Clients: <ul style="list-style-type: none"> • Release the client so that the DHCP address can be reallocated

Releasing a DHCP lease

If you are running short of addresses in the DHCP pool and you know of computers that are unlikely to connect to your network soon, you can release the IP address allowing it to be reallocated to another PC.

STEP 1 From the navigation pane, select **Network > DHCP Server**.

The DHCP Server page opens.

STEP 2 In the **DHCP Client Summary** table, click the **Release** icon to end the lease and update the table.

Configuring the DHCP Server

You can configure the X family device to be your DHCP server, thereby allowing computers on your network to obtain an IP address and subnet mask automatically.



Note Ensure that the firewall rules configured on the device allow DHCP clients to send DHCP requests to the correct security zone and to receive their IP address by DHCP. For details, see [“Firewall” on page 59](#).

Default DHCP Configuration

The DHCP server is enabled by default and configured with the default IP address group DHCP-Pool, which includes 20 IP addresses in the subnet defined for the internal IP interface. These DHCP addresses are 192.168.1.1–192.168.1.20. The default lease duration is one hour. You can disable the DHCP server or modify the default configuration based on your network requirements.

You can view and manage the DHCP configuration on the DHCP Configuration page (**Network > DHCP Server**, click **Configure DHCP** tab). From this page, you can complete the following tasks:

- Enabling or disabling DHCP
- Changing the lease duration
- Configuring the DHCP address pool from which the device allocates addresses
- Selecting DHCP server options for DNS, WINS, NBX, and VCX services

Enabling and configuring the DHCP server

STEP 1 From the navigation pane, select **Network > DHCP Server**.

The DHCP Server page opens.

STEP 2 Click the **Configure DHCP** tab.

The Configure DHCP Server page opens.

STEP 3 Check **Enable DHCP Server** to enable the DHCP server. Then, configure the following options as required:

- In the **Lease Duration** field, enter a value between 1 and 600 minutes (default 60 minutes) for the duration of the lease to the DHCP client.
- Check **Allow BOOTP clients** if you want the device DHCP server to respond to lease requests from BOOTP clients.



Note Do not check **Allow BOOTP clients** if some LAN devices use the BOOTP protocol to retrieve their operating system or firmware from a separate BOOTP server.

STEP 4 In the **DHCP Address Pool** table, configure IP address pool options:

- To use an IP address group, select **IP Address Group**. Then, select an existing group from the drop-down list.
- To use a subnet, check **IP Subnet**. Then, type the subnet IP address and **Mask**.
- To use a range of IP addresses, check **IP Range**. Then, type the beginning and end of the address range.

- STEP 5** To allow the device to provide the DHCP clients with different DNS server IP addresses than those configured on the device, check **Override Default DNS Settings**. DNS settings are configured and managed from the **Network > Configuration > DNS** menu option.
- STEP 6** Optionally, in the **WINS Servers** fields, type the IP addresses of up to two WINS servers for use by the client if you are using Windows networking.
- STEP 7** Optionally, in the **NBX NCP** field, type the NBX network call processor (NCP) IP address if you want to allow NBX phones to retrieve the NCP IP address.
- STEP 8** Click **Apply** to save the changes.



Note Ensure that the firewall rules configured on the device allow DHCP clients to send DHCP requests to the correct security zone and to receive their IP address by DHCP. For details, see [“Firewall” on page 59](#).

Disabling the DHCP server

- STEP 1** From the navigation pane, select **Network > DHCP Server**.
The DHCP Server page opens.
- STEP 2** Click the **Configure DHCP** tab.
The Configure DHCP Server page opens.
- STEP 3** Clear the **Enable DHCP Server** checkbox.
- STEP 4** Click **Apply** to save the changes.

Editing the duration of a DHCP lease

The DHCP Server will attempt to supply a computer with the same lease as was issued previously, even if that lease has expired. Expired leases are only reused when there are no free leases available. When an expired lease is re-issued, the oldest lease that is not a fixed association is used.

- STEP 1** From the navigation pane, select **Network > DHCP Server**.
The DHCP Server page opens.
- STEP 2** Click the **Configure DHCP** tab.
The Configure DHCP Server page opens.
- STEP 3** Change the value in the **Lease Duration** field (the default is 60 minutes).
- STEP 4** Click **Apply** to save the changes.

DHCP Relay Page

DHCP relay allows DHCP to operate between a DHCP client on one security zone and a DHCP server on another. To use DHCP relay, you configure the X family device to act as a DHCP relay agent. The device will relay DHCP packets to the destination DHCP server and back to the client across security zone boundaries. This enables DHCP clients on different networks to use the same DHCP server.



Note To use DHCP relay, you must disable the DHCP server. See [“Disabling the DHCP server” on page 188](#) for more information.

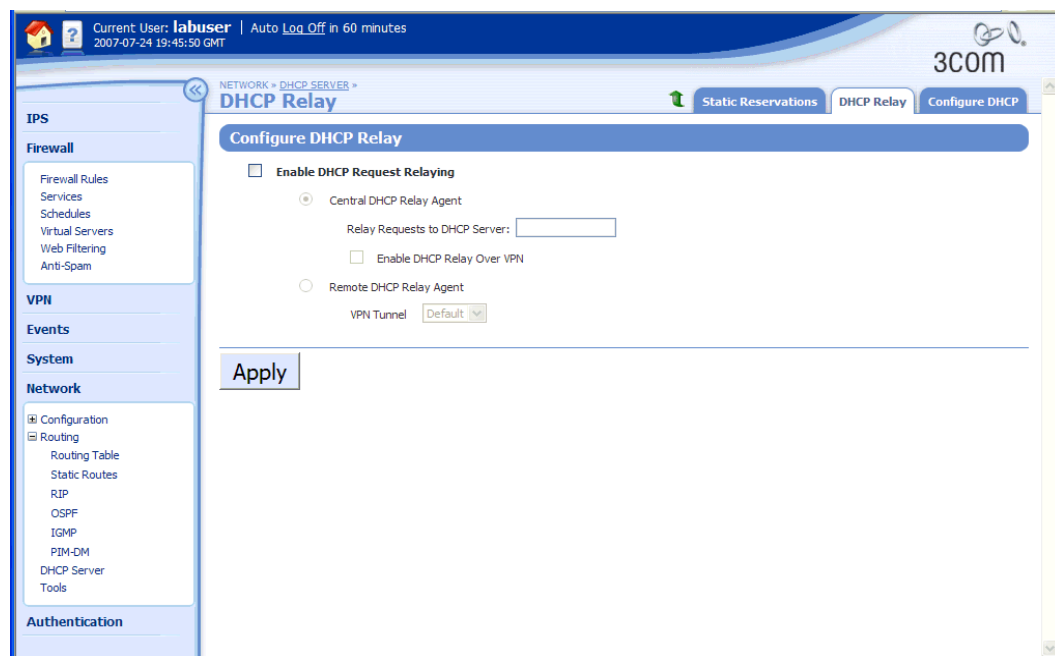
Configuring DHCP Relay

You can configure DHCP relays from the DHCP Relay page (**Network > DHCP Server**, click **DHCP Relay** tab). From this page, you can complete the following tasks:

- Enabling or disabling the DHCP relay option
- Configuring the device as a central DHCP agent with or without the Relay Over VPN option
- Configuring the device as a remote DHCP relay agent

The following figure shows the DHCP Relay page:

Figure 6–17: DHCP Server: DHCP Relay Page



The following table shows the configuration parameters to set up DHCP relay:

Table 6–6: Network: DHCP Relay Configuration Parameters

Parameter	Description
Enable DHCP Request Relaying	Select this option to enable DHCP relay. You must disable the DHCP server before using this feature.
Central DHCP Relay Agent	Select this option if the device is directly connected to a network that contains the DHCP server (that is, the device is in the head office next to the DHCP server). In this configuration, the device receives requests from remote agents (possibly X family devices) and forwards them to the DHCP server on its LAN.
Relay Requests to DHCP Server	The IP address of the central DHCP server where requests are sent.
Enable DHCP Relay Over VPN	For a central DHCP relay agent, selecting this checkbox allows the device to act as a VPN relay agent and supports DHCP requests arriving over VPN tunnels using IKE. The device will forward the requests to the DHCP server.
Remote DHCP Relay Agent	Select this option if the device is connected to a client network that sends DHCP lease requests. In this configuration, the device listens for DHCP requests from its LAN. This option is recommended for an device in a remote office that is relaying DHCP requests to a central DHCP server in the head office.
VPN Tunnel	If Remote DHCP Relay Agent is selected, this parameter identifies the VPN tunnel the device uses to pass DHCP requests to the central DHCP relay agent.



Note If you are using **DHCP Relay over VPN**, any LAN devices attached to the remote VPN relay agent that are not using DHCP must be configured as static reservations. (See [“Static Reservations Page” on page 191](#)). To configure, navigate to **Network > DHCP Server**. Then, select the Static Reservations page.

You can only use DHCP Relay Over VPN when the VPN between two devices is configured to use Internet Key Exchange (IKE).

Configuring DHCP relay as a central DHCP relay in the main office

- STEP 1** From the navigation pane, select **Network > DHCP Server**.
The DHCP Server page opens.
- STEP 2** Click the **DHCP Relay** tab.
The DHCP Relay page opens.
- STEP 3** Check **Enable DHCP Request Relaying** to enable DHCP relay.
- STEP 4** Check **Central DHCP Relay**. With this configuration, the device is configured to receive requests from a remote agent which are then forwarded to the DHCP server on its LAN.

STEP 5 In the **Relay Requests to DHCP Server** field, type the address of the central DHCP server.

STEP 6 If you want the device to act as a central VPN relay agent, check **Enable DHCP Relay over VPN**.



Note Make sure that the tunnels connecting to the device configured as the remote VPN relay agent are configured as **Destination network addresses assigned by DHCP** in the **Tunnel Setup** section of the Create Security IPSec Configuration page.

STEP 7 Click **Apply** to save the configuration.

Configuring the DHCP relay mode as remote VPN relay agent

STEP 1 From the navigation pane, select **Network > DHCP Server**.

The DHCP Server page opens.

STEP 2 Click the **DHCP Relay** tab.

The DHCP Relay page opens.

STEP 3 Check **Enable DHCP Request Relaying** to enable DHCP relay.

STEP 4 Check **Remote DHCP Relay Agent**. With this configuration, the device listens for DHCP requests from its LAN and forwards them to a central DHCP relay.

STEP 5 From the **VPN Tunnel** drop-down list, select the tunnel that will be used to relay the requests from the remote DHCP Relay agent to the central DHCP relay agent.



Note If the VPN Tunnel list is empty, navigate to **VPN > IPSec/IKE Status** and configure an IPSec tunnel.

STEP 6 Click **Apply** to save the configuration.

Static Reservations Page

Static reservations let you assign a particular IP address to a device such as a printer or DNS server. You can create and manage static reservations from the Static Reservations page (**Network > DHCP Server**). From this page, you can complete the following tasks:

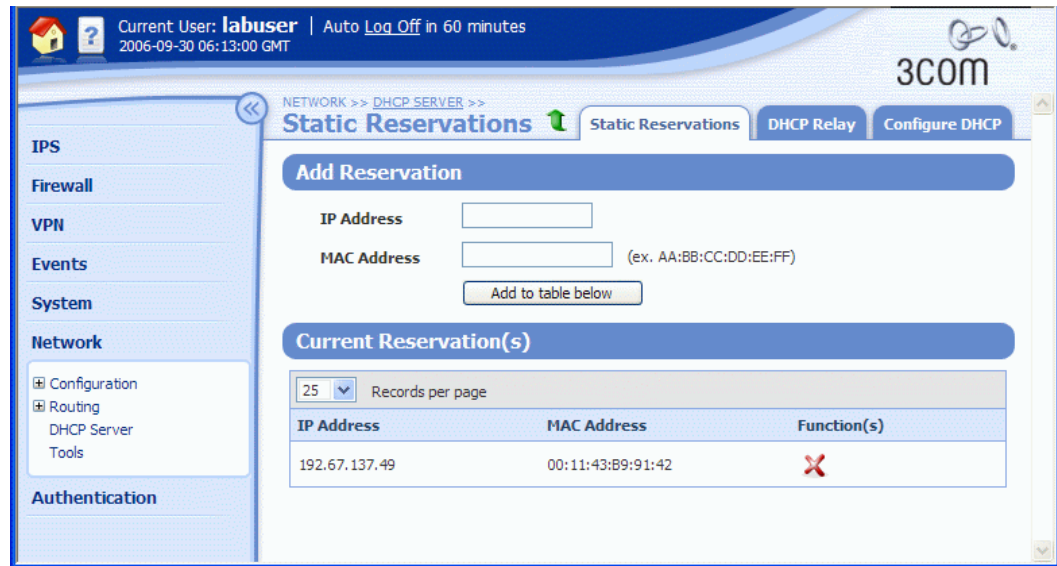
- Viewing a list of current static reservations
- Creating a new reservation
- Deleting a reservation



Note If you are using [DHCP Relay Page](#), any LAN devices attached to the remote VPN relay agent that are not using DHCP must be configured as static mappings.

The following figure shows the Static Reservations page:

Figure 6–18: Static Reservations Page



The **Current Reservation(s)** table provides the following information for each static reservation:

Table 6–7: Static Reservation Details

Column	Description
IP Address	The IP address you want to assign to the device
MAC Address	The MAC address of the device
Function(s): ✘	The available functions for static reservations: <ul style="list-style-type: none"> Delete a static reservation

Adding a static reservation

- STEP 1** From the navigation pane, select **Network > DHCP Server**.
The DHCP Server page opens.
- STEP 2** Click the **Static Reservations** tab.
The Static Reservations page opens.
- STEP 3** Type the **IP Address** you want to assign to the device.
- STEP 4** Type the **MAC Address** for the device.
- STEP 5** Click **Add to table below** to update the **Current Reservations** table.
- STEP 6** Repeat Steps 3 to 5 to add reservations to the table as required.

See [Appendix C, “Device Maximum Values”](#) for information on the maximum number of reservations your device supports.

Network Tools

The LSM provides the following network tools:

- **DNS Lookup** — Displays the IP address for a given DNS name.
- **Find Network Path** — Displays the physical interface/security zone (and router IP address if appropriate) that the X family device would use to reach a given location.
- **Traffic Capture** — Lets you capture network packets into a file. This is useful for analyzing the type of traffic flowing through the device.
- **Ping** — Lets you send out ping requests to test whether devices on an IP network are accessible and functioning correctly. This feature helps diagnose connectivity problems such as a failed network device between the device and the Web server being accessed, or to help diagnose DNS setup problems.
- **Traceroute** — Lets you display the network hops from the device to another device on an IP network. This is useful for network troubleshooting.

For additional information, see the following topics:

- [“DNS Lookup” on page 193](#)
- [“Find Network Path” on page 194](#)
- [“Traffic Capture” on page 194](#)
- [“Ping” on page 195](#)
- [“Traceroute” on page 196](#)

DNS Lookup

Use the DNS Lookup tool to find the IP address for a given DNS name (or vice versa). DNS lookup can be used to verify that the DNS servers on the device are configured properly.

Finding the IP address for a DNS name

STEP 1 From the navigation pane, select **Network > Tools**.

The TOOLS page opens.

STEP 2 In the **DNS Lookup** section, type the **Hostname** or the **IP Address**.

STEP 3 Click **Lookup**.

The page displays the IP address or alias as appropriate.

Find Network Path

Use the **Find Network Path** tool to display the security zone or tunnel name (and router IP address if appropriate) that the X family device would use to reach a given location.

Finding a network path

STEP 1 From the navigation pane, select **Network > Tools**.

The TOOLS page opens.

STEP 2 In the **Find Network Path** section, type the hostname or IP address of the device to which you want to find the network path.

STEP 3 Click **Find**.

The Find Network Path page opens, showing the name of the security zone or tunnel the device uses to contact the specified destination. If the device cannot resolve the specified destination, `Unknown host` displays.

The device uses the routing table to determine where to send a packet destined for this address.

Traffic Capture

Use the **Traffic Capture** tool to capture network packets in a file. This is useful for analyzing the type of traffic flowing through the device.

From the Traffic Capture page, you can complete the following tasks:

- Viewing and managing existing packet capture files
- Capturing packets

Viewing and managing packet capture files

STEP 1 From the navigation pane, select **Network > Tools**.

The TOOLS page opens.

STEP 2 Click the **Traffic Capture** tab.

The Traffic Capture page opens.

STEP 3 Click **Create Capture File**.

The Create Traffic Capture page opens.

- To stop capturing traffic, click the Stop icon.
- To delete a capture file, click the Delete icon. You are prompted to verify the deletion; click OK.
- To download a capture file, click the Stop icon and then click the Save icon. The standard browser download window opens; click Save.

Capturing packets

- STEP 1** From the navigation pane, select **Network > Tools**.
- The TOOLS page opens.
- STEP 1** Click the **Traffic Capture** tab.
- The Traffic Capture page opens.
- STEP 2** Click **Create Capture File**.
- The Create Traffic Capture page opens.
- STEP 3** Specify the Capture File Details:
- STEP A** Enter a file name.
- STEP B** If required, change the settings for the **Max File Size** (the upper limit is 10000000) and the **Max Packets** (the upper limit is 10000).
- STEP C** Select the **Security Zone Pair** on which you want to capture traffic.
- STEP 4** Optionally, to further specify which packets to include in the capture, enter the IP protocol and source/destination addresses parameters in the **Capture Filter** section.
- STEP 5** Click **Start Capture**.

Ping

Use the **Ping** tool to send ping requests to test whether devices on an IP network are accessible and functioning correctly. The ping tool can help diagnose connectivity problems such as a failed network device between the X family device and the Web server being accessed, or to help diagnose DNS setup problems.

Ensure that the firewall rules configured on the X family device allow the security zone to send Ping (ICMP) requests. The following table shows a firewall rule allowing Ping requests between zones to be sent to the destination zone and the response to be allowed back to the source zone:

Table 6–8: Example Firewall Rule — Allowing the Device to Ping Devices in LAN Security Zone

Action	Service	Source zone	Destination zone	Destination IP
Permit	ICMP Ping	This Device	LAN	ANY



Note Some network environments block Ping traffic on the network. The Ping request can therefore fail even if the network device is operating normally.

Pinging a device

- STEP 1** From the navigation pane, select **Network > Tools**.
- The TOOLS page opens.

STEP 1 Click the **Ping** tab.

The Ping page opens.

STEP 2 In the **Ping Configuration** section, type the host name or IP address for the device that you want to ping.

STEP 3 If required, configure any of the following options:

- **Inter Packet Interval** — The number of seconds between each packet.
- **TTL (IP Time To Live)** — The maximum number of IP routers that the packet can go through before being thrown away. Each router will decrease the TTL value on the packet by one. The maximum value is 255.
- **Number Of Packets** — The number of packets you want to send. (default 4)
- **Record Route** — The route the packet took through the network/Internet. Some routers will add their address to the packet if you check this option.
- **Perform Reverse Lookup on Results** — If you locate a domain name, this function returns the IP address. If you have located an IP address, this returns the domain name.
- **Silent** — Do not display any extra information.
- **Verbose** — More details about the ping will be displayed if you check this option.



Note To reset the Ping Configuration default values, click **Defaults**.

STEP 4 Click **Start Ping**.

The ping request is sent to the specified system.

If the system is accessible and functioning correctly, a message similar to the following is displayed:

```
64 bytes from 192.168.1.254: icmp_seq=0 ttl=248 time=195.2 ms
```

If the system is not accessible, or is not functioning correctly, a message similar to the following is displayed:

```
No answer from 192.168.1.254
```

Some network environments block ping traffic on the network. The ping request may therefore fail even if the network device is operating normally.

Traceroute

Use the **Traceroute** tool to display the network hops from the X family device to another device on an IP network. This feature is useful to diagnose connectivity problems such as a failed network device between the X family device and the Web server being accessed.

Tracing a route

STEP 1 From the navigation pane, select **Network > Tools**.

The TOOLS page opens.

STEP 1 Click the **Traceroute** tab.

The Traceroute page opens.

STEP 2 In the **Traceroute Configuration** section, type the host name or IP address of the destination device to which you want to trace the route.

STEP 3 Configure any of the following options:

- **First Hop** — You can choose which is the first hop that you get information about. For example, if you already know about the first four hops, enter 5.
- **Probe Type** — Select the communications protocol or the traceroute: **UDP** or **ICMP**.
- **Max Hops** — The maximum number of hops for the traceroute.
- **Print Name** — Whether or not you want the traceroute to query and display the DNS names of the routers.
- **Port Base** — The port number from which the packet is sent. You cannot change the default value (33434).
- **Max Number of Timeouts** — The maximum number of timeouts after which the traceroute stops.
- **Number Of Queries** — The number of packets that will be sent to each hop.
- **Max Wait** — The maximum time in milliseconds the traceroute will wait for a response from the destination host before stopping. (The default is 1000 ms or one second.)

STEP 4 Click **Start Traceroute**. The device sends a traceroute request to the specified device and a message similar to the following is displayed:

```
traceroute to 192.168.1.251, 30 hops max, 38 byte packets
```

If the device is accessible and functioning correctly, a message similar to the following is displayed which displays the network hops. Each hop may take a few seconds to complete:

```
1.router1 (192.168.1.252) 1.292ms, 1.343ms, 1.810ms
2.router2 (192.168.1.253) 26.027ms, 27.156ms, 44.902ms
3.router3 (192.168.1.254) 24.323ms, 24.854ms, 30.096ms
4.router4 (192.168.1.255) 27.303ms, 33.639ms
```

If the device is not accessible, or is not functioning correctly, only the hops that worked are displayed.



Note Some network environments block traceroute traffic on the network. The Traceroute request can therefore fail even if the network device is operating normally.

7 VPN

The VPN section provides an overview of Virtual Private Networks and describes how they are implemented.

Overview

The VPN menu pages let you configure the protocol and authentication method for Virtual Private Network (VPN) tunnels so that remote users and devices can access the X family device. The following menu options are available:

- **IPSec Status** — View and manage IPSec configurations. This page also provides access to the IPSec Configuration page to enable and configure IPSec and to manage the IPSec security associations. Use this option when you are configuring a site-to-site VPN connection, or a client-to-site connection that relies on the IPSec or L2TP over IPSec tunneling protocol.
- **IKE Proposal** — View, set up, or modify configurations for IKE phase 1 and phase 2. Use this option if you want to use IKE as the keying mode to negotiate an IPSec or L2TP over IPSec VPN connection.
- **L2TP Status** — View current L2TP connections or configure the device to act as an L2TP server. Use this option for client-to-site connections that use L2TP or L2TP over IPSec.
- **PPTP Status** — View current PPTP connections, configure the device to act as a PPTP server. Use this option for client-to-site connections to support remote users. The PPTP protocol is the least secure method for VPN connections.

Before using the available menu options, review the VPN chapter in the *Concepts Guide*.

For additional information, see the following topics:

- [“VPN Configuration Overview” on page 200](#)
- [“IPSec Configuration” on page 201](#)
- [“IKE Proposal” on page 215](#)
- [“L2TP Configuration” on page 225](#)
- [“Configuring Client-to-Site VPNs for Windows Clients” on page 232](#)
- [“PPTP Configuration” on page 236](#)

VPN Configuration Overview

The VPN setup process consists of the following steps:

1. Install the high-encryption service pack on the device.
By default, all new devices are supplied with 56-bit DES encryption only. To enable the strong encryption functionality (3DES, 128-AES, 192-AES, 256-AES) required to create secure VPN connections, install the correct Strong Encryption Service Pack for your device, available from the TMC Web site.
2. Decide whether you require a site-to-site or client-to-site VPN connection.
For client-to-site VPNs, determine whether you will use the PPTP, L2TP, or L2TP over IPSec tunneling protocol. PPTP and L2TP are not recommended because they are not very secure.
For site-to-site VPN connections, you must use the IPSec protocol. For authentication, you can use either X.509 certificates or Pre-Shared Key (PSK). X.509 certificates are recommended because they are more secure.
3. If you are using PPTP or L2TP, configure the user accounts, privilege groups, and RADIUS server settings for user authentication. Then, configure the PPTP or L2TP VPN tunnel. For details, see [“Enabling PPTP server and configuring PPTP client and addresses” on page 239](#) and [“Enabling L2TP server and configuring L2TP client and addresses” on page 231](#).
If you are using L2TP over IPSec or IPSec with X.509 certificates for authentication as recommended, configure the certificates. For details, see [“X.509 Certificates” on page 286](#).
4. For IPSec or L2TP over IPSec, configure the IKE proposals that can be used to encrypt and authenticate VPN tunnel connections. You will use the proposal when you configure the IPSec security association for each remote site. To simplify configuration for client-to-site (L2TP over IPSec) and site-to-site VPN connections, you can edit the default IKE proposal pre-configured on the device.
5. For site-to-site connections, if the VPN traffic will come from multiple subnets or go to multiple subnets, configure IP address groups with the subnets that will be used. For details, see [“IP Addresses: Configuration Overview” on page 143](#).
6. Enable IPSec and configure the security associations that set up authentication and determine what traffic is allowed over the VPN connection.

For site-to-site configuration, see [“Configuring an IPSec SA for a site-to-site VPN connection” on page 212](#). You must configure a separate security association for each remote site.

For client-to-site configuration using L2TP over IPSec, use the default SA pre-configured on the device. For details, see [“Editing the default SA for client-to-site VPN connections using L2TP over IPSec” on page 211](#).

IPSec Configuration

IPSec is a security protocol that can be used to secure IP traffic between two remote private networks connected through a public network. It is a flexible protocol with a wide range of encryption options. IPSec is commonly used for both site-to-site connections between separate private networks (tunnels) and for client-to-site connections between remote PCs and private networks. IPSec is the standard X family method of setting up a network-to-network VPN connection.



Note You must enable IPSec globally to use it for IPSec VPNs.

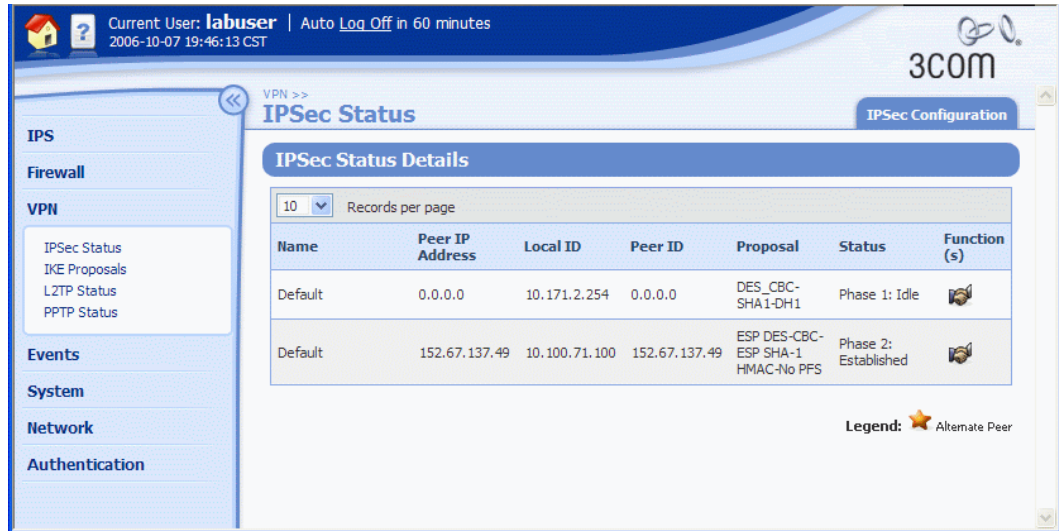
To use the IPSec protocol, you need to configure an **IPSec Security Association (IPSec SA)** which consists of configuration parameters that allow two devices to establish an IPSec tunnel for secure communication across a public network.

You can view and manage IPSec configuration from the IPSec Status page (**VPN > IPSec Status**). From this page, you can complete the following tasks:

- If IPSec is enabled, viewing current status of the IPSec SA Phase 1 and Phase 2 negotiation process.
- Viewing a summary of IPSec SA that have been used to negotiate tunnels on the device.
- Renegotiating IKE Phase 1 or Phase 2 of the IPSec VPN connection.
- Accessing the IPSec Configuration page to enable IPSec and view and manage the IPSec security associations required to establish a VPN connection.

The following figure shows the IPsec Status page:

Figure 7–1: IPsec Status Page



For additional information, see the following topics:

- [“IPsec Status Details” on page 202](#)
- [“IPsec Configuration Page” on page 203](#)


IPsec Status Details

If IPsec is enabled, the **IPsec Status** table provides information about the IPsec security associations currently configured on the device:

Table 7–1: IPsec Status Details

Column	Description
Name	The name of the security association that is configured for this connection. The Default SA is a pre-installed SA used if no other SA matches the VPN connection.
Peer IP Address	The public IP address of the remote VPN device that is currently the peer. If the active device is the alternate peer its IP address is shown here.
Local ID	The Local ID information used to negotiate IKE Phase 1.
Peer ID	The Peer ID information used to negotiate IKE Phase 1.
Proposal	The IKE proposal used to negotiate the VPN connection.

Table 7–1: IPSec Status Details (Continued)

Column	Description
Status	<p>The current status of the connection:</p> <p>Phase 1: Idle — Phase 1 negotiation has not started, or it has started but the connection subsequently timed out, or did not complete successfully</p> <p>Phase 1: Negotiating — The device is in the process of authenticating Phase 1 of the IPSec VPN connection</p> <p>Phase 1: Failed — The negotiation failed</p> <p>Phase 1: Established — The device has successfully completed Phase 1 negotiation</p> <p>Phase 2: Idle — Phase 2 negotiation has not started, or it has started but the connection subsequently timed out, or did not complete successfully</p> <p>Phase 2: Negotiating — The device is in the process of establishing Phase 2 of the IPSec VPN connection</p> <p>Phase 2: Established — A remote device is successfully connected</p> <p>Phase 2: Failed — The negotiation failed</p> <p>Note If you have selected the Enable Verbose messages in the VPN Log option in the IPSec Configuration, you can view more detailed information on the status of the Phase 1 and Phase 2 negotiation in the VPN Log (Events > Logs > VPN Log).</p>
Function(s) 	<p>The functions available to manage the IPSec SA VPN connection:</p> <ul style="list-style-type: none"> • Renegotiate a Phase 1 or Phase 2 connection for the IPSec SA

IPSec Configuration Page

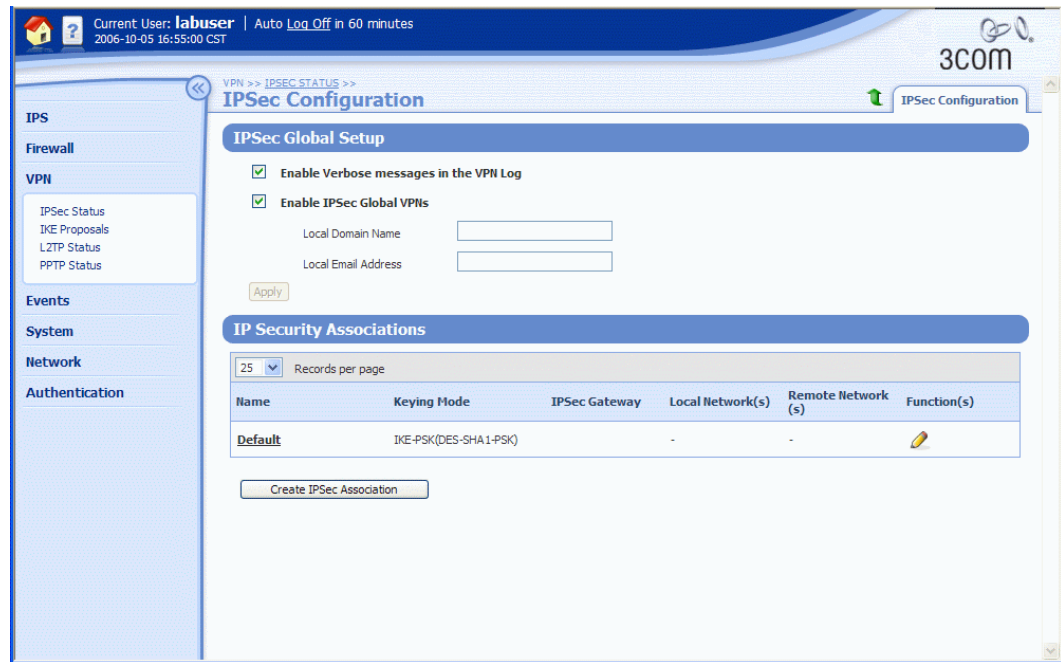
Use the IPSec Configuration page (**VPN > IPSec Status, IPSec Configuration** tab) to view and manage the IPSec configuration and the IPSec security associations. IPSec configuration is required if you want to use site-to-site or client-to-site L2TP over IPSec VPN tunnels.

You can complete the following tasks from this page:

- Enabling IPSec Global VPNs on the X family device
- Configuring the Local ID Domain Name and Email address used to negotiate IKE proposals
- Viewing current IP security associations configured on the X family device
- Creating or editing security associations used to establish VPN tunnel connections

The following figure shows the IPsec Configuration page:

Figure 7–2: VPN: IPsec Configuration Page



For additional information, see the following topics:

- [“Enabling and configuring IPsec global settings” on page 205](#)
- [“Configuring an IPsec Security Association” on page 206](#)
- [“Editing the default SA for client-to-site VPN connections using L2TP over IPsec” on page 211](#)

IPsec Configuration Parameters and IP Security Association Details

The following table describes the configuration parameters for the IPsec security protocol:

Table 7–2: IPsec Configuration Parameters and IP Security Association Details

Parameter	Description
IPsec Global Setup	
Enable Verbose messages in the VPN Log	Select this option to log more detailed information when the device is establishing a VPN connection.
Enable IPsec Global VPNs	Check this option to enable IPsec globally on the device.
Local Domain Name	Enter the domain name for the local ID. If specified, this value can be used to authenticate Phase 1 of the IKE proposal. You only need to specify this parameter if the IKE proposal is configured for aggressive mode.

Table 7-2: IPSec Configuration Parameters and IP Security Association Details (Continued)

Parameter	Description
Local Email Address	Enter the email address to use for the local ID. If specified, this value can be used to authenticate Phase 1 of the IKE proposal. You only need to specify this parameter if the IKE proposal is configured for aggressive mode.
IP Security Association Details: This table displays the IPSec security associations (SAs) configured on the device.	
Name	The name of the IPSec security association.
Keying Mode	Shows the keying mode configured for the IPSec security association. For additional information on keying modes, see “Configuring an IPSec SA for a site-to-site VPN connection” on page 212 and “Editing the default SA for client-to-site VPN connections using L2TP over IPSec” on page 211 .
IPSec Gateway	The IP address of the peer VPN device in use. If the alternate peer is in use it is shown here.
Local Network	Shows what local traffic may access or be accessed over the VPN based on the SA configuration.
Remote Network	Shows what traffic can be sent over the VPN tunnel based on the SA configuration.
Functions	Icons representing functions to manage the IPSec security associations. The following functions are available: <ul style="list-style-type: none"> • Delete an SA <p>Note You cannot delete the default SA.</p> <ul style="list-style-type: none"> • Edit an SA

Enabling and configuring IPSec global settings



Note Before configuring IPSec and the IPSec security association, configure the required IP address groups and the IKE proposals. For details, see [“Configuring IKE Proposals” on page 217](#).

STEP 1 From the navigation pane, select **VPN > IPSec Status**.

The IPSec Status page opens.

STEP 2 Click the **IPSec Configuration** tab.

The IPSec Configuration page opens.

STEP 3 Check **Enable IPSec Global VPNs**.

STEP 4 Check **Enable Verbose messages in the VPN log** to generate more detailed information on the VPN connection process.

This option is only recommended if you need to troubleshoot problems with the VPN tunnel connection.

STEP 5 Type a **Local Domain Name** and **Local Email Address** for the device.

The values specified define the local ID for the device which can be used to authenticate Phase 1 of the IKE proposal. You only need to complete these fields if the authentication type for the IKE proposal used by the SA is configured for aggressive mode.

STEP 6 Click **Apply**.

After configuring IPsec, you need to create the security association that allows two devices to establish the secure IPsec tunnel for the VPN connection. You can edit the default security association, or create a new one. For details, see [“Configuring an IPsec Security Association” on page 206](#).

Configuring an IPsec Security Association

An IPsec security association (IPsec SA) consists of configuration parameters that allow two devices to establish an IPsec tunnel. On the X family device, you need to configure an IPsec security association that allows the device to connect to the remote network (site-to-site) or device (client-to-site)

The device provides a default security association (named **Default**), mainly for client-to-site VPNs.

- The default SA is typically used for the deployment of multiple VPN clients. All the clients can use this default SA, instead of creating one SA per client. The default SA is for incoming connections only, and is used if the device cannot match the IKE identification to any other SA.
- The default SA can also be used to terminate incoming VPN site-to-site connections if the **Enable IPsec Tunnel connections** option is selected.



Note You cannot delete the default SA and you cannot edit the default SA name, peer IP address, or keying mode.

If you want the device to initiate the VPN connection for a site-to-site connection, you must create a unique security association for each site-to-site VPN connection.

The following is an overview of the security association configuration process:

1. **IPsec security association Setup** — Configure the peer ID address, terminated security zone, and keying mode
2. Select the **Keying Mode**, either **IKE** or **Manual**.
Manual keying is only recommended for testing as this mode is not secure.
3. Set up the keys used to authenticate the VPN connection. Depending on the keying mode selected, specify the parameters for **IKE Setup** or **Manual Setup**.

4. **Tunnel Setup** — Select the method to route VPN traffic on the local and remote networks. In this step, you can also enable NAT if you want to perform NAT on traffic entering a VPN tunnel, or configure a VPN supernet for a hub-and-spoke network (for details, see the *Concepts Guide*.)

For additional information on IPSec SA configuration, see the following topics:

- [“Editing the default SA for client-to-site VPN connections using L2TP over IPSec” on page 211](#)
- [“Configuring an IPSec SA for a site-to-site VPN connection” on page 212](#)
- [“Editing the default SA for site-to-site VPN connections” on page 214](#)
- [“Configuring Phase 1 setup parameters for an IKE proposal” on page 221](#)

IPSec Security Association Configuration Parameters

The following table describes the IPSec SA configuration parameters. To review the parameter descriptions for a particular group of settings, see the following topics:

- [“IPSec Security Association Setup” on page 207](#)
- [“Keying Mode” on page 208](#)
- [“IKE Setup:” on page 208](#)
- [“Manual Setup:” on page 209](#)
- [“Tunnel Setup” on page 209](#)

Table 7-3: IPSec Security Association Configuration Parameters

Parameter	Description
IPSec Security Association Setup	
Name	Enter the name for the security association. When a VPN connection is established using IPSec, this name identifies the SA used to make the connection on the IPSec Status page.
Peer IP Address or FQDN	Enter the IP address or fully qualified domain name of the terminating X family or other network device (the target of the VPN link). Note If you set this to 0.0.0.0, the IPSec can only terminate VPNs.
Alternate peer IP Address or FQDN	VPN peer to use if connection to primary VPN peer is lost.

Table 7-3: IPSec Security Association Configuration Parameters (Continued)

Parameter	Description
Terminated Security Zone	<p>Select the remote security zone on which to terminate the VPN from the Terminated Security Zone drop-down list.</p> <p>All devices within the termination zone have unrestricted access to the VPN. Traffic received over the VPN has unrestricted access to all devices within the termination zone. Firewall rules must be used to access other zones.</p> <p>To use NAT within a VPN tunnel, you must select a virtual security zone (such as the VPN default security zone) that contains no physical ports.</p>
Keying Mode	<p>Select the method to use for authenticating access to the VPN from the Keying Mode drop-down list, either:</p> <ul style="list-style-type: none"> • IKE — provides more security than manual keying. If this option is selected, the IKE Setup table displays the IKE parameters. • Manual — provides the lowest level of security. If this option is selected, the Manual Setup table displays the Manual Key parameters.
Enable Security Association	Check this box to enable the security association so that it can be used to establish VPN connections.
Support GRE and L2TP (Transport Mode)	Check this box to use this security association for L2TP or GRE VPNs. Both tunneling protocols can use IPSec to authenticate and encrypt the connection.
IKE Setup: These configuration options are available if IKE is selected as the Keying mode.	
IKE Proposal	Select the IKE proposal the device will use to authenticate VPN connections from the drop-down list. IKE Proposals are setup from the IKE Proposal page (VPN > IKE Proposal).
Shared Secret	If you selected an IKE proposal that authenticates with a Pre-shared Key (PSK), enter the Pre-Shared Key used to validate access to the VPN.
Peer Email Address	If the selected IKE proposal uses Email Address for the Peer ID, enter the Email Address that the device will use to authenticate Phase 1 of the IKE proposal.
Peer Domain Name	If the selected IKE proposal uses Domain Name for the Peer ID, enter the Domain Name for the Peer ID that the device will use to authenticate Phase 1 of the IKE proposal.
Peer Distinguished Name	If the selected IKE proposal uses Distinguished Name for the Peer ID, enter the Domain Name that the device will use to authenticate Phase 1 of the IKE proposal.

Table 7-3: IPSec Security Association Configuration Parameters (Continued)

Parameter	Description
Manual Setup: These configuration parameters are available if Manual Keying is selected as the Keying mode.	
Encryption	<p>Select an appropriate encryption method:</p> <ul style="list-style-type: none"> • ESP DES-CBC (weak encryption, not recommended) • ESP 3DES-CBC (strong encryption) • ESP AES-CBC-128 (strong encryption) • ESP AES-CBC-192 (strong encryption) • ESP AES-CBC-256 (strong encryption) <p>Enter a hexadecimal Key value for the key.</p> <p>Note By default all new X family devices are supplied with 56-bit DES encryption only. To enable the strong encryption functionality (3DES, 128-AES, 192-AES, 256-AES) required to create secure VPN connections, install the correct Strong Encryption Service Pack for your device available from the TMC Web site.</p>
Authentication	<p>Select an appropriate authentication method:</p> <ul style="list-style-type: none"> • ESP MD5-HMAC • ESP SHA-1-HMAC (recommended) • AH MD5 • AH SHA-1 <p>Enter a hexadecimal Key value for the key.</p>
Incoming SPI (hex) Outgoing SPI (hex)	<p>Enter unique hexadecimal values (from 1 to 8 characters) for the incoming and outgoing SPI.</p> <p>When you configure the remote device, specify the same SPI values in reverse order; that is, use the incoming SPI value specified here as the outgoing SPI on the remote device. Use the outgoing SPI value specified here as the incoming SPI on the remote device.</p> <p>The Security Parameter Index (SPI) identifies the cryptographic keys and algorithms to be used to establish a VPN tunnel. For additional information, see the <i>Concepts Guide</i>.</p>
Tunnel Setup	
Enable IPSec tunnel connections	Select to enable further configuration parameters.

Table 7-3: IPSec Security Association Configuration Parameters (Continued)

Parameter	Description
Local Networks	<p>Select one of the following methods to determine what local traffic may access or be accessed from the VPN tunnel. This method is only used for IPSec tunnel mode connections:</p> <ul style="list-style-type: none"> • IP Address Group (configure from Network > Configuration > IP Address Groups) — use this option if traffic allowed over the VPN tunnel is from multiple IP subnets. • IP Subnet and Mask • IP Range • Peer uses tunnel as default route — Select this method if you have want the IPSec tunnel to be used as the default route for the device. • Local addresses assigned by DHCP through this tunnel — Select this method if the connection will be used to connect two X family devices that have been configured to use DHCP Relay over VPN.
Enable NAT of local network addresses	<p>Enable this option to perform NAT on traffic entering a VPN tunnel. Selecting this option allows multiple remote VPN sites can use the same IP subnet.</p> <p>If you enable NAT, enter the NAT IP Address. This address must be included in the Local ID configured for the local network.</p> <p>Only one NAT IP address can be used for outgoing sessions for one VPN tunnel. However, you can configure an <i>all-services</i> virtual server for other specific IP addresses. These servers will use the virtual server public IP address for outgoing sessions when VPN NAT is enabled. This provides one-to-one NAT capability within VPN tunnels. For details, see “Configuring Virtual Servers” on page 81.</p> <p>If you enable NAT for the VPN tunnel, the <i>Terminated Security Zone</i> configured for the security association must be virtual, no physical ports assigned to the zone.</p>

Table 7-3: IPSec Security Association Configuration Parameters (Continued)

Parameter	Description
Remote Networks	<p>Select one of the following methods to determine what traffic should be routed over the VPN tunnel. This method is only used for IPSec tunnel mode connections:</p> <ul style="list-style-type: none"> • IP Address Group (configure from Network > Configuration > IP Address Groups) — use this option if traffic allowed over the VPN tunnel is from multiple IP subnets. • IP Subnet and Mask • IP Range • Peer uses tunnel as default route — Select this method if you have want the IPSec tunnel to be used as the default route for the device. • Remote addresses assigned by DHCP through this tunnel — Select this method if the connection will be used to connect two X family devices that have been configured to use DHCP Relay over VPN.

Editing the default SA for client-to-site VPN connections using L2TP over IPSec

STEP 1 From the navigation pane, select **VPN > IPSec Status**.

The IPSec Status page opens.

STEP 2 Select the **IPSec Configuration** tab.

The IPSec Configuration page opens.

STEP 3 In the IP security associations table, click the **Edit** icon for the **Default** SA entry.

The Edit IP Security Association page opens.

STEP 4 In the IP Security Association Setup table, check **Enable Security Association** to enable the Default SA.

STEP 5 To enable the device to use the Default SA for L2TP VPNs, check **Support L2TP**.

L2TP uses IPSec transport mode.

STEP 6 For **IKE Setup**, select the **IKE Proposal** from the drop-down list of proposals currently configured.

STEP 7 If you have selected an IKE Proposal with pre-shared key (PSK), type the **Shared Secret**.

The same pre-shared key or X.509 Certificate must be available on the remote device establishing a VPN tunnel with the local device.

STEP 8 Click **Save** to save the configuration, or click **Cancel** to return to the IPSec Configuration page without saving the changes.

All devices within the termination zone have unrestricted access to the VPN. Traffic received over the VPN has unrestricted access to all devices within the termination zone. Firewall rules must be configured to access the other zones.

Configuring an IPsec SA for a site-to-site VPN connection

If you want the device to initiate the connection, you must configure a unique security association for each site-to-site VPN connection.

STEP 1 From the navigation pane, select **VPN > IPsec Status**.

The IPsec Status page opens.

STEP 2 Select the IP Configuration tab.

The IPsec Configuration page opens.

STEP 3 Click **Create IPsec Association**, or to edit an existing security association, click its **Edit** icon. The Create/Edit IP Security Association page opens.

STEP 4 Type or edit the name for the security association in the **Name** field.

Choose a name that helps you identify the link for which you are creating the security association.

STEP 5 In the **Peer IP Address or FQDN** field, type the public IP address or fully qualified domain name of the terminating VPN X family or network device (the remote target of the VPN link).



Note If you set this to 0.0.0.0, the IPsec SA can only terminate VPNs.

STEP 6 In the **Alternate peer IP Address or FQDN** field, type the IP address or fully qualified domain name of a VPN peer to use if the connection to the primary VPN peer is lost.

STEP 7 Select the security zone on which to terminate the VPN from the **Terminated Security Zone** drop-down list.

If you want to enable NAT for the VPN tunnel, select a virtual security zone (such as the VPN default security zone) that contains no physical ports.

STEP 8 Select the method to obtain authentication keys from the **Keying Mode** drop-down list, either:

- **IKE** — Automatically generates keys periodically, which provides more security than manual keying.
- **Manual Keying** — Uses the fixed keys configured for the SA. This method provides the lowest level of security and is not recommended.

STEP 9 Check **Enable Security Association** to enable this security association.

STEP 10 For GRE and L2TP over IPsec VPN tunnels, check **Support GRE and L2TP**.

STEP 11 Configure the key information based on the keying mode selected:

- For **IKE Setup**, select the **IKE Proposal** from the drop-down list of proposals currently configured and then:
 - o For **IKE with PSK (Main Mode and Aggressive Mode)**, enter the Pre-shared Key (between 8 and 128 characters) used to validate access to the VPN in the **Shared Secret** field.

The same pre-shared key must be configured on the remote device establishing a VPN tunnel with the local device.

- o Additionally, for **IKE with PSK (Aggressive Mode only)**, enter the peer (remote) ID you want to use in the appropriate field, either **Peer Email Address** or **Peer Domain Name**, depending on the **Peer ID Type** specified for the IKE Proposal (VPN > IKE Proposal). If you specified **IP Address** as the **Peer ID Type** in the IKE Proposal page, the address you entered in the **Peer IP Address** field in step 3 is used, and no entry is required here.
- o For **IKE with X.509 Certificates (Main Mode and Aggressive Mode)**, enter the peer ID you want to use in the appropriate field, either **Peer Distinguished Name**, **Peer Email Address** or **Peer Domain Name**, depending on the **Peer ID Type** specified for the IKE Proposal (VPN > IKE Proposal).



Note If you have selected aggressive mode and are using email or domain for the local ID, you must have configured the local email or domain name on the IPSec Configuration page.

- For **Manual Keying**:
 - o From the **Encryption** drop-down list, select the encryption method and enter the key. For details, see [“Encryption” on page 209](#).
 - o From the **Authentication** drop-down list, select the authentication method and enter the key. For details, see [“Authentication” on page 209](#).
 - o In the **Incoming SPI (hex)** and **Outgoing SPI (hex)** fields respectively, enter unique hexadecimal values (from 1 to 8 characters) for the incoming and outgoing SPI. For details, see [“Incoming SPI \(hex\)” on page 209](#).

You must use the same key information on the remote device.

STEP 12 For IPSec tunnel connections (site-to-site), configure the **Tunnel Setup** for the Local Network and Remote Networks:

STEP A Check **Enable IPSec Tunnel connections**.

STEP B In the **Local Networks** section, select the source IP addresses that the originating device allows to route VPN traffic to the peer VPN firewall, for the specific security association. This applies only to IPSec tunnel mode connections.

- To use specific IP addresses for routing, select **IP Address group**, **IP Subnet**, or **IP Range**. Then, configure the value(s) for the selected field.
- If you have configured the remote (peer) device to use the tunnel as the default route (overriding the default gateway), select **Peer uses tunnel as default route**.
- To use DHCP Relay over VPN, select **Local addresses assigned by DHCP through this tunnel**.

STEP C In the **Remote Networks** table, select the destination IP addresses that the terminating X family or network device allows to route VPN traffic to the local VPN firewall, for the specific security association.

- To use specific IP Addresses for routing, select **IP Address**, **IP Subnet**, or **IP Range**. Then, configure the value(s) for the selected field.
- To override the default gateway, select **Use Tunnel as default route**. Only one SA can be configured with this option.

- To use DHCP Relay over VPN, select **Remote addresses assigned by DHCP through this tunnel**.

STEP 13 Click **Save/Create** to save/create the configuration, or click **Cancel** to return to the IPsec Summary page without saving the changes.

Editing the default SA for site-to-site VPN connections

STEP 1 From the navigation pane, select **VPN > IPsec Status**.

The IPsec Status page opens.

STEP 2 Select the **IPsec Configuration** tab.

The IPsec Configuration page opens.

STEP 3 In the **IP Security Associations** table, click the **Edit** icon for the **Default** SA entry.

The Edit IP Security Association page opens.

STEP 4 In the **IP Security Association Setup** section, check **Enable Security Association** to enable the default SA.

STEP 5 In the **IKE Setup** section, select the **IKE Proposal** from the drop-down list of proposals currently configured.

STEP 6 If you have selected an IKE proposal with pre-shared key (PSK), type the **Shared Secret**. If you have selected a proposal with X.509 certificates, type the certificate key.

The same pre-shared key or X.509 certificate and key must be available on any remote device using this IKE proposal to establish a VPN connection.

STEP 7 In the **Tunnel Setup** section, check **Enable IPsec Tunnel connections** if you want to use the default SA as the tunnel mode for terminating the site-to-site connection.

All devices within the termination zone have unrestricted access to the VPN. Traffic received over the VPN has unrestricted access to all devices within the termination zone. Firewall rules must be configured to access other zones.

STEP 8 Click **Save** to save the configuration, or click **Cancel** to return to the IPsec Configuration page without saving the changes.

IKE Proposal

Internet Key Exchange (IKE) is used to negotiate the keying material used by the IPsec VPN encryption and integrity algorithms. IKE uses UDP port number 500 and precedes the actual IPsec data flow. IKE is a two-stage mechanism for automatically establishing IPsec tunnels with dynamically generated keying material.

IKE proposals are divided into two phases:

1. The device negotiates **Phase 1** of the IKE and establishes a shared, secure connection. Phase 1 uses Aggressive Mode or Main Mode (the default) for packet exchange.
2. In **Phase 2**, the device establishes keying material for the VPN. Phase 2 is much quicker than Phase 1, since it can rely on the checks established during Phase 1, without needing to re-establish a shared, secure connection. Phase 2 uses Quick Mode for packet exchange.

Phase 1 of the IKE negotiation requires authentication between the two devices to be connected over the VPN tunnel. When you configure the IKE proposal, you can select one of the following Authentication methods based on your network security requirements:

- IKE with Pre-shared Key (Main Mode)
- IKE with Pre-shared Key (Aggressive Mode)
- IKE with X.509 Certificates (Main Mode)
- IKE with X.509 Certificates (Aggressive Mode)
- Manual Keying



Note To use X.509 certificate authentication, you must first import matching X.509 CA certificates and local certificates on the X family and remote device(s). On the X family device, you can create certificates from the X.509 Certificates page (**Authentication > X.509 Certificates**).

On the X family device, you configure the IKE proposals with the authentication and encryption configuration (used for Phase 1 and Phase 2 IKE negotiation) required for the different types of remote devices that will connect via the VPN tunnel connection. Then, when you create the IPsec security association required for each remote device, you can select the IKE proposal to use for key exchange and specify the key information.

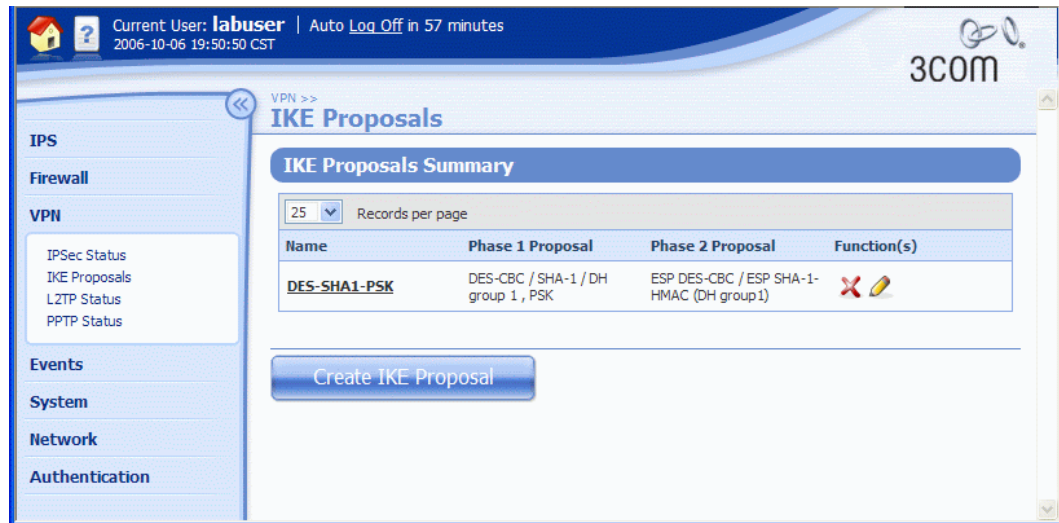
Managing IKE Proposals

You can view, manage, and configure IKE proposals from the IKE Proposals page (**VPN > IKE Proposals**). From this page you can complete the following tasks:

- Viewing and managing existing IKE proposals configured on the device
- Creating or editing an IKE proposal
- Deleting an IKE proposal

The following figure shows the IKE Proposals page:

Figure 7–3: IKE Proposals Page



IKE Proposal Details

The IKE Proposals page provides the following information about the existing proposals:

Table 7–4: IKE Proposal Details

Column	Description
Name	The name of the IKE proposal.
Phase 1 Proposal	The encryption and integrity protocols, the Diffie-Hellman (DH) Group number, and whether Aggressive Mode and NAT-Transversal (NAT-T) are enabled.
Phase 2 Proposal	The encryption and integrity protocols and the Diffie-Hellman (DH) Group number if using perfect forward secrecy.
Function(s)	Icons representing functions to manage IKE proposals. The following functions are available: <ul style="list-style-type: none"> • Delete a proposal • Edit a proposal

Configuring IKE Proposals

IKE proposals provide the authentication and encryption methods that are used to configure the IPsec security associations for IPsec VPN tunnel. Configure an IKE proposal for each type of remote network device that requires a VPN connection.

Main Mode and Aggressive Mode

When you configure an IKE proposal, you have options to use main mode or aggressive mode. Main mode is the default and recommended configuration. You can use this mode if all the addresses of the remote sites to connect via VPN have fixed IP addresses. This is the recommended configuration. If the remote sites have dynamic addresses (not recommended), then you must use Aggressive mode for the IKE proposal. However, this mode is less secure.

Create IKE Proposal Page

You can configure an IKE proposal from the Create/Edit IKE Proposal page (VPN > IKE Proposals).

The following figure shows the Edit IKE Proposal page:

Figure 7–4: Edit IKE Proposal Page

Current User: **labuser** | Auto Log Off in 59 minutes
2006-10-07 23:17:23 CST

3COM

VPN >> **Edit IKE Proposal**

IKE Phase 1 Setup

Proposal Name:

Encryption:

Integrity:

Diffie-Hellman Group:

Lifetime: seconds

Authentication Type:

Options:

- Enable Aggressive Mode
- Enable NAT Traversal
- Enable Dead Peer Detection
- Automatically connect on system start-up
- Delete Phase 2 SA when Phase 1 SA terminates

IKE Phase 2 Setup

Encryption:

Integrity:

Lifetime: seconds

Diffie-Hellman Group:

Options:

- Enable Perfect Forward Secrecy
- Enable strict ID checking of local network
- Use ID of 0.0.0.0/0 for local and remote networks

IKE Proposal Configuration Parameters: Phase 1 and Phase 2

The following table describes the IKE Phase 1 and Phase 2 Configuration parameters:

Table 7–5: IKE Proposal Phase 1 and Phase 2 Configuration Parameters

Parameter	Description
<p>IKE Phase 1 Setup: Specify the parameters the device uses to negotiate Phase 1 of the IKE to establish a shared, secure connection. Phase 1 uses Aggressive Mode or Main Mode for packet exchange. The default is Main Mode.</p>	
Proposal Name	Specifies a name for the IKE proposal. When you configure an IPSec security association, this name is used to select the IKE proposal to be used with the SA.
Encryption & Integrity	<p>Encryption and Integrity work in combination to provide the degree of security required. Recommended combinations for IKE Phase 1 and IKE Phase 2 are listed below in order from least secure to most secure:</p> <ul style="list-style-type: none"> • DES-CBC encryption with MD5 or SHA1 integrity (not recommended) <p>The following combinations are recommended combinations for IKE Phase 1:</p> <ul style="list-style-type: none"> • DES-CBC encryption with MD5 or SHA1 integrity • 3DES-CBC (strong encryption device only) with MD5 or SHA1 integrity • AES-CBC-128 (strong encryption device only) with SHA1 integrity • AES-CBC-192 (strong encryption device only) with SHA1 integrity • AES-CBC-256 (strong encryption device only) with SHA1 integrity <p>DES should only be used if it is supported on the remote device(s).</p> <p>Note The strong encryption options are only available if the device is configured with strong encryption. To enable strong encryption (3DES, 128-AES, 192-AES, 256-AES), install the correct Strong Encryption Service Pack for your X family device, available from the TMC Web site.</p>
Diffie Hellman Group	<p>Diffie-Hellman is the protocol used to establish shared security, to prevent unauthorized access to the key negotiation. The higher the Diffie-Hellman Group number, the more secure the connection. For interoperability or export restrictions, you may need to select a lower group number. Supported groups are:</p> <ul style="list-style-type: none"> • 1 (768 bits) — This setting is not recommended • 2 (1024 bits) • 5 (1536 bits) (high-encryption device only)
Lifetime	Specify the length of time the security association remains valid before new authentication and encryption keys must be exchanged (between 1 and 65535 seconds, default 28800). A lower value increases security, but may be inconvenient, since the connection is temporary disabled.

Table 7–5: IKE Proposal Phase 1 and Phase 2 Configuration Parameters (Continued)

Parameter	Description
Authentication Type: Pre-Shared Key	<p>If selected, the device uses a shared password to authenticate access to the VPN connection.</p> <p>If you select this option and use the Aggressive Mode option, you need to specify a Local ID Type and Peer ID Type.</p>
Authentication Type: X.509 Certificates	<p>If X.509 certificates is selected as the authentication type, select the local certificate to be used for authentication from the drop-down list. To specify a CA certificate to validate access to the VPN, check Only accept peer certificates signed by. Then, select the CA certificate from the drop-down list. If you do not specify a certificate, the device will use any of the imported CA certificates available on the device.</p> <p>Note Import certificates from the X.509 Certificates page (Authentication > X.509 Certificates) to upload CA certificates and local certificates for use on the device.</p>
Options: Enable Aggressive Mode	<p>To enable Aggressive mode, check Enable Aggressive Mode. Aggressive mode is required when using dynamic WAN IP addresses. However, this mode is less secure. By default, the device uses Main Mode. If you select aggressive mode, configure the local ID and peer ID information that will be used to authenticate the Phase 1 of the IPSec connection.</p> <p>If Pre-Shared Key is selected for authentication:</p> <ul style="list-style-type: none"> From the Local ID Type drop-down list, select the type of information the device will use to negotiate Phase 1 of the IPSec connection: IP Address, Email Address, or Domain Name. <p>The values for the local ID email address and domain name are configured on the IPSec Configuration page. The local ID IP address value is the external IP address.</p> <ul style="list-style-type: none"> From the Peer ID Type drop-down list, select the type of information the device will use to negotiate Phase 1 of the IPSec connection: IP Address, Email Address, or Domain Name. <p>The values for the peer ID IP address, email address, and domain name are configured from the Create/Edit IP Security Association page.</p> <p>If X.509 Certificate is selected for authentication:</p> <ul style="list-style-type: none"> The Local ID Type defaults to Distinguished Name. From the Peer ID Type drop-down list, select the type of information in the X.509 certificate that the device will use to negotiate Phase 1 of the IPSec connection: Distinguished Name, Email Address, or Domain Name. Enter the appropriate information that is contained in the certificates on the device and on the remote device.
Enable NAT Traversal	Select this option if there is a NAT device between the two VPN devices.

Table 7–5: IKE Proposal Phase 1 and Phase 2 Configuration Parameters (Continued)

Parameter	Description
Enable Dead Peer Detection	Check this option to enable the device to check that the VPN link is still functioning. If the device detects a dead peer, it switches to the alternate SA peer (if defined) for the duration of the Phase 1 lifetime of the VPN tunnel.
Automatically connect phase 1 on system start-up	Check this option to initiate the VPN upon startup with IKE phase 1 proposal automatically established. Use this option if the device is using a dynamic WAN IP address.
Automatically connect phase 2	This option is enabled if “Automatically connect phase 1 on system start-up” is checked.
Delete Phase 2 SA when Phase 1 SA terminates	Check this option to delete all Phase 2 security associations if the Phase 1 security association terminates. If this option is selected, it can improve interoperability with VPN devices that automatically delete all the Phase 2 security associations if the Phase 1 security association terminates.
<p>IKE Phase 2 Setup: Specify the parameters the device uses to negotiate Phase 2 of the IKE to establishes keying material for the VPN. Phase 2 is much quicker than Phase 1, since it can rely on the checks established during Phase 1 without needing to reestablish a shared, secure connection. Phase 2 uses Quick Mode for packet exchange.</p> <p>Note If “Automatically connect phase 1 on system start-up” and “automatically connect phase 2” are both checked in IKE Phase 1 setup, then after a Phase 1 connection is established, every defined Phase 2 connection is negotiated with the peer and brought up. Traffic can flow through the tunnel without further negotiation.</p>	
Encryption & Integrity	Encryption and Integrity work in combination to provide the degree of security required. For a list of combinations for IKE Phase 1 and IKE Phase 2, see “Encryption & Integrity” on page 218 .
Lifetime	The duration of IKE Phase 2 (between 1 and 65535 seconds, default 28800). IKE Phase 2 will time out after this interval expires. Note This feature must be supported by the device by both VPN devices.
Enable Perfect Forward Secrecy	Check this option to enhance VPN security if the remote device also supports the Perfect Forward Secrecy feature.

Table 7–5: IKE Proposal Phase 1 and Phase 2 Configuration Parameters (Continued)

Parameter	Description
Diffie-Hellman Group	<p>This setting is only required if Perfect Forward Secrecy is enabled.</p> <p>Diffie-Hellman is the protocol used to establish shared security, in order to prevent unauthorized access to the key negotiation. The higher the Diffie-Hellman Group number, the more secure the connection. For interoperability or export restrictions, you may need to select a lower group number. Supported groups are:</p> <ul style="list-style-type: none"> • 1 (768 bits) • 2 (1024 bits) • 5 (1536 bits) (high-encryption device only)
Phase 2 Local ID configuration options	<p>These options determine how the device negotiates IKE Phase 2 local ID checking:</p> <ul style="list-style-type: none"> • Select Enable strict ID checking of local network to restrict the use of the Phase 2 tunnel to packets with a source IP address corresponding to a local ID configured for the local network of the IPsec security association. For backwards compatibility with the 2.2 release, this field is disabled by default. • Select Use ID of 0.0.0.0/0 for local and remote networks to create a single Phase 2 SA for all traffic using a local ID of 0.0.0.0/0 and a remote ID of 0.0.0.0/0. This option allows interoperability with devices from other vendors such as Netscreen which always negotiate Phase 2 IDs as 0.0.0.0/0.

Configuring Phase 1 setup parameters for an IKE proposal

The values specified for Phase 1 IKE negotiation must match the values configured on the remote device.

STEP 1 From the navigation pane, select **VPN > IKE Proposals**.

The IKE Proposals page opens.

STEP 2 Click **Create**, or to edit an existing IKE proposal, click its **Edit** icon.

The Create or Edit IKE Proposal page opens.

STEP 3 If you are creating a new proposal, type the **Proposal Name**.

You cannot change the name of an existing proposal.

STEP 4 Select the required encryption and integrity combinations from the **Encryption** and **Integrity** drop-down lists.

For information on these fields, see [“IKE Proposal Configuration Parameters: Phase 1 and Phase 2” on page 218](#).

STEP 5 Select the **Diffie-Hellman Group** from the drop-down list.

STEP 6 In the **Lifetime** field, enter the length of time you want the security association to last before new authentication and encryption keys must be exchanged (between 1 and 65535 seconds, default 28800).

A lower value increases security, but may be inconvenient, since the connection is temporary disabled.

STEP 7 From the **Authentication Type** drop-down list, select the method to use for authenticating access to the VPN:

- **Pre-Shared Key** — default level of security
- **X.509 Certificates** — highest level of security

STEP 8 Optionally, check **Enable Aggressive Mode** if the external IP address is not fixed.

This setting is not recommended.

STEP 9 If you are using **Pre-Shared Key** with **Aggressive Mode**:

- From the **Local ID Type** drop-down list, select the identifier for the device to use for validation purposes: **IP Address**, **Email Address**, or **Domain Name**.
- From the **Peer ID Type** drop-down list, select the identifier for the device to use for validation purposes: **IP Address**, **Email Address**, or **Domain Name**.

You must select the same local ID and peer ID types that are configured on the remote device that will connect via the VPN tunnel.

STEP 10 If you are using **X.509 certificates** (with either **Aggressive Mode** or **Main Mode**):

- Select the local certificate you want to use from the **Local Certificate** drop-down list.
- Select the type of information in the certificate to use for validation purposes from the **Peer ID Type** drop-down list: **Distinguished Name**, **Email Address**, or **Domain Name**. You must select the same type that is used on the remote device.
- To specify the CA certificate you want to use to validate access to the VPN, check **Only accept peer certificates signed by**, and select the certificate from the drop-down list. This increases security on the VPN



Note If you do not specify a certificate, by default the device will use any of the available CA certificates. CA certificates are imported from the X.509 Certificates page (**Authentication > X.509 Certificates**).

STEP 11 If there is a NAT device between the two VPN devices, check **Enable NAT-Traversal**.

STEP 12 To enable the device to check that the VPN link is still functioning, check **Enable Dead Peer Detection**.

STEP 13 To initiate the VPN upon startup with IKE Phase 1 proposal automatically established, check **Automatically connect phase 1 on system start-up**.

Use this option if the device is using a dynamic external IP address.

If this option is checked, and you want to configure Phase 2 connections to connect automatically, check **Automatically connect phase 2**.

- STEP 14** To delete all Phase 2 security associations if the Phase 1 security association terminates, check **Delete Phase 2 SA when Phase 1 SA terminates**.



Note Some VPN devices automatically delete all the Phase 2 security associations if the Phase 1 security association terminates. To improve interoperability with such devices, check this option.

Configuring Phase 2 setup parameters for an IKE proposal

- STEP 1** Select the required encryption and integrity combinations from the **Encryption** and **Integrity** drop-down lists.
- STEP 2** Enter the duration of IKE Phase 2 in the **Lifetime** field (between 1 and 65535 seconds, default 28800). IKE Phase 2 will time out after this interval.
- STEP 3** To provide enhanced security, check **Enable Perfect Forward Secrecy**, and then select the **Diffie-Hellman Group** to use from the drop-down list.



Note This feature must be supported by both VPN devices.

- STEP 4** Configure the Phase 2 local ID checking options to determine how the X family device negotiates IKE Phase 2 local ID checking. For details, see [“Phase 2 Local ID configuration options” on page 221](#).
- STEP 5** Click **Create/Save** to save the configuration, or click **Cancel** to return to the IKE Proposals page without saving the changes.

For detailed field descriptions, see [“IKE Proposal Phase 1 and Phase 2 Configuration Parameters” on page 218](#).

Client-to-Site Configuration

This section provides a brief overview of the typical steps in setting up a client-to-site VPN, using one of the available methods.

Client-to-site configuration using standard IPSec

- STEP 1** From the navigation panel, select **VPN > IPSec**. Then, select the **IPSec Configuration** tab. Then, check the **Enable IPSec Global VPNs** box. If this option is not selected, the VPN connections configured for the X family device will not be activated.
- STEP 2** On the IPSec Configuration page, edit the default SA. Then, check **Enable Security Association**.
- STEP 3** Configure the IKE setup.
- STEP 4** Enable IPSec Tunnel connections and configure the Tunnel security zone.
- STEP 5** On the VPN clients (for example, Windows 2000/XP), ensure that the relevant configuration settings match those you have configured on your T10 device.

Client-to-site configuration using L2TP

- STEP 1** From the navigation panel, select **VPN > L2TP Status > Server Configuration**, enable the security zone to terminate the VPN, check **Require encryption**, enter the client configuration, and select the method for assigning L2TP addresses.
- STEP 2** Select **VPN > IPSec/IKE Status > IPSec Configuration** and check the **Enable IPSec Global VPNs** box. If this option is not selected, the VPN connections configured for the device will not be activated.
- STEP 3** Select **VPN > IPSec/IKE Status > IPSec Configuration**, select the **Default SA** and in the VPN - Edit Security Association page, check **Enable Security Association** and enable **Support GRE and L2TP**. Configure the SA and associated IKE proposal appropriately.
- STEP 4** On the VPN clients (for example, Windows 2000/XP), ensure that the relevant configuration settings match those you have configured on your device.

Configuring Windows Clients

- Windows 2000/NT — To set up an L2TP/IPSec connection on Windows 2000/NT, create a new connection in the Dial-Up Networking (Network Connections on XP) folder by using the **Make A New Connection** wizard. Then select the Microsoft L2TP/IPSec VPN Adapter (or RASL2TPM for Windows NT 4.0) as the device. Provide the IP address of the device instead of a telephone number for this connection.
- Windows XP — To set up an L2TP/IPSec connection on Windows XP, create a new connection in the Network Connections folder by using the **Create A New Connection** wizard. Then select the Microsoft L2TP/IPSec VPN Adapter as the device. Provide the IP address of the T10 device.

Client-to-site configuration using PPTP

- STEP 1** From the navigation panel, select **VPN > PPTP Status > Server Configuration**, enable the PPTP server, and select the security zone to terminate the VPN.
- STEP 2** Check the **Require encryption** box to use the Microsoft Point-to-Point Encryption, provide the client configuration, and select the method for assigning PPTP addresses.
- STEP 3** On the VPN clients (e.g., Windows 95/98/NT), ensure that the relevant configuration settings match those you have configured on your T10 device.

Troubleshooting Client-to-Site Configuration

The following may help you if you are having problems with a client-to-site VPN connection:

- Incorrectly configured IP addressing information can prevent the X family device from establishing a connection with the remote VPN clients.
- Ensure that the VPN client is compatible with the method selected (for example, older Windows VPN clients do not support L2TP).
- Check the IPSec/IKE Status page to determine if there is a problem and to see the status of the VPNs.
- Check the device logs to see if a problem is indicated in any of the entries.
- Incorrect authentication setup can prevent the client from authenticating with the device.
- Incorrect firewall rule setup can block VPN traffic.

L2TP Configuration

Layer 2 Tunneling Protocol (L2TP) allows a dial-up user to make a virtual Point-to-Point Protocol (PPP) connection to an L2TP Server on the VPN. L2TP sends PPP frames through a tunnel between a user and the L2TP Server.

You can configure the X family device to act as an **L2TP Server** with support for **L2TP over IPSec**. L2TP over IPSec is a combination of protocols commonly used to authenticate a user (L2TP) and encrypt data (using IPSec). The combination is much more secure than using the L2TP protocol alone.

As an L2TP server, the device can terminate L2TP connections from VPN clients, such as those included with Windows XP or Windows Vista.



Note To use the device as an L2TP VPN terminator, you must check **Support L2TP** when you are configuring the IPSec default SA. For details, see [“Editing the default SA for client-to-site VPN connections using L2TP over IPSec” on page 211](#).

L2TP/IPSec VPN Configuration

L2TP over IPSec is the method recommended by Microsoft for remote access VPN. L2TP/IPSec uses the security attributes of an IPSec tunnel for data transfer, and the Layer 2 tunneling protocol for user authentication and client IP address allocation to essentially make the client appear as part of the workplace network. Although more difficult to set up (due to the IPSec steps), this is a far more secure solution than PPTP.



Note The device and Windows XP offer a choice between using a Pre-shared Secret Key (PSK) or X.509 Digital Certificates to secure the IPSec VPN. The following description only illustrates the PSK configuration.

This section describes configuration of L2TP/IPSec termination into the VPN zone. The following steps are required:

1. Creating an IP address pool for L2TP/IPSec VPN clients.
2. Configuring and enabling L2TP server on the device.
3. Configuring the Default SA entry on the device.
4. Verifying firewall rules.
5. Creating a user account.

6. Configuring the Windows XP client using dial-up networking.

Step 1: Create an IP address pool for L2TP/IPSec

The device uses the IP address pool to issue addresses for use by the VPN clients. You must ensure that the IP address pool configuration meets the following criteria:

- The range is part of the security zone within which the L2TP tunnel will terminate.
- The terminating security zone in the L2TP Server configuration is assigned to an internal virtual interface.
- The address range does not conflict with others used for the DHCP server or other services.

STEP 1 From the navigation panel, select **Network > IP Address Groups**. Create an address group and give it a name, such as L2TP_Pool.

STEP 2 Select the method to specify the address group; for example, **IP Range**. Then, type the range; for example, **192.168.1.10 to 192.168.1.201**.

STEP 3 Click **Add to table below** to enter the range.

STEP 4 Add more ranges, subnets, or hosts as required.

STEP 5 Click **Create** to save your changes.

Step 2: Configure the L2TP server on the device

STEP 1 From the navigation panel, select **VPN > L2TP Status**. Then, select the **L2TP Server Configuration** tab.

STEP 2 Click **Enable L2TP Server**.

STEP 3 Set the **L2TP Security Zone** to **LAN**.

STEP 4 Select **Require Encryption** to secure the connection.

STEP 5 Enter any DNS and WINS settings.

STEP 6 Select the IP Address Group created previously (L2TP_Pool).

STEP 7 Click **Apply**.

STEP 8 To enable IPSec VPNs:

STEP A On the IPSec Configuration page, click **Enable IPSec Global VPNs**. Because the tunnel will be main mode, you do not need to supply a Local Domain Name or Local Email Address.

STEP B Click **Apply**.

Step 3: Configure the default SA

STEP 1 On the IPSec Configuration page, edit the Default Security Association.

STEP 2 On the Edit Security Association page:

STEP A Check **Enable Security Association**.

STEP B Ensure that **Support GRE and L2TP** is enabled.

- STEP C** In the **Terminated Security Zone** drop-down list, select the security zone (such as LAN) where L2TP/IPSec connections terminate.
- STEP D** Verify that **Keying Mode** is set to IKE.
- STEP E** In **IKE Setup**, select the IKE Proposal from the drop-down list. Then, type the **Shared Secret** to be used. The Shared Secret is masked as you type it.
- STEP 3** In **Tunnel Setup**, verify that **Enable IPSec tunnel connections** is enabled.
- STEP 4** Click **Save**.
- STEP 5** Edit the IKE Proposal:
 - STEP A** Select **VPN > IKE Proposals**.
 - STEP B** On the VPN - IKE Proposals page, edit the default IKE proposal **DES-SHA1-PSK**.
 - STEP C** On the Edit IKE Proposal Setup page, check **Delete Phase 2 SA when Phase 1 SA terminates**.
 - STEP D** Verify that the **Diffie-Hellman Group** on both Phase 1 and Phase 2 is set to 1 (768 bits).
 - STEP E** Click **Save**.

Step 4: Verify firewall rules

Perform this step if you are using multiple security zones, and/or have changed the terminating zone from LAN, and/or have changed the firewall rules for traffic allowed to the device from the WAN.

- STEP 1** From the navigation panel, select **Firewall > Firewall Rules**.
- STEP 2** On the Firewall Rules page, review the entries to verify that the following rules have been configured:
 - Allow traffic to/from other security zones and the security zone you have set for the L2TP Server.
 - Allow traffic to/from other security zones and the security zone you have set for the L2TP Server.
 - Allow the IPSec tunnel traffic to the WAN security zone2.
 - Allow L2TP traffic (UDP port 1701) from the terminating security zone for L2TP Server to *this-device*. This allows the L2TP traffic to flow after the IPSec tunnel is terminated.
 - Allow *this-device* to send ANY protocol to ANY zone.
- STEP 3** Configure any rules that are missing.

Step 5: Create a user account

Only a user with Super-user security level can create a user account.

- STEP 1** From the navigation panel, select **Authentication > User List**.
- STEP 2** On the User List page, click **Create A New User**.
- STEP 3** On the Create User page, enter a **Username**.
- STEP 4** The user name is case sensitive.

- STEP 5** For the **User Type**, select **Local User**.
- STEP 6** For the **Privilege Group**, select **Allow_VPN_Access**.
- STEP 7** Enter and confirm the **Password**.
The user name is case sensitive.
- STEP 8** Click **Create**.

Step 6: Configure the Windows XP client with L2TP/IPSec

The following instructions are for configuring a Windows XP client for a PPTP connection. If you are using another operating system, such as Mac OS or Linux, see the documentation for details on configuring the client for a PPTP connection.

- STEP 1** From the Windows **Start** menu, select **Network Connections**.
- STEP 2** Click **Create a New Connection** to launch the New Connection Wizard.
- STEP 3** Use the following table to complete the New Connection Wizard prompts.

Network Wizard Prompt	Select or type...
Connection Type	Connect to the network at my workplace
Network Connection	Virtual Private Network connection
Connection Name	Type a connection name, such as L2TPIPsecVPN
Public Network Setting	Do not dial the initial connection
VPN Server	Type the public WAN IP address of the device
Connection Availability	Select Anyone's use or My use only
Completing the New Connection Wizard	Finish

- STEP 4** After creating the connection, you are prompted to connect for the first time.
- STEP 5** On the **Connection** dialog box, click the **Properties** button.
- STEP 6** To force the Windows client to use the VPN connection type:
- STEP A** Select the **Networking** tab.
- STEP B** Under **Type of VPN**, select **L2TPIPsec VPN** from the pull-down list.
- STEP C** Select the **Security** tab, then click the **IPSec Settings** button.
- STEP D** On the **IPSec Settings** dialog box, check **Use pre-shared key for authentication**.
- STEP E** Type the shared secret that you configured for the IKE proposal. Click **OK** to save the settings.
- STEP F** On the **Network Properties** dialog, click **OK** to return to the Network Connection username/password prompt.

STEP 7 On the Network Connections page, enter the user details configured on the device for the local users.



TIP The username and password are case sensitive.

L2TP Status

You can view and manage L2TP connections and configuration from the L2TP Status page (**VPN > L2TP Status**). From this page, you can complete the following tasks:

- Viewing current L2TP connections on the device
- Terminating a current connection
- Accessing the L2TP Server Configuration page to enable and configure the L2TP server

The following figure shows the L2TP Status page:

Figure 7–5: VPN: L2TP Status Page




L2TP Status Page Details

The L2TP Connections table provides the following information about current connections:

Table 7–6: VPN: L2TP Status Page Details

Column	Description
IP Address	The IP address allocated to the L2TP client.
Remote IP Address	The public IP address of the L2TP client.
Hostname	The name of the device hosting the L2TP client.
Username	The name used by the client for authentication by the local database or RADIUS.

Table 7–6: VPN: L2TP Status Page Details (Continued)

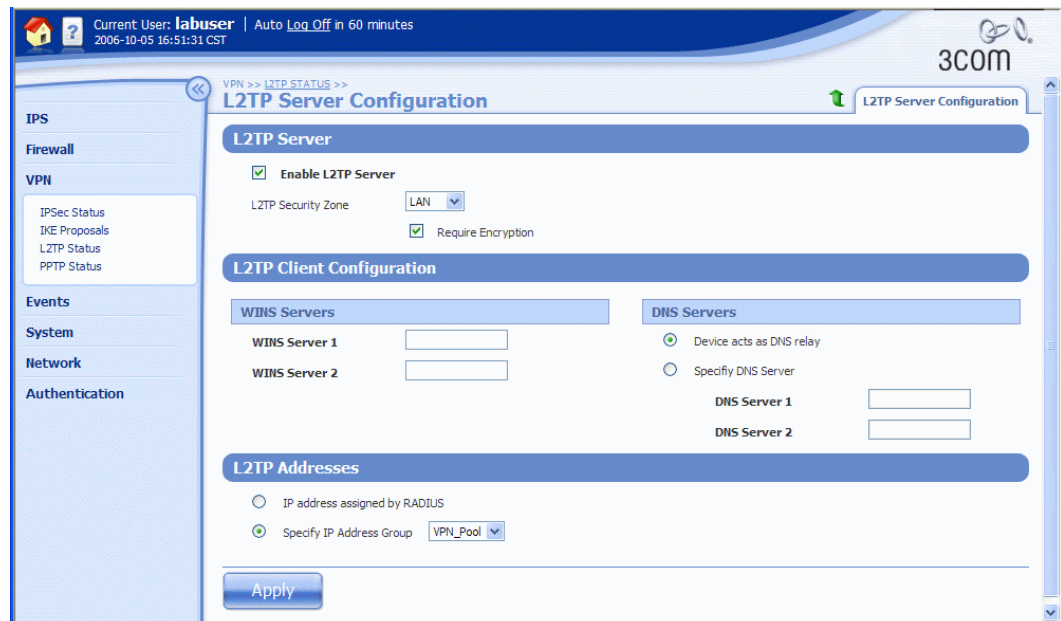
Column	Description
PPP Authentication	The PPP authentication mechanism: PAP , CHAP , MS CHAP , or MS CHAPv2 .
Function(s) 	Icons representing functions to manage the L2TP connection: <ul style="list-style-type: none"> • Delete the current connection. Deleting a connection disconnects the remote user (client-to-site configurations) or network (site-to-site configurations) using the VPN link.

L2TP Server Configuration Page

You can configure the X family device to act as an L2TP server from the L2TP Server Configuration page (VPN > L2TP Status, L2TP Server Configuration tab).

The following figure shows the L2TP Server Configuration page:

Figure 7–6: VPN: L2TP Server Configuration Page



L2TP Server Configuration Parameters

The following table provides descriptions for the L2TP Server Configuration Parameters:

Table 7–7: L2TP Server Configuration Parameters

Parameter	Description
L2TP Server	
Enable L2TP Server	Allows VPN clients to use the device as a VPN terminator for L2TP.
L2TP Security Zone	Selects the remote security zone on which to terminate the VPN from the L2TP Security Zone drop-down list.
Require Encryption	Enables Microsoft Point-to-Point Encryption to provide additional security. This feature is supported by Windows VPN clients.
L2TP Client Configuration	
WINS Servers	If you are using Microsoft Networking, type the IP addresses of your primary (WINS Server 1) and secondary (WINS Server 2) WINS servers.
DNS Servers	Determines the DNS servers that the PPTP server uses: <ul style="list-style-type: none"> • Select Device Acts as DNS Relay to enable the device to act a proxy-DNS server (DNS relay), passing DNS queries to its configured DNS servers. • Select Specify DNS Server to enter up to two local DNS server IP addresses, in order in which they are to be accessed, in the DNS Server fields.
L2TP Addresses	Determines how IP addresses are allocated to clients connected through the L2TP server: <ul style="list-style-type: none"> • Select IP address assigned by RADIUS to enable the device to use the RADIUS server to assign the L2TP client IP address. The RADIUS server must be enabled on the RADIUS page (Authentication > RADIUS). • Specify IP address group and select an existing address group to enable the device to assign the L2TP client an IP address from the addresses included in the IP address group. Use the IP Addresses page (Network > Configuration > IP Address Groups) to create IP address groups.

Enabling L2TP server and configuring L2TP client and addresses

- STEP 1** If you are not using RADIUS to assign IP addresses, create an IP address group (**Network > Configuration > IP Address Groups**) containing the pool of IP addresses that the device will use to allocate IP addresses to L2TP VPN clients.
- STEP 2** From the navigation pane, select **VPN > L2TP Status**.
The L2TP Status page opens.
- STEP 3** Click the L2TP Server Configuration tab.
The L2TP Server Configuration page opens.
- STEP 4** Check **Enable L2TP Server**.

This allows VPN clients to use the device as a VPN terminator for L2TP.

- STEP 5** Select the remote security zone on which to terminate the VPN from the **L2TP Security Zone** drop-down list.
- STEP 6** To use Microsoft Point-to-Point Encryption, check **Require Encryption**.
This option provides additional security, and is supported by Windows VPN clients.
- STEP 7** To use Microsoft Networking, enter the IP addresses of your primary and secondary WINS servers in the **WINS Server 1** and **WINS Server 2** fields, respectively.
- STEP 8** To configure DNS servers, select one of the following in the **DNS Servers** section:
- **Device Acts as DNS relay** if you want the device to act as a proxy-DNS server (DNS relay), passing DNS queries to its configured DNS servers
 - **Specify DNS Server** and enter up to two local DNS server IP addresses, in the order in which they are to be accessed, in the **DNS Server** fields
- STEP 9** To assign L2TP IP addresses, select one of the following in the **L2TP Addresses** section:
- If you want the device to use the RADIUS server to assign the L2TP client IP address, select **IP Address Assigned by RADIUS**
 - If you want the device to use an IP address group for the client, select **Specify IP Address Group** and select an existing group from the drop-down list
- STEP 10** Click **Apply** to save the changes.

Configuring Client-to-Site VPNs for Windows Clients

The following sections provide details on how to configure the X family device to work with Windows VPN clients using either PPTP or L2TP/IPSec. The PPTP configuration is easier to set up than L2TP/IPSec, but L2TP/IPSec provides a more secure connection.

The configuration instructions provided are based on setting up the device configuration and configuring the connection in Windows XP. The following scenarios are presented:

- [“Client PPTP VPN Access Configuration” on page 232](#)
- [“L2TP/IPSec VPN Configuration” on page 225](#)

Client PPTP VPN Access Configuration

The following procedure configures PPTP termination into the VPN zone. The following steps are required:

1. Create an IP address pool for PPTP VPN clients
2. Configure and enable the PPTP server on the device
3. Check firewall rules
4. Create a local-user account on device for VPN Client users

5. Configure the Windows XP client using dial-up networking



Note PPTP is the default client setup for earlier versions of Windows when creating VPNs to a remote workplace. It is quick and easy to set up but is less secure than alternatives such as L2TP/IPSec.

Step 1: Create an IP address pool

X family devices use the IP address pool to issue addresses for use by the VPN clients. You must ensure that the IP address pool configuration meets the following criteria:

- The range is part of the security zone within which the PPTP tunnel will terminate.
- The IP address range corresponds to the subnets on the terminating security zone.
- The address range does not conflict with other static or DHCP IP pools.

STEP 1 From the navigation panel, select **Network > IP Address Groups**. Create an address group, and give it a name such as PPTP_Pool.

STEP 2 Select the method to specify the address group, such as **IP Range**. Then, type the range; for example, **192.168.1.10 to 192.168.1.201**.

STEP 3 Click **Add to table below** to enter that range.

STEP 4 Add more ranges, subnets, or hosts as required.

STEP 5 Click **Create** to save your changes.

Step 2: Configure and enable the PPTP server on the device

STEP 1 From the navigation pane, select **VPN > PPTP Status > Server Configuration**.

STEP 2 Click **Enable PPTP Server**.

STEP 3 Set **PPTP Security Zone** to **LAN**.

STEP 4 Select **Require Encryption** to enable MPPE.

STEP 5 Enter any DNS and WINS settings.

STEP 6 Select the IP Address Group created previously.

STEP 7 Click **Apply**.

Step 3: Verify firewall rules

Perform this step if you are using multiple security zones, have changed the terminating zone from LAN, or have changed the rules for traffic allowed to the X family device from the WAN.



Note Firewall rules are evaluated from the top down.

- STEP 1** Verify that firewall rules have been configured to allow traffic to and from other security zones and the security zone you have set for the PPTP Server.
- STEP 2** Verify that a firewall rule has been configured to allow IPSec tunnel traffic to the WAN security zone.

Step 4: Create a user account

Only a user with Super-user security level can create a user account.

- STEP 1** From the navigation pane, select **Authentication > User List**.
- STEP 2** On the User List page, click **Create A New User**.

Figure 7-7: Authentication - User Details

The screenshot shows a web interface for creating a user. At the top, it says 'AUTHENTICATION » Create User'. Below that is a blue header with 'Enter User Information'. There is an information icon. The form has several fields: 'Username' with a text input box; 'User Type' with two radio buttons, 'TOS User' (selected) and 'Local User'; 'Access Level' with a dropdown menu set to 'Operator'; 'Privilege Group' with a dropdown menu set to 'RADIUS'; 'Password' with a text input box; and 'Confirm Password' with a text input box. At the bottom, there are two buttons: 'Create' and 'Cancel'.

- STEP 3** On the Create User page, enter a **Username**.
The user name is case sensitive.
- STEP 4** For the **User Type**, select **Local User**.
- STEP 5** For the **Privilege Group**, select **Allow_VPN_Access**.
- STEP 6** Enter and confirm the **Password**.
The password is case sensitive.
- STEP 7** Click **Create**.

Step 5: Configure the Windows XP client using dial-up networking

The following instructions are for configuring a Windows XP client for a PPTP connection. For other operating systems such as Mac OS or Linux, see the OS documentation for details on configuring the client for a PPTP connection.

- STEP 1** From the Windows **Start** menu, select **Network Connections**.
- STEP 2** Click **Create a New Connection** to launch the New Connection Wizard.
- STEP 3** Use the following table to complete the New Connection Wizard prompts:

Network Wizard Prompt	Select or type...
Connection Type	Connect to the network at my workplace
Network Connection	Virtual Private Network connection
Connection Name	Type a connection name
Public Network Setting	Do not dial the initial connection
VPN Server	Type the public WAN IP address of the T10 device
Connection Availability	Select Anyone's use or My use only
Completing the New Connection Wizard	Finish

- STEP 4** After creating the connection, you are prompted to connect for the first time. To connect, type the username and password you created for the user account that you created previously.
- STEP 5** After connecting, 3Com recommends that you complete the following steps to force the client to use PPTP even though this is the default setting that Windows XP will use:
- STEP A** From the Windows **Start** Menu, select **Network Connections**.
- STEP B** Select the connection for the PPTP tunnel and right click.
- STEP C** Click Properties. Then, select the **Networking** tab.
- STEP D** Under Type of VPN, select **PPTP VPN** from the pull-down list.
- STEP E** Click **OK**.
- STEP 6** On the Network Connections page, double-click the connection to establish the VPN tunnel.

Troubleshooting L2TP/IPSec Connections

If the L2TP tunnel cannot be established or does not operate correctly, use the following diagnostic techniques to troubleshoot the problem:

- In the LSM client, verify that the IPSec Security Association (SA) is set to **Enable IPSec tunnel connections**.
- Verify that the **Enable GRE and L2TP** is checked in the IPSec SA.
- If using a DES encryption proposal, ensure that the **Diffie-Hellman Group** on both Phase 1 and Phase 2 is set to 1 (768 bits) before clicking Save. Unless set back to Group 1, the LSM will always set

the DH Group to 2 when Save is clicked in the IKE proposal edit screen. This will cause problems for other products using low encryption (such as Windows XP IPsec clients) that expect to use DH Group 1 with DES.

- If using RADIUS, check the RADIUS troubleshooting section in Troubleshooting RADIUS Authentication.
- Verify that the firewall rules allow:
 - IPsec from the WAN to this-device.
 - L2TP from the zone configured in L2TP Server to this-device for service L2TP.
 - From this-device to ANY for ANY service. A more specific rule is possible but this is recommended for many reasons.
- Review the Block Log on the device to see if the connection is being refused. You may have to enable logging on the Block firewall rules that you suspect may be blocking the request.

PPTP Configuration

Point-to-Point Tunneling Protocol (PPTP) is an encrypted VPN protocol like IPsec, although not as secure as IPsec. PPTP does not support gateway-to-gateway connections and is only suitable for connecting remote users. A **PPTP server** can terminate PPTP connections from VPN clients, such as those included with Windows 2003.

You can configure the X family device to act as a PPTP server for VPN termination that is compatible with Windows PPTP VPN clients. The PPTP server function also supports MPPE 128-bit encryption.

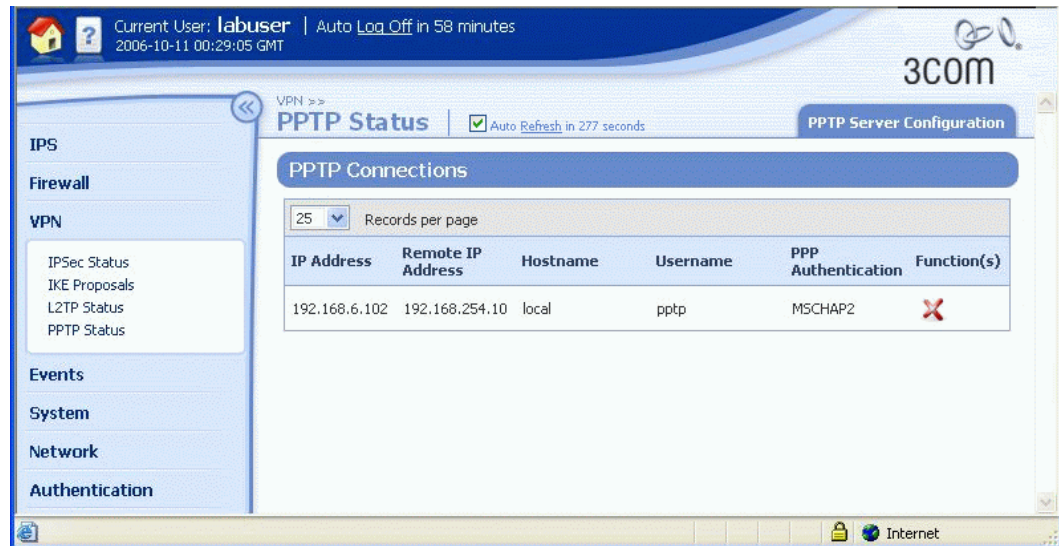
PPTP Status Page

You can view and manage PPTP connections and configuration from the PPTP Status page (**VPN > PPTP Status**). From this page, you can complete the following tasks:

- Viewing current PPTP connections on the device
- Terminating a current connection
- Accessing the PPTP Server Configuration page to enable and configure the PPTP server

The following figure shows the PPTP Status page:


Figure 7–8: PPTP Status Page



PPTP Status Page Details

On the PPTP Status page, the **PPTP Connections** table provides the following information about current connections:

Table 7–8: PPTP Status Page Details

Column	Description
IP Address	The IP address allocated to the PPTP client.
Remote IP Address	The public IP address of the PPTP client.
Hostname	The name of the device hosting the PPTP client.
Username	The name used by the client for authentication by the local database or RADIUS.
PPP Authentication	The PPP authentication mechanism: PAP , CHAP , MS CHAP , or MS CHAPv2 .
Function(s) 	Icons representing functions to manage the PPTP connection: <ul style="list-style-type: none"> Delete the current connection. Deleting a connection disconnects the remote user using the VPN link.

For additional information, see the following topics:

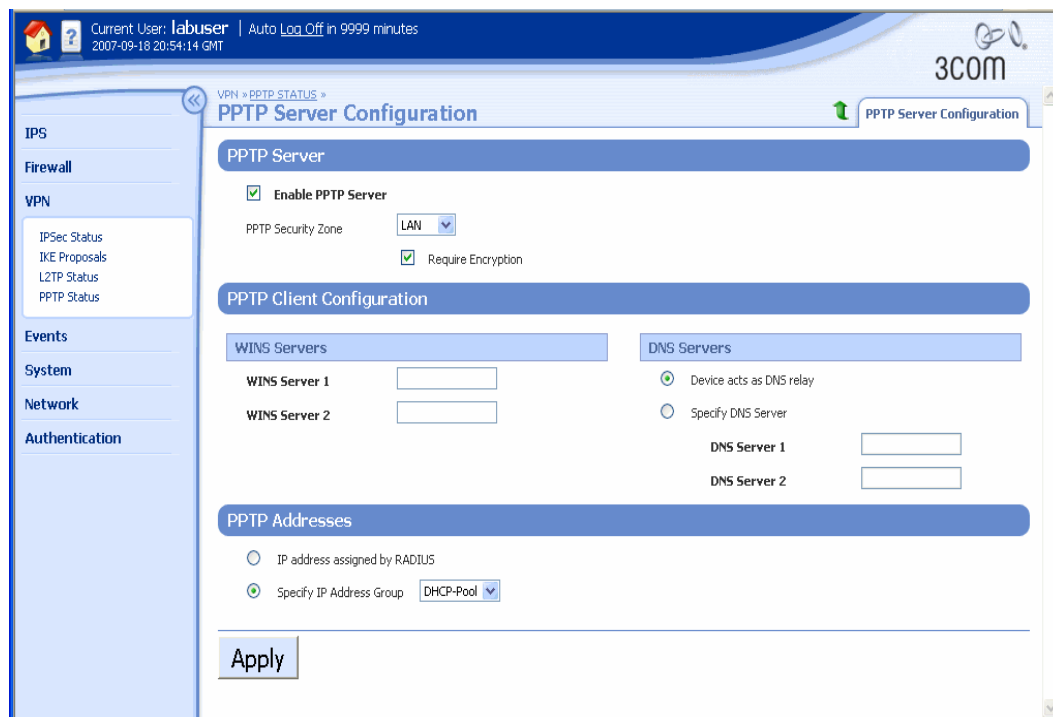
- [“PPTP Server Configuration Page” on page 238](#)
- [“Enabling PPTP server and configuring PPTP client and addresses” on page 239](#)

PPTP Server Configuration Page

You can configure the X family device to act as a PPTP server from the PPTP Server Configuration page (VPN > PPTP Status, PPTP Server Configuration tab).

The following figure shows the PPTP Server Configuration page:

Figure 7–9: PPTP Status: PPTP Server Configuration Page



PPTP Server Configuration Parameters

The following table provides descriptions for the PPTP Server configuration parameters:

Table 7–9: VPN: PPTP Server Configuration Parameters

Parameter	Description
PPTP Server	
Enable PPTP Server	If checked, allows VPN clients to use the device as a VPN terminator for PPTP.
PPTP Security Zone	Select the remote security zone on which to terminate the VPN from the PPTP Security Zone drop-down list.
Require Encryption	If checked, enables Microsoft Point-to-Point Encryption to provide additional security. This feature is supported by Windows VPN clients.
PPTP Client Configuration	

Table 7-9: VPN: PPTP Server Configuration Parameters (Continued)

Parameter	Description
WINS Servers	If you are using Microsoft Networking, type the IP addresses of your primary (WINS Server 1) and secondary (WINS Server 2) WINS servers.
DNS Servers	Determines the DNS servers that the PPTP server uses: <ul style="list-style-type: none"> • Select Device Acts as DNS Relay to enable the device to act a proxy-DNS server (DNS relay), passing DNS queries to its configured DNS servers. • Select Specify DNS Server to enter up to two local DNS server IP addresses, in order in which they are to be accessed, in the DNS Server fields.
PPTP Addresses	Determines how IP addresses are allocated to clients connected through the PPTP server: <ul style="list-style-type: none"> • Select IP address assigned by RADIUS to enable the device to use the RADIUS server to assign the PPTP client IP address. The RADIUS server must be enabled on the RADIUS page (Authentication > RADIUS). • Select IP Address Group and select an existing address group to enable the device to assign the PPTP client an IP address from the addresses included in the IP address group. Use the IP Addresses page (Network > Configuration > IP Address Groups) to create IP address groups.



Note If the PPTP server is disabled, the table is not displayed and the message **PPTP Server is currently disabled** is displayed.

Enabling PPTP server and configuring PPTP client and addresses

- STEP 1** If you are not using RADIUS to assign IP addresses, create an IP address group (**Network > Configuration > IP Address Groups**) containing the pool of IP addresses that the device will use to allocate IP addresses to L2TP VPN clients.
- STEP 2** Select **VPN > PPTP Status**.
The PPTP Status page opens.
- STEP 3** Click the **PPTP Server Configuration** tab.
The PPTP Server Configuration page opens.
- STEP 4** Check **Enable PPTP Server**.
This allows VPN clients to use the device as a VPN terminator for PPTP.
- STEP 5** Select the remote security zone on which to terminate the VPN from the **PPTP Security Zone** drop-down list.
- STEP 6** If you want to use Microsoft Point-to-Point Encryption, check **Require Encryption**.
This provides additional security, and is supported by Windows VPN clients.
- STEP 7** If you are using Microsoft Networking, enter the IP addresses of your primary and secondary WINS servers in the **WINS Server 1** and **WINS Server 2** fields, respectively.

- STEP 8** To configure DNS servers, select one of the following from the **DNS Servers** section:
- If you want the device to act as a proxy-DNS server (DNS relay), passing DNS queries to its configured DNS servers, select **Device acts as DNS relay**
 - If you want to use an external DNS server, select **Specify DNS Server** and enter up to two local DNS server IP addresses, in the order in which they are to be accessed, in the **DNS Server** fields
- STEP 9** To assign PPTP IP addresses, select one of the following:
- If you want the device to use the RADIUS server to assign the PPTP client IP address, select **IP address assigned by RADIUS**
 - If you want the device to use an IP address group for the client, select **Specify IP Address Group** and select an existing group from the drop-down list
- STEP 10** Click **Apply** to save the changes.

Troubleshooting PPTP Connections

If the PPTP tunnel cannot be established or does not operate correctly, use the following diagnostic techniques to troubleshoot the problem.

- If you get an invalid username/password error:
 - Check the Local User username/password configured on the device matches the credentials entered on the VPN client.
- If the client gets no response at all from the device:
 - Verify that the IP address configured for the PPTP client matches that of the external interface of the device.
 - Verify that the firewall policy rules allow PPTP and GRE as appropriate from the *WAN* zone to *this-device*. It is worth checking the Block Log on the device to see if the connection is being refused. This may require you to enable Logging on the Block firewall rules that you suspect may be blocking the request.
 - On the Windows client try forcing the VPN type to PPTP in Network Properties.
- If the client gets logged in but traffic does not flow:
 - Verify that the local user on the device has been configured with *Allow_VPN_access* privileges in the **Authentication > User List** dialogs.
 - Verify that the terminating zone for the PPTP Server is associated with an internal virtual interface. For a Full Transparent Mode deployment you only have the external virtual interface, but you must verify that the terminating zone is not the WAN zone. Has the correct DNS server information been configured for the PPTP server?
 - Verify that all firewalls on the client PC or between PC and the device are configured to allow GRE traffic.
 - Try disconnecting and re-connecting.



Note Check the Block Log on the device to see if the connection is being refused. This may require you to enable “Logging” on the Block rules in the firewall that you suspect may be blocking the request.

8 System

The System menu provides options to update and manage TOS and Digital Vaccine packages, configure timekeeping options, access for remote management applications (SMS and third-party NMS systems), enable high availability to provide system failover, configure email and syslog servers, and access the Setup Wizard to change device and network configuration settings.

Overview

The System menu lets you manage TOS and Digital Vaccine packages, change device configuration options, and configure access to external resources such as syslog and email servers and remote management applications. The System menu provides the following options:

- **Update** — View current software versions, update software, configure automatic Digital Vaccine (DV) updates, and manage system snapshots.
- **Time Options** — Specify the timekeeping mechanism (internal clock or NTP) and time zone for the X family device.
- **SMS/NMS** — Enable remote management of the device.
- **High Availability** — Configure the device for high availability to provide a failover mechanism to minimize network downtime due to device failure.
- **Thresholds** — Specify the disk and memory usage settings that trigger major and critical usage level alarms on the Health Monitor and System Summary pages.
- **Email Server** — Configure the email server for the device to send event notifications.
- **Syslog Servers** — Configure remote syslog servers to maintain and backup data from the System, Audit, VPN, and Firewall Session logs.
- **Setup Wizard** — Configure critical device configuration settings to quickly install a new X family device on the network with Internet access. The setup wizard can be reused to change system-wide configuration settings after the initial configuration is complete.

For details, see the following sections:

- [“Updating TOS and Digital Vaccine Software” on page 242](#)
- [“Time Options” on page 254](#)
- [“Security Management System \(SMS\)” on page 258](#)
- [“High Availability” on page 260](#)
- [“Thresholds to Monitor Memory and Disk Usage” on page 265](#)
- [“Email Server” on page 266](#)
- [“Syslog Servers” on page 267](#)
- [“Setup Wizard” on page 268](#)

Updating TOS and Digital Vaccine Software

For up-to-date network protection, the following update options are provided:

- TOS update package for the IPS firmware and software
- Digital Vaccine Filter update package for IPS filters to provide protection for new and emerging network security threats

You can download software updates from the Threat Management Center (TMC) Web site (<https://tmc.tippingpoint.com>). Register for a TMC account from [eSupport.3com.com](https://esupport.3com.com). To create an account, you need the serial number of one of your X family devices and your customer ID. If you don't have the customer ID, contact your customer representative.

In the LSM, you can manage system software and Digital Vaccine filter packages from the Update page available on the System menu. From this page, you can perform the following tasks:

- Viewing current device information, installed TOS and Digital Vaccine version information, and a list of previously installed software
- Deleting previous TOS versions to free disk space
- Performing a software rollback
- Downloading and installing a TOS or DV update
- Configuring the Auto DV update function
- Creating and managing System Snapshots

The following figure shows the Update page:

Figure 8–1: Update Page

The screenshot shows the 3COM Update page. The top navigation bar includes 'TOS/DV Update', 'Auto DV Config', and 'System Snapshots'. The main content area is divided into three sections:

- Device Information:**
 - Product Code: 3CRTPX506-96
 - Serial Number: X-X506-STLAB-0034
- Current Installed Versions:**

Type	Version	Package Size	Function(s)
TOS Software	2.5.0.6667	23 MB	🔄
Digital Vaccine	2.5.0.6824	824 KB	
- Previous TOS Versions:**

Type	Version	Package Size	Function(s)
TOS Software	2.5.0.6665	23 MB	✗
TOS Software	2.5.0.6657	23 MB	✗

For additional information, see the following topics:

- [“Viewing and Managing Current TOS and DV Software” on page 243](#)
- [“Rolling back to a previous TOS version” on page 244](#)
- [“Deleting a previously installed TOS version” on page 245](#)
- [“Downloading and Installing a TOS or DV Update” on page 246](#)
- [“System Snapshots” on page 251](#)



Viewing and Managing Current TOS and DV Software

The Update page provides information on the software for the X family device. From this page, you can complete the following tasks:

- Viewing information on the device model and on current and previously installed software versions
- Performing a software rollback
- Accessing the TOS/DV Update, Auto DV Config, and System Snapshot functions

The Update page provides the following information about the device and its software state:

Table 8- 1: Update Page Details

Field	Description
Device Information:	
Product Code	The manufacturing code assigned to the device.
Serial Number	The serial number of the device. This number can be used to create an account to access the TMC Web site. You may also need this number when you contact Technical Support.
Current Installed Version:	
Type, Version, Package Size	Identifies the properties of the current TOS software and Digital Vaccine versions installed on the device. Any functions available are listed in the function(s) column.
Function(s): 	Any functions available are listed in the function(s) column. The rollback icon indicates that there is at least one prior version of the software on the device that you can roll back to. For details, see “Rolling back to a previous TOS version” on page 244 .
Previous TOS Versions:	
Type, Version, Package Size	Identifies the properties of previous TOS software packages that have been installed on the device. You can delete TOS software and Digital Vaccine versions installed on the device. Any functions available are listed in the function(s) column.
	If you delete all previously installed TOS software versions, you cannot perform a software rollback.

Rolling back to a previous TOS version



CAUTION To make sure you understand the effects of a software rollback, read the release notes for the current software version and the software version you are rolling back to before performing the rollback operation.

A rollback operation reverts the currently running software version on the device to a previous working version. The device retains settings and configurations. However, not all functions may be available depending on the version of the TOS you roll back to. For details, see the release notes for that version of the software.

When you perform a rollback of the software, the Update page displays a set of status messages. See [“System Update Status Messages” on page 328](#) for details.

Persistent Settings

When you perform a TOS rollback, your current configuration settings are preserved, but filter settings roll back to the settings that were in effect when the rollback version was archived. Any changes to filter

setting made after your target rollback version are deactivated, including attack protection filter updates.

Performing a software rollback



CAUTION If you perform a rollback, read the release notes for both the software version you are rolling back from and the software version you are rolling back to.



Note When you update and roll back, the LSM does not lose your settings or configurations.

STEP 1 From the navigation pane, select **System > Update**.

The Update page opens.

STEP 2 In the **Current Installed Versions** section, click the **Rollback** icon in the **Function(s)** column for the TOS Software.

A confirmation message is displayed.

The device deletes the current TOS files and reinstalls the previous TOS files. When the installation is complete, the device performs a soft reboot.

STEP 3 After the device installs the previous TOS version, log back into the LSM.

To restore the TOS version you rolled back from, you will need to reload it on the device. For more information, see the following topics:

- [“Software Update Process Overview” on page 249](#)
- [“Installing a software update” on page 250](#)

Deleting a previously installed TOS version




CAUTION Unless the device is out of disk space, do not delete the previous TOS image that you were running. If the current TOS image becomes corrupted, you can roll back to the previous version, as explained in [“Performing a software rollback” on page 245](#).

STEP 1 From the navigation pane, select **System > Update**.

The Update page opens.

STEP 2 In the **Previous TOS Versions** section, review the list of previous versions and decide which is safe to delete. Typically, there may be several versions. It is safest to delete the older files.

You may want to keep the most recent version in case you need to perform a software rollback.

STEP 3 Click the  icon in the **Function(s)** column for the TOS software package to delete.

A confirmation message is displayed.

STEP 4 Click **OK**.

Downloading and Installing a TOS or DV Update

You can download and install TOS and DV updates from the TOS/DV Update page.

When downloading and installing a software or Digital Vaccine package, verify that the package you download is not larger than the listed amount of free space. An unpacked package may require more space than anticipated, depending on your device model, saved snapshots and rollback versions, and the size of the available update. To make sure the device has enough disk space, you can delete previously installed software images from the Update page.

For additional information, see the following topics:

- [“Updating Digital Vaccine \(Filters\)” on page 246](#)
- [“Updating the TOS Software” on page 248](#)

Updating Digital Vaccine (Filters)

When new types of network attack are discovered, or when detection methods for existing threats improve, the Digital Vaccine team at the Threat Management Center (TMC) creates and releases new filters to add to your filter database. These filters are released as Digital Vaccine (DV) packages.

When a new DV package is available for download, the TMC team sends notifications to existing customers. You have two options to update the DV on your device:

- Configure the Auto DV option on your device so that the device can check for new DV packages and automatically update the device as necessary.
If AutoDV is configured, the device automatically checks the DV version when you open the Auto DV Configuration page. The status is listed in the **Auto Update** section. To perform an update immediately, click **Update Now**.
- Manually download and install the DV package.

You can manually download the most current DV from the Threat Management Center, and then manually install the DV update.



Note You cannot roll back to a previous Digital Vaccine version. If you want to use a previous version of a Digital Vaccine, select an older version of the Digital Vaccine package from the TMC.

To make sure the device has enough disk space, you may need to delete previously installed software images from the Update page. For details, see [“Deleting a previously installed TOS version” on page 245](#).

Enabling Auto Update for Digital Vaccine

STEP 1 From the navigation pane, select **System > Update**.

The Update page opens.

STEP 2 Click the **Auto DV Config** tab.

The Auto DV Config page opens.

STEP 3 In the **AutoDV** section, click the **Enabled** check box to turn on the option.

When you select the check box, scheduling fields appear so you can establish a DV update schedule:

- STEP 4** To set a Periodic update:
- STEP A** Select **Periodic**.
 - STEP B** Enter the interval number of days.
 - STEP C** Select a day of the week to begin the interval from.
 - STEP D** Select the hour and minute for the update to be performed (in 24-hour time).
- STEP 5** To set a Calendar update:
- STEP A** Select **Calendar**.
 - STEP B** Select a day of the week to perform the update.
 - STEP C** Select an hour and minute for the update to be performed (in 24-hour time).
- STEP 6** Click **Apply**, or to perform an update immediately, click **Update Now**.

Manually downloading a DV update

- STEP 1** From the navigation pane, select **System > Update**.
The Update page opens.
- STEP 2** Click the **TOS/DV Update** tab.
The TOS & DV Update page opens.
- STEP 3** In Step 1, click **Threat Management Center** to access the Threat Management Center.
- STEP 4** Log in to the Threat Management Center. If necessary, create an account from the login page.
The TMC home page opens.
- STEP 5** From the top menu bar, select **Releases > Digital Vaccine** to display the list of Digital Vaccine filters available.
- STEP 6** Click on the software update that you want to download.
The Software Details page opens.
- STEP 7** Review the information about the package.



Note For DV packages, you cannot roll back to a previous version. To use a previous version, download that version from the TMC.

- STEP 8** Click the **Download** tab to download the package to your local device. Make sure to note the download location and the file size.

Manually installing a DV update

- STEP 1** From the navigation pane, select **System > Update**.
The Update page opens.

STEP 2 Click the **TOS/DV Update** tab.

The TOS & DV Update page opens.

STEP 3 In the Step 2 section, locate the line that says “Make sure the file you downloaded is smaller than: *number* MB.”

- If the update package that you downloaded is smaller than *number*, proceed to Step 3.
- If the update package is larger than *number*, delete older versions of the software to free disk space. For details, see [“Deleting a previously installed TOS version” on page 245](#). After freeing disk space, return to the TOS & DV Update page and repeat steps 1 to 3.

STEP 4 In the Step 3 section, check **Enable High Priority Preference** if there is an immediate need for the update, and it is during normal working hours. This setting will give requests from the update process the highest system priority until the update completes.



Note The Enable High Priority Preference option provides the priority for downloading the package. However, the device does not give package installation processes priority over attacks. If an attack occurs during an update, the device does not give priority to the update process.

STEP 5 In the Step 4 section, type the full path and file name for the update package that you downloaded in the **Package File** field, or click **Browse** to select the file.

STEP 6 Click **Install Package**.

While the new file is loaded onto your device, an Update Progress page displays the current status of the update. After the installation completes, you are returned to the Update page. The new version displays in the **Version** column of the **Current Installed Versions** table.

Updating the TOS Software

When improvements or additions are made to the X family software, we release a software update on the TMC Web site (<https://tmc.tippingpoint.com>). You can download and install updates from this site.



CAUTION You must read the release notes posted with the TOS software update package on the TMC. The release notes contain information that may make the difference between a successful software update and an unsuccessful software update.

When you perform an update of the software, the Update page displays a set of status messages. See [“System Update Status Messages” on page 328](#) for details.

Persistent Settings

When you perform a software update, your current configuration and filter settings are carried forward.



Note When you install a software update, an archive copy of your current filters settings is saved. If you perform a software rollback in the future, any changes made to your filters settings after the update are not preserved.

During a graceful shutdown, as during an update or reboot (in the LSM or the CLI), Packet Trace data may not be automatically written to disk. To ensure that Packet Trace data is written to disk, do the following:

- Click on any Packet Trace icon in the alert or block logs
- Click on the Packet Trace (TCPDUMP) icon

Software Update Process Overview

The update procedure takes approximately 30 minutes for the entire procedure, depending on your download speed. The following table provides a summary of the process with time estimates.

Step	Task	Manual or Automatic	Estimated Time	Link Status
1	Download the package	Manual	Varies	Up
2	Install the package	Manual	15–20 minutes	Up
3	Reboot the device	Automatic	5 minutes	Down
4	Commit and update the changes	Automatic	A few seconds	Down

Downloading a TOS software update

- STEP 1** From the navigation pane, select **System > Update**.
The Update page opens.
- STEP 2** Click the **TOS/DV Update** tab.
The TOS & DV Update page opens.
- STEP 3** In the Step 1 section, click **Threat Management Center** to access the Threat Management Center.
- STEP 4** Log in to the Threat Management Center. If necessary, create an account from the login page.
The TMC home page opens.
- STEP 5** From the top menu bar, select **Releases > Software > modeltype > modelnumber**.
The model number and type of your device is displayed on the LSM home page.
- STEP 6** Click on the software update that you want to download.
The Software Details page opens.
- STEP 7** Review the information about the package and click the **Download** tab to download the package to your local device. Make sure to note the download location and the file size.
- STEP 8** After you have downloaded the update, you can install it from the LSM Update page. For details, see [“Installing a software update” on page 250](#)

Installing a software update



CAUTION Prior to installing the new software, back up any custom filters you have created and implemented. The update will overwrite these files.

- STEP 1** If necessary, download a software update package from the TMC. For details, see [“Downloading a TOS software update” on page 249](#)
- STEP 2** From the navigation pane, select **System > Update**.
The Update page opens.
- STEP 3** Click the **TOS/DV Update** tab.
The TOS & DV Update page opens.
- STEP 4** In the Step 2 section, locate the line that says “Make sure the file you downloaded is smaller than: *number* MB.”
- If the update package that you downloaded is smaller than *number*, proceed to Step 5.
 - If the update package is larger than *number*, delete older versions of the software to free disk space. For details, see [“Deleting a previously installed TOS version” on page 245](#). After freeing disk space, return to the TOS & DV Update page and repeat step 4.
- STEP 5** In the Step 3 section, check **Enable High Priority Preference** if there is an immediate need for the update, and it is during normal working hours. This setting will give requests from the update process the highest system priority until the update completes.



Note The High Priority Enabled option provides the priority for downloading the package. However, the device does not give package installation processes priority over attacks. If an attack occurs during an update, the device does not give priority to the update process.

- STEP 6** In the Step 4 section, type the full path and file name for the update package that you downloaded in the **Package File** field, or click **Browse** to select the file.
- STEP 7** Click **Install** to install the software update.

When updating the software, the bar showing update progress may be interrupted by a pop-up message window. If this occurs, you will need to monitor the update process using the system log. If the system log does not show any errors during the update process, the device reboots when the update is complete.

When the installation completes, the device performs a soft reboot. After the reboot, you can log back in to the device.



CAUTION During LSM installation, do not close the browser window or navigate off the Update page.

System Snapshots

From the System Snapshots page, you can create, manage, restore, and import local snapshots for the X family device. After restoring a snapshot, the device always restarts.



CAUTION You can apply a single snapshot to multiple devices. However, applying the snapshot to devices managed by an SMS can cause a device ID conflict. Do not apply a snapshot to multiple devices when managed by SMS.

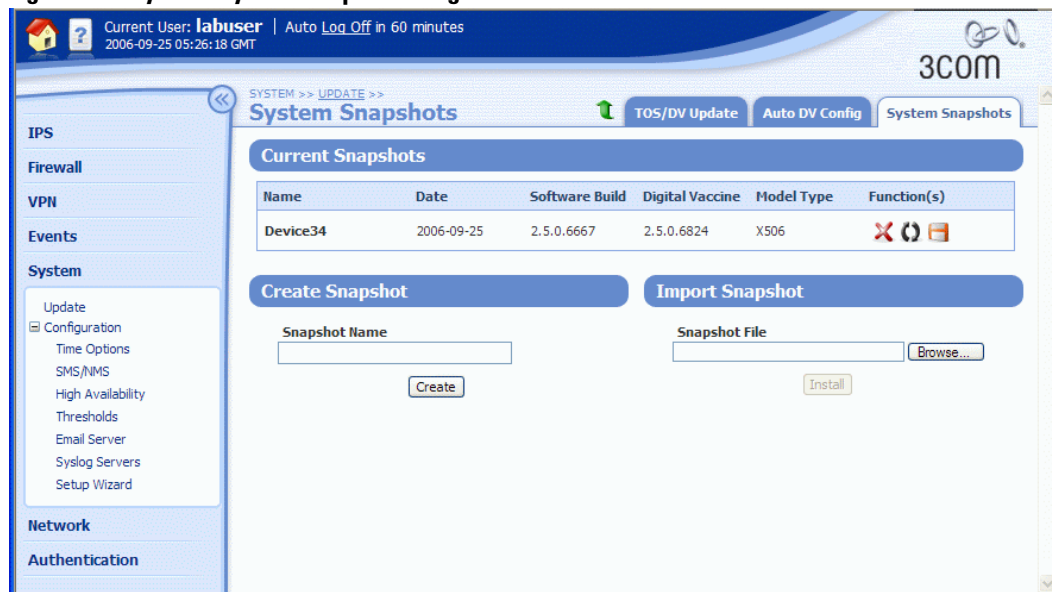
Do not update your software while running a snapshot. The device can experience conflicts.

From this page, you can complete the following tasks:

- [“Creating a snapshot” on page 253](#)
- [“Importing a snapshot” on page 253](#)
- [“Restoring a snapshot” on page 253](#)
- [“Exporting a snapshot” on page 253](#)
- [“Deleting a snapshot” on page 254](#)




The following figure shows the System Snapshots page:

Figure 8–2: System: System Snapshots Page



The System Snapshots page provides the following information:

Table 8- 2: System Snapshots Details

Column	Definition
Name	Name of the snapshot.
Date	The date the snapshot was generated.
Software Build	The build number for the TOS software running when the snapshot was generated.
Digital Vaccine	The version number of the Digital Vaccine package running when the snapshot was generated.
Model Type	The model name of the device on which the snapshot was generated.
Function(s)	Icons representing functions to manage snapshots. The following functions are available: <ul style="list-style-type: none">  • Delete a snapshot  • Restore a snapshot  • Import a snapshot

Creating a snapshot

STEP 1 From the navigation pane, select **System > Update**.

The Update page opens.

STEP 2 Click the **System Snapshots** tab.

The System Snapshots page opens.

STEP 3 In the **Create Snapshot** section, type a name for the snapshot.

STEP 4 Click **Create**.

Importing a snapshot

STEP 1 From the navigation pane, select **System > Update**.

The Update page opens.

STEP 2 Click the **System Snapshots** tab.

The System Snapshots page opens.

STEP 3 In the **Import Snapshot** section, type the snapshot file name into the **Snapshot File** field, or click **Browse** to select the file to import.

STEP 4 Click **Import**.

The selected snapshot uploads and displays in the list of snapshots.

Restoring a snapshot

STEP 1 From the navigation pane, select **System > Update**.

The Update page opens.

STEP 2 Click the **System Snapshots** tab.

The System Snapshots page opens.

STEP 3 In the **Current Snapshots** table, locate the snapshot you want to restore.

STEP 4 In the **Function(s)** column, click  (**Restore**). When you restore a snapshot, you replace all current settings with those from the snapshot.

After restoring a snapshot, the device restarts.



CAUTION You can apply a single snapshot to multiple devices. However, applying the snapshot to devices managed by SMS can cause a device ID conflict. Do not apply a snapshot to multiple devices when managed by SMS.

Exporting a snapshot

STEP 1 From the navigation pane, select **System > Update**.

The Update page opens.

STEP 2 Click the **System Snapshots** tab.

The System Snapshots page opens.

STEP 3 In the **Current Snapshots** table, locate the snapshot you want to export.

STEP 4 In the **Function(s)** column, click  (**Export**). When you export a snapshot, you save the snapshot to a local directory to later import if needed.


Deleting a snapshot

STEP 1 From the navigation pane, select **System > Update**.

The Update page opens.

STEP 2 Click the **System Snapshots** tab.

The System Snapshots page opens.

STEP 3 In the **Current Snapshots** table, locate the snapshot you want to delete and click  (**Delete**).

Time Options

The X family device uses the system time in log files and also for schedule-based firewall rule configurations. To ensure log file accuracy, facilitate log analysis, and establish predictable scheduling, configure the correct time zone and timekeeping mechanism before using the device in a live environment.

Use the Time Options page (**System > Configuration > Time Options**) to configure the following time zone and timekeeping mechanisms for the device:

- **Internal Clock** — Configures the device to keep time independently using its internal clock.
- **NTP Server** — Configures the device to synchronize its internal clock by querying user-defined Network Time Protocol (NTP) servers.
- **Time Zone** — Logs are kept in Universal Time (UTC or Greenwich Mean Time). Use this option to configure the time zone so that log times are translated into local values when displayed.

The following figure shows the Time Options page:

Figure 8–3: Time Options Page

For additional information, see the following topics:

- [“Internal Clock” on page 255](#)
- [“NTP Server” on page 256](#)
- [“Time Zones” on page 257](#)

Internal Clock

Setting the internal clock time

STEP 1 From the navigation pane, select **System > Configuration > Time Options**.

The Time Options page opens.

- STEP 2** In the **Clock Source** section, click **Internal Clock**.
- STEP 3** To automatically populate the date and time settings, do one of the following:
- Click **Set to Local Browser Time**.
 - Type the **Date** and **Time** in the formats specified next to the fields.
- STEP 4** Click **Apply**.

NTP Server

To synchronize the system time with an external time server (NTP server), select NTP as the clock source for your device. The device synchronizes time with the NTP server, which allows the timing of network events on different hosts to be compared more accurately.



TIP To ensure that event times from different network entities can be meaningfully compared, configure the same NTP clients for all X family and other network devices.



CAUTION Using external NTP servers could possibly make your device susceptible to a man-in-the-middle attack. It is more secure to use an NTP server on a local, protected network.

The following table provides information on the NTP protocol configuration parameters:

Table 8- 3: NTP Protocol Configuration Parameters

Parameter	Description
Duration	Interval at which the device will check with the time server. A zero value will cause the time to be checked once on boot.
Offset	If the difference between the new time and the current time is equal to or greater than the offset, the new time is accepted by the device. A zero value will force time to change every time the device checks.
Fast Sync	If this field is set to 1, the device is allowed to trust the NTP server after the first time query. This sets the local time on the device immediately, but there is a risk that the time set will be incorrect. To disable this option, set this value to 0.
Server Host and Port	The IP address and port for the NTP server.
Peer Host and Port	The IP address and port for a symmetric NTP service peer.

Configuring the device for NTP servers

- STEP 1** From the navigation pane, select **System > Configuration > Time Options**.
The Time Options page opens.
- STEP 2** In the **Clock Source** section, click **NTP protocol**.

STEP 3 Type the **Server Host** IP address and **Port** for the NTP server. Then, click **Add to table below**.

You can add multiple NTP server hosts.

STEP 4 In the **Duration** field, type the interval (in minutes) at which the device will check the time server (the default is 5 minutes).

Type 0 to cause the time to be checked once at device startup.

STEP 5 In the **Offset** field, type the allowable time difference between the server time and the current time (the default is 1).

If the difference between the new time and the current time is equal to or greater than the offset, the device accepts the new time. Type 0 to force the time to change every time the device synchronizes with the server.

STEP 6 In the **Fast Sync** field, type 1 to allow the device to trust the NTP server after the first time query and immediately update the time.

For more accurate time synchronization, type 0 to disable the Fast Sync option.

STEP 7 For each symmetric NTP server peer, type the **Peer Host** and **Port**. Then, click **Add to table below**.

STEP 8 Click **Apply**.

Time Zones

Use the Time Zone configuration option to specify the time zone. The default time zone for the device is GMT (Greenwich Mean Time or Universal Time). If you change the default, logs will display time data based on the specified time zone.

Setting the time zone

STEP 1 From the navigation pane, select **System > Configuration > Time Options**.

The Time Options page opens.

STEP 2 In the **Time Zone** section, select the time zone from the drop-down list.

STEP 3 Optionally, click **Automatically adjust clock for daylight saving changes**.

STEP 4 Click **Apply**.

Security Management System (SMS)

From a Security Management System (SMS), you can remotely monitor and manage multiple X family devices. When an SMS is managing a device, you can view, manage, and edit the device configuration, and review logs and reports. You can also configure security zones and security policy (firewall rules, IPS filters, and traffic threshold filters) from the SMS and distribute the configuration to multiple X family devices.

When a device is under SMS management, the message (DEVICE UNDER SMS CONTROL) displays in red at the top of each page in the LSM. In this state, you can view system configuration and status but editing is not available with the exception of Authentication configuration. The serial number and the IP address of the controlling SMS are displayed on the SMS & NMS page.

Configure and manage SMS systems from the SMS & NMS page in the LSM. For more information, see the following topics:

- [“Configuring SMS information” on page 259](#)
- [“Disabling or enabling SMS management” on page 260](#)
- [“Management by Third-Party NMS Software” on page 260](#)

The following figure shows the SMS & NMS page:

Figure 8–4: SMS & NMS Page

Current User: labuser | Auto Log Off in 44 minutes
2006-09-22 19:18:13 GMT

3COM

SYSTEM >> CONFIGURATION >>
SMS & NMS

Configure SMS

SMS Authorized IP Address/CIDR: 10.100.230.1/24

SMS Control: Enabled

SMS Serial#: X-SMA-DEV-SMS28-0001

SMS IP Address: 10.100.230.128

SMS Port: 8162

SNMP V2: Enabled

NMS Settings

NMS Community String: [Text Field]

NMS Trap IP Address: [Text Field]

NMS Trap Port: [Text Field]

Add to table below

NMS Trap IP Address	NMS Trap Port
---------------------	---------------

Apply



CAUTION Communication between the X family device and the SMS or NMS is managed by the SNMP server, which provides access to interface counters and other statistics, configuration data, and general system information. You enable the SNMP server by selecting the SNMP V2 option during the SMS or NMS configuration process. If you disable this option, SMS or NMS functionality is also disabled.

Additional Configuration Requirements

To communicate with the SMS, you may need to configure firewall rules on the device such that the following protocols are allowed between the device and the zone where the SMS resides:

- **HTTPS** (HyperText Transfer Protocol, Secure) — Protocol for handling secure transactions
- **SNMP** (Simple Network Management Protocol) — Protocol for managing nodes on an IP network and monitoring various types of equipment including computers, routers, and wiring hubs
- **NMS** (Management Management Station) — Protocol for managing the device by a restricted NMS, such as HP OpenView

For more information about configuring the firewall, see [“Firewall” on page 59](#).

Configuring SMS information

STEP 1 From the navigation pane, select **System > Configuration > SMS/NMS**.

The SMS & NMS page opens.

STEP 2 Type an **SMS Authorized IP Address/CIDR**.

The default value is *any*, which means that any SMS can manage the device. To specify a range of IP addresses, enter an IP address block (for example, 10.100.230.0/24). This allows any SMS on the specified IP subnet to manage the device.

STEP 3 Verify that the **SNMP V2** check box is selected.

STEP 4 Click **Apply**.



Note If the device has previously been managed by SMS, the serial number, IP address, and port for SMS displays.

Viewing or configuring NMS information

STEP 1 From the navigation pane, select **System > Configuration > SMS/NMS**.

The SMS & NMS page opens.

STEP 2 In the Configure SMS section, verify that **SMS V2** is enabled.

STEP 3 In the NMS Settings section, type the following:

STEP A An **NMS Community String** that identifies the NMS (1–31 characters).

STEP B An **NMS Trap IP Address**.

STEP C An **NMS Trap Port**.

STEP D Click **Add to table below**.

The NMS address and port information is added to the list. The device will send event and activity notifications as SNMP traps to each specified NMS.

STEP 4 Repeat step 3 for each NMS you want to add.

STEP 5 When you finish, click **Apply**.

Disabling or enabling SMS management

STEP 1 From the navigation pane, select **System > Configuration > SMS/NMS**.

The SMS & NMS page opens.

STEP 2 If the device has never been managed by SMS, the **SMS Control** check box is not available. You can start managing it by logging into an SMS system with an authorized IP address. (For details on configuring an authorized IP address, see [“Configuring SMS information” on page 259](#).)

STEP 3 If the **SMS Control** check box is available, do one of the following:

- To disable SMS management, uncheck **SMS Control**.
- If an SMS serial number and IP address appear, to enable SMS management click **SMS Control**.

Management by Third-Party NMS Software

The X family device supports remote management by third-party network management station (NMS) software. From an NMS, you can remotely monitor the events and system status of the X family device. Configuring an NMS enables applications such as HP OpenView to monitor the device.

High Availability

X family devices support a high-availability configuration to provide a failover mechanism to minimize network downtime due to device failure. High availability allows two X family devices with the same configuration and licensing to be configured as a high availability pair. One device is the active device, forwarding packets; the other is a standby device, constantly monitoring the active device. The standby device automatically shifts from standby to active mode if the active device fails.

Once defined, a high-availability configuration can be synchronized between the primary and secondary X family devices.

Configuration Overview

To use high availability, you need two X family devices of the same type, software version, and encryption level. Configure one unique HA management IP address per virtual interface that can be used to manage the device from the network regardless of whether the device is active or on standby. In addition, 3Com recommends that you configure a HA management IP address for each internal and external interface on the device. The IP addresses must conform to the following rules:

- The IP address for the external interface must be a static IP address.
- Each HA management IP addresses must be on the same IP subnet as its respective IP interface.

When the devices are configured for high availability, the devices use the HA management IP addresses to communicate with each other and to monitor their current states.

You configure and manage high availability from the High Availability page (**System > Configuration > High Availability**). From this page you can complete the following tasks:

- [“Setting up devices for high availability” on page 261](#)
- [“Enabling high availability synchronization” on page 263](#)
- [“Synchronizing configurations” on page 263](#)
- [“Forcing a high availability state change” on page 263](#)
- [“Tuning high availability parameters” on page 264](#)
- [“Replacing a high availability device” on page 264](#)
- [“Configuring High Availability with AutoDV” on page 265](#)
- [“Troubleshooting High Availability with AutoDV” on page 265](#)

Setting up devices for high availability



TIP You can use this procedure to enable synchronization for existing X family devices that have been upgraded to support HA configuration synchronization.

- STEP 1** Configure two identical X family devices with the same configuration. Create firewall rules that permit **this-device** to establish an outgoing session with the high availability configuration synchronization TCP port (the default is port 843). An incoming firewall rule is not required unless you change the default port number, which is not recommended.
- STEP 2** Configure the network:
- STEP A** Connect the devices in parallel so that the respective ports on each device are connected together through a switch or similar device.
- STEP B** Shut down any unused ports and leave them disconnected.
- STEP 3** Set up the zones and IP interfaces for the first device.
- STEP A** From the navigation pane, select **Network > Configuration > Security Zones**. Then, verify or create a LAN security zone on Port 1.
- STEP B** Select **Network > Configuration > IP Interfaces**. Then, create an internal interface for the LAN zone with NAT disabled. The IP address for this interface will be the same on both devices.
- STEP C** From the IP Interfaces page, create an external, static IP interface for the WAN zone. The IP address for this interface will be the same on both devices.
- STEP 4** Configure high availability for the primary device:
- STEP A** From the navigation pane, select **System > Configuration > High Availability**. The High Availability page opens.
- STEP B** In the **Communication Channel** table, type an **HA Management IP Address** for at least one interface.

To enable management of the device whether it is in active or standby mode, type a Management IP Address for the internal interface. You can use this address to access the device from the Management IP Address field.

STEP C Verify that the HA management IP address for each IP interface is on the same subnet as the IP interface. Then, ensure that the address specified for every external interface is a static IP address.

STEP D For every interface with an HA Management IP Address specified, type the **HA Peer IP Address** of the secondary device. This is the management IP address of the other HA device.

STEP E When you finish, click **Apply**.

STEP 5 Enable high availability:

STEP A On the primary device, from the navigation pane, select **System > Configuration > High Availability**.

The High Availability page opens.

STEP B In the **State** section, click **Enabled**.

STEP 6 Save the device configuration:

STEP A From the navigation pane, select **System > Update > System Snapshots**.

The System Snapshots page opens.

STEP B Type a file name into the Snapshot Name field and click **Create**.

STEP C Click the **Export** button next to the created snapshot and save the snapshot.

STEP 7 Restore the saved configuration onto the peer HA device:

STEP A Configure a virtual interface IP address to allow network management. This IP address should be different from any IP addresses on the other HA device.

STEP B From the navigation pane, select **System > Update > System Snapshots**.

The System Snapshots page opens.

STEP C Import the snapshot created on the other device.

STEP D Click **Restore snapshot**.

The device restarts. After it restarts, the configuration on both devices is synchronized.

If the Restore snapshot icon does not appear, check on the System Status page that the HA devices are running the same software build and encryption level.

Enabling high availability synchronization

Once you have configured a primary and secondary device for high availability (for details, see [“Setting up devices for high availability” on page 261](#)), you can enable configuration synchronization.

STEP 1 On the primary device, from the navigation pane, select **System > Configuration > High Availability**.

The High Availability page opens.

STEP 2 In the **Configuration Synchronization** section:

STEP A Note the value in the **HA Primary device Serial Number** field.

STEP B Check **Automatically synchronize configuration**.

STEP 3 On the secondary device, from the navigation pane, select **System > Configuration > High Availability**.

The High Availability page opens.

STEP 4 In the **Configuration Synchronization** section:

STEP A Type the primary device serial number in the **HA Primary device Serial Number** field.

STEP B Check **Automatically synchronize configuration**.

Synchronizing configurations

Once you have configured a primary and secondary device for high availability (for details, see [“Setting up devices for high availability” on page 261](#)) and enabled configuration synchronization (for details, see [“Enabling high availability synchronization” on page 263](#)), you can synchronize the configurations.



Note You must synchronize the primary and secondary devices at least once. This procedure causes the secondary device to reboot.

STEP 1 On the primary device, from the navigation pane, select **System > Configuration > High Availability**.

The High Availability page opens.

STEP 2 In the **Configuration Synchronization** section, click **Synchronize configuration now**.

You may have to wait a few minutes until the HA link has been established before you can click this button.

Forcing a high availability state change

If two devices are configured as a high-availability pair, one device is always in active mode while the other is in standby mode. From the High Availability page, you can force a device to change modes.

STEP 1 Log in to one of the devices in the high availability pair.

STEP 2 From the navigation pane, select **System > High Availability**.

The High Availability page opens.

STEP 3 In the **State** section, click **Switch**.

The status display for the local and remote devices reflects the change. It may take a moment for the device to change states.

Tuning high availability parameters

You can tune high availability polling parameters to compensate for network latency issues. Note that if you poll too aggressively, the devices might not have time to receive messages from one another and might switch states unnecessarily.

STEP 1 From the navigation pane, select **System > Configuration > High Availability**.

The High Availability page opens.

STEP 2 Click **Show Advanced Options**.

Additional options appear.

STEP 3 In the **Tuning** section:

STEP A (Optional) Type a new value in the **Polling Interval** field. (The default is 4 seconds.)

STEP B (Optional) Type a new value in the **Retransmission Interval** field. (The default is 100 milliseconds.)

STEP C (Optional) Type a new value in the **Number of Retries** field. (The default is 2 retries.)

STEP 4 In the **Preemption** section, you can specify that the primary device is always the active device (unless it fails). Check **HA Primary device Preempts HA Secondary device**.

STEP 5 When you finish, click **Apply**.

Replacing a high availability device

If the primary device in a high availability pair physically fails, follow this procedure to replace it.

STEP 1 On the secondary device, from the navigation pane, select **System > Configuration > High Availability**.

The High Availability page opens.

STEP 2 In the **Configuration Synchronization** section, reconfigure the **HA Primary device Serial Number** field to be the serial number of the replacement device.

If you fail to perform this step, the devices will be unable to establish communication links.

STEP 3 Click **Apply**.

STEP 4 Export a snapshot created by the secondary device and import it into the replacement device. (For more information, see [“Setting up devices for high availability” on page 261](#).)

If the secondary device in a high availability pair physically fails, export a snapshot created by the primary device and import it into the replacement secondary device. (For more information, see [“Setting up devices for high availability” on page 261](#).)

Configuring High Availability with AutoDV

For the standby device to perform AutoDV, it needs a separate Digital Vaccine license.

The standby device uses the high availability management IP address as the source IP address when doing AutoDV. Therefore, the HA management IP address must be public and routed to the Internet in addition to the external virtual interface IP address. When the active device does AutoDV it uses its external VI address.

If you have a separate NAT device (that is, the Internet side of the device), then there is no need for a public IP address for either device so long as both can route to the Internet.

Troubleshooting High Availability with AutoDV

If the standby device cannot do AutoDV, check for the following:

- Verify that the primary device can do AutoDV. If so, it suggests a routing or licensing issue.
- If the standby device cannot do AutoDV, can it do so if you make the standby device active? If so, it suggests a licensing issue and not a networking issue.
- If the standby device cannot do AutoDV even when it becomes the primary device, and licenses have been checked, it suggests that the standby device has a problem routing to or from the Internet via its high availability management IP address.

Thresholds to Monitor Memory and Disk Usage

From the LSM Health menu (**Events > Health > Monitor**) you can monitor current disk and memory usage levels for the X family device. The Monitor page has a State field that indicates whether usage is at normal, high, or critical levels. The settings that determine these levels are specified on the Thresholds page.

You can specify the following settings for the disk and memory thresholds:

- **Major Level** — Set the major threshold to a level that provides enough time to react before the situation is critical. For example, for disk usage, set a level where the disk is nearly full, but is not so full that system activity is interrupted. The default value for both disk and memory usage is 90%.
- **Critical Level** — Set the critical threshold at a level that warns users *before* damage is about to occur. The default value for both disk and memory usage is 95%.

Setting disk usage and memory thresholds

STEP 1 From the navigation pane, select **System > Thresholds**.

The Thresholds page opens.

STEP 2 Specify the disk and memory thresholds:

STEP A For **Disk Usage Threshold**, enter a numeric value for the **Major Levels** and the **Critical Levels**. The major level value must be set lower than the critical level value.

STEP B For **Memory Usage Threshold**, enter a numeric value for the **Major Levels** and the **Critical Levels**. The major level value must be set lower than the critical level value.

STEP 3 When you finish, click **Save**.

To reset the values to the default settings, click **Reset to Defaults**.

For additional information, see [“Health” on page 117](#).



Note 3Com recommends not modifying these values from their defaults.

Email Server

The X family device can be configured to send an email message when an IPS filter is triggered. The Email Server page lets you configure the default email server settings to provide the email address, domain server, and SMTP address for the messages being sent from the device. After the email server settings have been configured, you can specify the email address contacts from the Notification Contacts page when you create or edit an action set.

The following figure shows the Email Server configuration page:

Figure 8–5: Email Server Page

Configuring the email server

STEP 1 From the navigation pane, select **System > Configuration > Email Server**.

The Email Server page opens.

STEP 2 Type the **Default To Email Address**.

This address displays in the **To Email Address** field when a user creates an email contact from the LSM.

- STEP 3** Type the **From Email Address**.
This address is used as the **Reply-To** address for messages sent from the device.
- STEP 4** Type the **From Domain Name**, such as `Acme.com`.
- STEP 5** Enter the **SMTP Server IP Address**.
The device must be able to reach the SMTP server that will be handling the email notifications. You may have to add static routes (see [“Static Routes Page” on page 169](#)) so that the device can communicate with the SMTP server.
- STEP 6** Enter a value for the **Email Threshold** (the default is 10 per minute).
This limits the numbers of emails sent per minute.
- STEP 7** Click **Test Email** to verify your configuration settings.
- STEP 8** When you finish, click **Apply**.

For additional information on sending emails from the X family device, see [“Notification Contacts” on page 49](#).

Syslog Servers

To maintain and back up all log data from the X family device, you can configure remote syslog servers for system-related logs (System, Audit, VPN, and Firewall Session logs).

For the Firewall Session Log, messages will only be offloaded for firewall rules that have the **Enable syslog logging** option turned on.

The contents of the VPN log can be customized to include messages to troubleshoot problems establishing a VPN tunnel.



Note You can also configure syslog servers for traffic-related event logging (entries in the Alert, IPS Block, and Firewall Block logs). For details, see [“Configuring the remote system log contact” on page 50](#).

Configuring the Syslog Server log contact

- STEP 1** From the navigation pane, select **System > Configuration > Syslog Servers**.
The Syslog Servers page opens.
- STEP 2** Select the **Enable syslog offload** option for each log you want to offload. Then, type the **IP Address** for the remote server.



TIP Be sure that the device can reach the remote system log server on your network. If the server is on a different subnet than the device management port, you may have to add static routes (see [“Static Routes Page” on page 169](#)).

For additional information, see the following topics:

- [“Logs” on page 100](#)
- [“Firewall Session Log” on page 104](#)
- [“VPN Log” on page 105](#)

Setup Wizard

The System Setup Wizard lets you configure system settings. After you set up the hardware (see the *Quick Start Guide* for your device) and navigate to the default address for the LSM, the wizard automatically launches and steps through the configuration process. After the initial configuration, you can re-run the Setup Wizard if necessary by selecting **System > Configuration > Setup Wizard** from the navigation pane.

You can also set up the devices from an ssh command line using the CLI Setup Wizard. The CLI Setup Wizard provides additional options for configuring SMS and NMS management. The CLI Setup Wizard is documented in the *Command Line Interface Reference*.

The following table lists the configuration steps included in the Setup Wizard along with links to documentation on the configuration task.

Table 8–4: Configuration Steps in Setup Wizard

Prompt	Description
Host Name & Location	Enter a name and physical location for the host. The name specified displays in the title bar of the browser window when a user is logged in to the LSM application. The name is also used to identify the device when it is managed by an SMS or NMS system.
Timekeeping Options	Specify the clock source (internal or NTP server) and time zone for the device. For details, see “Time Options” on page 254 .
IP Interfaces	Add or delete the IP interfaces that provide the device with the interfaces to make the network connections required for your environment. An IP interface is the Layer 3 configuration for the device. For details, see “Static Routes Page” on page 169 .
Security Zones	Add or delete the security zones used to segment the network so that the device can apply security policy to traffic passing between the zones. For details, see “Security Zone Configuration” on page 135 .
Security Zone to IP Interface Mappings	Change the IP interface associated with each security zone. Each security zone must be associated with an internal or external IP interface so that it can be reached through the device. For details, see “Managing Security Zones for IP Interfaces” on page 150 .
DNS Settings	Configure DNS servers for the device. For details, see “DNS Page” on page 159 .

Table 8–4: Configuration Steps in Setup Wizard (Continued)

Prompt	Description
Web & CLI Management Options	Specify how the device can be managed: through the LSM, through the CLI via SSH, or both. You can also configure whether the Web interface uses a secure (HTTPS) connection or an insecure HTTP connection.
Ethernet Port Configuration	Configure the line speed and duplex setting for the device's Ethernet ports. For details, see “Network Ports Page” on page 133 .
Email Configuration	Configure the email server so that the device can send event notifications. For details, see “Email Server” on page 266 .

9 Authentication

The Authentication section describes how to create and manage user accounts, configure privilege groups, use a RADIUS or LDAP server, and create X.509 certificates used for VPN authentication.

Overview

The LSM Authentication menu pages enable administrators to create and manage user accounts and configure authentication rules. The Authentication menu provides the following options:

- **User List** — create and manage user accounts to provide access to LSM operators and administrators, and provide local users with access to network services through the X family device
- **Active User List** — display information about logged-in users; log out users as necessary
- **Privilege Groups** — set up access rights for VPN clients and network services protected by firewall rules
- **RADIUS** — configure the device to use an external RADIUS server for user authentication
- **LDAP** — configure the device to use an external LDAP server for user authentication
- **X.509 Certificates** — create, import and manage the CA certificates, certificate requests, and local certificates used for VPN authentication
- **Preferences** — configure session and device timeouts, security level check required for passwords, and account login security

For additional information, see the following topics:

- [“User List Page” on page 272](#)
- [“Active User List” on page 277](#)
- [“Privilege Groups Page” on page 278](#)
- [“RADIUS Page” on page 280](#)
- [“LDAP Configuration Page” on page 282](#)
- [“X.509 Certificates” on page 286](#)
- [“Preferences Page” on page 298](#)
- [“Setting Up User Authentication” on page 301](#)

User List Page

The User List page lets you create and manage user accounts to provide access to LSM operators and administrators and to provide local users with access to network services through the X family device. You can also configure authentication parameters that ensure secure access to the device and network services.

The following topics describe how user accounts and authentication are configured:

- [“TOS and Local User Accounts” on page 272](#)
- [“TOS User Security Level” on page 273](#)
- [“Username and Password Requirements” on page 273](#)

For instructions on using the User List menu options, see the following topics:

- [“Managing User Accounts” on page 274](#)
- [“X.509 Certificates” on page 286](#)

TOS and Local User Accounts

The device supports two types of user accounts: a TOS user account and a local user account.

A TOS user account provides access to the administrative interfaces of TOS to manage the device through either the LSM web interface or from the Command Line Interface (CLI). The management functions available to a TOS user are determined by the account access level configured on the account. TOS users can only be defined in the embedded TOS user database on the device. TOS users cannot be configured in an external server.

A local user account provides controls on client access to network services through the device. Access to services is controlled through the device authentication mechanism. Local users cannot access the TOS administrative interfaces to manage the device. Local users can be authenticated using the embedded user database within the TOS, or can be defined in an external server.

TOS User Security Level

For TOS user accounts, you can configure one of three access security levels:

- **Operator** — Base level user who monitors device and network traffic
- **Administrator** — Enhanced user who can view, manage, and configure functions and options in the device
- **Super-user** — User who has full access to the entire device



Note For local users, access to network services is controlled by privilege groups. For details, see [“X.509 Certificates” on page 286](#).

The following table summarizes the functions available to users based on the Security Level access (Operator, Administrator, or Super-user) assigned to their user account:

Table 9–1: LSM Functions Available to TOS Users Based on Security Level

Functional Area	Operator	Administrator	Super-User
IPS/Quarantine	view	all	all
Firewall	view	all	all
Network	view	all	all
VPN	view	all	all
System	view	all	all
Events/Logs	view (except Audit log)	view all (except Audit log)	all
Update	view	all	all
Configure	view	all except system time	all
Admin	change own password view system log	change own password view system log	all, including: change Idle Timeout change Password Expiration
Help	view	view	view

Username and Password Requirements

Restrictions on username and password values for user accounts are determined by the Security Level setting configured on the Preferences page. Username and password requirements are the same for local users and TOS users.

For the X family device, the default security access level is **Level 2, Maximum Security Checking**. For details on the available security levels and instructions for changing the security level, see [“Preferences Parameter Details” on page 298](#).

The following table provides examples of valid and invalid usernames and passwords based on the default setting for username/password security level (Level 2, Maximum Security Checking):

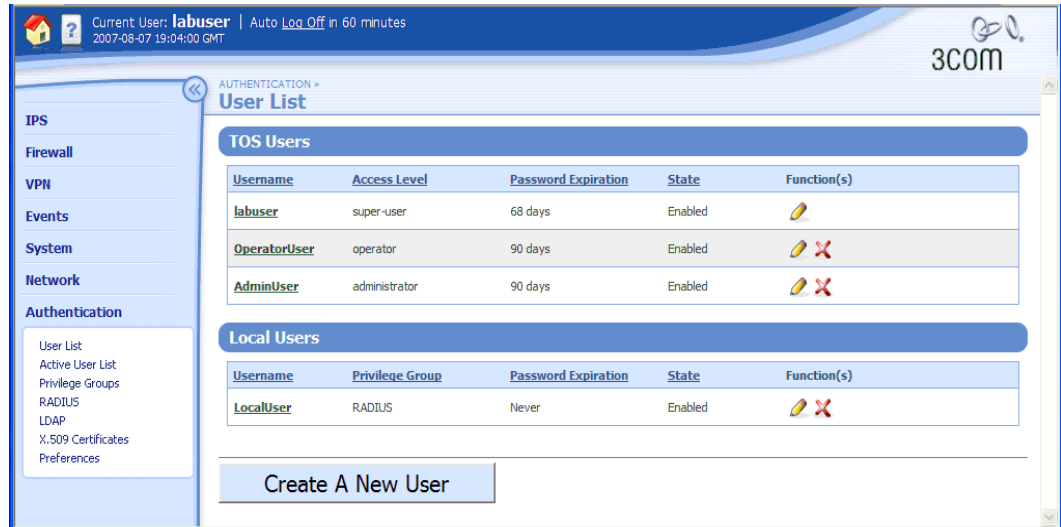
Table 9-2: Username and Password Examples

Valid	Invalid
Username Examples:	
fjohnson	fredj (too short)
fredj123	fred j 123 (contains spaces)
freDj-123	fj123 (too short)
fRedj-*123	fj 123 (contains spaces)
Password Examples:	
my-pa55word	my-pa55 (too short)
my-b1rthday52	my-birthday (must contain a numeric character)
myd*g'snam3	mydogsnam3 (must contain a non-alphanumeric character)

Managing User Accounts

The following figure shows the User List page:

Figure 9-1: User List Page



From the User List page, you can complete the following tasks:

- Creating an account
- Editing an existing account
- Changing a password

User Account Parameter Details

The configuration parameters for user accounts are provided in the following table:

Table 9-3: User Account Parameters

Detail	Description
TOS Users	
Username	The login name used to access LSM management functions. Usernames must be 6 to 31 alphanumeric characters.
Access Level	The Distinguished Name of the Certificate Authority for this CA certificate.
Password Expiration	The number of days remaining until the password expires.
State	Whether the user account is currently disabled or enabled.
Function(s)	<p>The functions available to manage the TOS User account:</p> <ul style="list-style-type: none"> • Delete the account. Only users with a Super-user security level can delete an account. • Edit the user account record to change the password, security level, and enable/disable the account. Only users with a Super-user or Administrator security level can modify another user's account. Operators can only modify their own account.
Local Users	
Login	<p>Username for the account. This is the login name used to access network services through the device.</p> <p>Usernames must be 6 to 31 alphanumeric characters.</p>
Privilege Group	Privilege group to which user account belongs. This determines whether the user has VPN client access and if they are subject to firewall rule authentication and Web content filtering policies. For details, see “X.509 Certificates” on page 286 .
Password Expiration	The number of days remaining until the password expires. When you create an account, the device uses the password expiration period configured from the Preferences page. For details, see “Preferences Page” on page 298 .
State	Whether the user account is currently disabled or enabled.
Function(s)	<p>The functions available to manage the local user account:</p> <ul style="list-style-type: none"> • Delete the account. Only users with a Super-user security level can delete an account. • Edit the user account record to change the password, security level, and enable/disable the account. Only users with a Super-user or Administrator security level can modify another user's account. Operators can only modify their own account.

Creating a new user account in the TOS authentication database

Only a user with Super-user security level can create a user account.

- STEP 1** From the navigation pane, select **Authentication > User List**.
The User List page opens.
- STEP 2** Click **Create A New User**.
- STEP 3** Type a **Username**.
See [“Username and Password Requirements” on page 273](#) for more information.
- STEP 4** Select a **User Type**:
- **TOS User** for administrators
 - **Local User** for users that require access to network services.
- STEP 5** Select the access level for the account:
- For TOS Users, select an Access Level: **Operator, Administrator, Super User**.
 - For Local Users, select a Privilege Group. (For more information about privilege groups, see [“X.509 Certificates” on page 286](#).)
- STEP 6** Type a **Password**.
See [“Username and Password Requirements” on page 273](#) for more information.
- STEP 7** Verify the password by re-entering it in **Confirm Password** field.
- STEP 8** When you finish, click **Create**.

Changing a password

All TOS users can change the password on their own accounts. Only users with Super-user access can change passwords on any account.

- STEP 1** From the navigation pane, select **Authentication > User List**.
The User List page opens.
- STEP 2** On the User List page, click the **Username**.
The Edit User page opens.
- STEP 3** Select the **Change password** check box.
Additional options appear.
- STEP 4** Type a **Password**.
See [“Username and Password Requirements” on page 273](#) for more information.
- STEP 5** Verify the password by re-entering it in **Confirm Password**.
Enter the password exactly as you did in Step 4.
- STEP 6** When you finish, click **Save**.

Active User List

You can manage and active users from the Active User List page. From this page you can complete the following tasks:

- Viewing currently logged in users
- Logging out a user

The following figure shows the Active User List page:

Figure 9–2: Active User List Page



The Active User List page provides the following information:

Table 9–4: Active User List Information

Column	Description
Username	The registered name of the user.
IP Address	Source IP address.
Logged In	When the user logged in.
Login Method	Indicates the login mechanism: local user, authenticated user, or TOS user.
Privilege Group	Name of the privilege group the user is associated with.
Function(s)	The available functions for active users: <ul style="list-style-type: none"> • Delete user

Logging out a user

STEP 1 From the navigation pane, select **Authentication > Active User List**.

The Active User List page opens.

- STEP 2** Click the **Delete** icon for the user to log off.
The user is immediately logged off the device.

Privilege Groups Page

Privilege groups let you set up access rights to specific services on the network that can then be enforced using firewall rules. After a privilege group is created, you can use it in conjunction with a firewall rule to either permit users from this privilege group access to specific services, such as FTP, or block their use of services.

The following types of global privileges can be enabled for users within a privilege group:

- VPN client access
- Firewall rule authentication
- Web filter bypass

The privilege group name is retrieved from the local user database, an LDAP server as the group name or a RADIUS server via a Vendor Specific Attribute (VSA). (For more information, see [“LDAP Configuration Page” on page 282](#) and [“Privilege Groups Page” on page 278](#).) See [Appendix C, “Device Maximum Values”](#) for the maximum number of privilege groups allowed on the device.

You can manage and configure privilege groups from the Privilege Groups page. From this page you can complete the following tasks:

- Viewing currently configured privilege groups
- Deleting a privilege group
- Creating privilege groups
- Adding local users to a privilege group

The following figure shows the Privilege Groups page:

Figure 9–3: Privilege Groups Page

Current User: labuser | Auto Log Off in 60 minutes
2007-10-29 21:00:44 GMT

3COM

AUTHENTICATION »
Privilege Groups

Privilege Group List

25 Records per page

Privilege Group	VPN Access	Firewall Auth	Web Filtering Bypass	Web Filter Profile	Priority	Function(s)
Allow VPN access	Yes	No	No	Default	0	
RADIUS	No	No	No	Default	0	

Create Privilege Group

Privilege Group Parameter Details

The Privilege Groups page provides the following information:

Table 9–5: Privilege Group Information

Column	Description
Privilege Group	The name of the privilege group.
VPN Access	Whether users in the group have VPN client dialup, inter-site VPN access, or Internet access.
Firewall Auth	Whether a user can bypass firewall rules configured for authentication.
Web Filtering Bypass	Indicates whether users in the group can bypass firewall rules enforcing Web content filtering.
Web Filter Profile	Name of the Web filter profile associated with the privilege group.
Priority	Web filter profile priority. If a user is a member of multiple LDAP groups, and those groups have different privilege groups associated with them, the Web filter profile with the highest priority (the lowest value) is used.
Function(s)	<p>The available functions for privilege groups:</p> <ul style="list-style-type: none"> • Delete a privilege group • Edit a privilege group (or click the linked privilege group name in the Privilege Group list) <p>CAUTION You must delete the privilege group from any firewall rules with which it is associated before you delete the group.</p>

Creating or editing a privilege group

STEP 1 From the navigation pane, select **Authentication > Privilege Groups**.

The Privilege Groups page opens.

STEP 2 Click **Create Privilege Group** to add a privilege group, or click a **Privilege Group** name to edit it.

The Create or Edit Privilege Group page opens.

STEP 3 Type or edit the **Privilege Group Name**.

The name can be up to 32 alphanumeric characters, using only **a** to **z**, **A** to **Z**, **0** to **9**, - (hyphen) and _ (underscore).

STEP 4 Check or uncheck each of the following:

- **VPN Client Access** — allow/deny VPN client dialup, inter-site VPN access, and Internet access
- **Firewall Rule Authentication** — allow or deny user authentication for firewall rules
- **Web Filtering Bypass** — allow/deny user to bypass Web content filtering

- STEP 5** Select a **Web Filter Profile** from the drop-down list and select its **Web Filter Profile Priority** from 1 to 10 (the default is 1, the highest priority). If a user is a member of multiple LDAP groups, and those groups have different privilege groups associated with them, the Web filter profile with the highest priority is used.
- STEP 6** Click **Create** or **Save** to save the changes and return to the Privilege Groups page, or click **Cancel** to return to the Privilege Groups page without saving the changes.

Adding local users to a privilege group

Once you define a privilege group, you can assign local users to it.

- STEP 1** From the navigation pane, select **Authentication > User List**.
The User list page opens.
- STEP 2** Add a new local user or edit the account of an existing local user.
For details, see [“Creating a new user account in the TOS authentication database” on page 276](#).
- STEP 3** Select a privilege group for the user.
- STEP 4** Repeat steps 2 and 3 for any other users who you want to add to the privilege group.

RADIUS Page

The X family device supports user authentication via **Remote Authentication Dial-In User Service (RADIUS)**. RADIUS authentication may be used in place of the embedded user database within TOS, and may be used for all authenticated access for local users.

The following activities can be authenticated using RADIUS:

- VPN client dialup
- Inter-site VPN access
- Internet access
- Web filtering bypass

To support privilege groups for RADIUS users, configure the user profiles with the standard RADIUS attribute called filter-ID. The filter-ID attribute must be in the form `profile=privilege-group`. For example, if you have a privilege group called teachers, then the filter-ID would be `profile=teachers`.

To support privilege groups for RADIUS users, the VSA attribute must match the privilege group name. After users are authenticated with the RADIUS server, they are assigned the privileges associated with the privilege group.

Consider the following points when configuring the RADIUS server:

- If you have privilege groups configured on the RADIUS server and want to use these groups with the device firewall policies, the RADIUS privilege groups will need to have the same name and access rights as the privilege groups that are configured locally on the device.
- If RADIUS is being used for PPTP authentication, then the RADIUS server must support MSCHAP authentication. Ensure that the RADIUS server is configured to return the MS-CHAP-MPPE-Keys attribute.
- If the RADIUS server is used to assign IP addresses, configure the server to use the `Framed-IP-Address` attribute.
- The user names and passwords stored in the local device database may not be the same as those stored on the RADIUS server. When a user account is created on a RADIUS server, an equivalent account is not automatically created in the local device database, and vice versa.

You can view and manage the RADIUS configuration parameters from the RADIUS page (**Authentication > Radius**). The following figure shows the RADIUS page:

Figure 9–4: RADIUS Page

Configuring RADIUS

STEP 1 From the navigation pane, select **Authentication > RADIUS**.

The RADIUS page opens.

STEP 2 To use remote user authentication, check **Enable RADIUS authentication**.

STEP 3 To specify the activities managed by RADIUS authentication, check **User Authentication** and/or **VPN Client Access**.

You can use RADIUS for VPN clients only or for both user authentication and VPN client access.

STEP 4 In the **RADIUS Server Setup** table:

STEP A Type the **Server Timeout** value (between 1 and 30).

If no response is received from the RADIUS server, this value defines the time in seconds before the device attempts to reconnect.

STEP B Type the **Server Retries** value (between 1 and 10).

This defines the number of times the device will attempt to connect to the RADIUS server.

STEP 5 For the **Primary** and **Secondary RADIUS Servers**, type:

- **IP Address** — The IP address or DNS name of the RADIUS server.
- **Port** — The UDP port number on the RADIUS server where you want device to send authentication requests. The default port number is 1812.



Note: Some older RADIUS servers use port 1645 for authentication.

- **Shared Secret** — The password (between 8 and 128 characters) that you want the device and the RADIUS server to use for communicating with each other.
- **Authentication Method** — The protocol for authentication: **PAP** (Password Authentication Protocol) or **CHAP** (Challenge Handshake Authentication Protocol).

STEP 6 If the RADIUS server has not been configured with a privilege group attribute (Vendor Specific Attribute or VSA), select the **Default Privilege Group** to be assigned from the drop-down list.

STEP 7 When you finish, click **Apply**.

LDAP Configuration Page

The X family device supports user authentication via **Lightweight Directory Access Protocol (LDAP)**. LDAP supports Internet access by profiles. LDAP can be used to authenticate a user and ascertain the user's privilege group. The privilege group defines the Web filter profile to use, regardless of the user's ingress zone.

To support privilege groups for LDAP users, the group name attribute must match the privilege group name. After users are authenticated by the LDAP server, they are assigned the privileges associated with the privilege group.

Consider the following points when configuring the LDAP server:

- To create a secure channel to the LDAP server, the server must have a server certificate, and you must install a certificate authority (CA) certificate for the issuing CA on the device. See [Appendix A. “Browser Certificates”](#) for more information about certificates.
- If you have group names configured on the LDAP server and want to use these groups with the device firewall policies, the LDAP group names need to have the same name and access rights as the privilege groups that are configured locally on the device.
- The user names and passwords stored in the local device database may not be the same as those stored on the LDAP server. When a user account is created on a LDAP server, an equivalent account is not automatically created in the local device database, and vice versa.

You can view and manage the LDAP configuration parameters from the LDAP Configuration page (**Authentication > LDAP**). The following figure shows the LDAP Configuration page:

Figure 9–5: LDAP Configuration Page

The screenshot shows the LDAP Configuration page with the following sections and fields:

- LDAP Authentication:**
 - Enable LDAP
 - Use LDAP to Authenticate Users
- LDAP Server Setup:**
 - Use Encryption (TLS) **TLS is strongly recommended**
 - Start TLS on LDAP port
 - Require valid certificate from LDAP Server
 - Use Local Certificate
- Local Certificate for Encryption (TLS):** None
- Server Name/IP:** [Text Field]
- Port:** 389
- Protocol:** Version 3
- Server Timeout:** 3 seconds
- Server Retries:** 5
- Anonymous Login
- LDAP Server Username:** [Text Field] This is the first component of the user accounts distinguished name (DN).
- LDAP Server Password:** [Text Field]
- LDAP Server Login Tree (DN):** [Text Field] Specify the DN to the LDAP Server Username (e.g. CN=Users, DC=3com, DC=com).
- User Tree for LDAP login (DN):** exam Specify the DN of the tree where all users log in (e.g. DC=3com, DC=com).
- LDAP Search Trees:**
 - Trees Containing Users:**
 - [Text Field] Distinguished Name
 - [Add >]
 - 25 Records per page
 - Table with columns: DN, Function(s)
 - Trees only Containing Groups:**
 - [Text Field] Distinguished Name
 - [Add >]
 - 25 Records per page
 - Table with columns: DN, Function(s)
- Local Certificate:**
 - File to Import: [Text Field] [Browse...]
 - [Import]
- [Apply] [Cancel]

Configuring LDAP

- STEP 1** From the navigation pane, select **Authentication > LDAP**.
- The LDAP Configuration page opens.
- STEP 2** Check **Enable LDAP**.
- STEP 3** Check **Use LDAP to Authenticate Users**. If you check **Enable LDAP** but not **Use LDAP to Authenticate Users**, you can still configure and test LDAP, but not use it for authentication.
- STEP 4** In the **LDAP Server Setup** section:
- STEP A** Check **Use Encryption (TLS)**. 3Com recommends always using Transport Layer Security encryption.
 - STEP B** Check **Start TLS on LDAP port**.
 - STEP C** Check **Require valid certificate from LDAP Server**. 3Com recommends requiring a certificate.
 - STEP D** Type the DNS **Server Name** or the **IP** address of the LDAP server.
 - STEP E** Type the server **Port**. This is normally 389 for unencrypted server access, or 636 (the default) for TLS connections.
 - STEP F** Select the LDAP **Protocol** from the drop-down list: **Version 3** (the default) or **Version 2**.
 - STEP G** Type the **Server Timeout** period (default 3 seconds).
 - STEP H** Type the number of **Server Retries** (default 5).
 - STEP I** Depending on whether or not the LDAP server allows anonymous browsing, do one of the following:
 - Check **Anonymous Login**. This enables an initial bind with no username or password for sites that allow browsing of the LDAP server tree, or some parts of the tree, without user credentials.
 - Type the **LDAP Server Username** (this is the first component of the user accounts distinguished name) and **LDAP Server Password** (the password used to access the LDAP service).
 - STEP J** Type the **LDAP Server Login Tree (DN)**. This is the Distinguished Name of the LDAP server username.
 - STEP K** Type the **User Tree for LDAP login (DN)**. This is the Distinguished Name of the tree where all users log in.
- STEP 5** In the **LDAP Search Trees** section:
- STEP A** Type the distinguished name of one of the **Trees Containing Users**. User trees are applicable only to direct search schemas (with membership attributes). Click **Add** to add the name to the list of DN's; click the **Delete** icon to remove a tree from the list.
 - STEP B** Type the distinguished name of one of the **Trees only Containing Groups**. Group trees are applicable only to indirect search schemas (without membership attributes). Click **Add** to add the name to the list of DN's; click the **Delete** icon to remove a tree from the list.

STEP 6 Some LDAP server configurations requires a client certificate for connections to ensure the identity of the device. (This setting is not required for Microsoft Active Directory.) In the **Local Certificate** section, do the following to designate a certificate:

STEP A Type the file pathname of the certificate file, or click **Browse** and select the file.

STEP B Click **Import**. The certificate name appears in the **Local Certificate for Encryption (TLS)** field.

STEP 7 When you finish, click **Apply**.

Setting LDAP Schema

Use the LDAP Schemas page to specify the schema used by the LDAP server.

STEP 1 From the navigation pane, select **Authentication > LDAP**.

The LDAP Configuration page opens.

STEP 2 Click the **LDAP Schemas** tab.

The **LDAP Schema Configuration** page opens.

STEP 3 Select the schema from the **Current LDAP Schema** list:

- **Microsoft Active Directory**
- **Novell eDirectory**
- **FedoraDS**
- **RFC2798**
- **RFC2307 NIS**
- **Samba SMB**
- **Custom** (to support a directory server not listed)

The user object and group object fields are populated with attribute names as appropriate.

STEP 4 If necessary, change the attribute names.

STEP 5 When you finish, click **Apply**.

Testing LDAP Lookup

Use the LDAP Test page to verify that the device can retrieve user data from the LDAP server. Before testing, ensure that the device is connected to the LDAP server and that the server is running.

STEP 1 From the navigation pane, select **Authentication > LDAP**.

The LDAP Configuration page opens.

STEP 2 Click the **LDAP Test** tab.

The LDAP Test page opens.

STEP 3 Enter a **User** and **Password** and click **Apply**.

If the LDAP server returns data, it is displayed; otherwise, the message “Test failed” appears.

X.509 Certificates

On the X family device, X.509 certificates are used for the following:

- Site-to-site VPN authentication
- Client-to-site VPN authentication

You can manage the following items required to perform authentication with X.509 certificates:

- **CA certificate** — Public certificate issued by a certificate authority. CA certificates are used to validate received local certificates that were signed by this CA for other devices. The X family device supports the PKCS#7 or DER format for importing CA certificates. An organization can install its own CA server or use a third-party organization for creating certificates. The same CA certificate is imported onto all devices that must authenticate with each other.
- **Certificate requests** — Provides a form and encoding method for the administrator to generate a signed local certificate from the CA server. The administrator has to export the certificate request, and then provide it to the CA server. The CA server signs the request to generate a local certificate and returns the signed certificate to the administrator who then imports it back into the device. Successfully importing the local certificate removes the corresponding certificate request, as the request has now been satisfied.
- **Distinguished Name** — Uniquely identifies a certificate. The Distinguished Name is defined when creating the certificate request is used by the local certificate. The device uses **PKCS#10 format** for certificate requests.
- **Local Certificates** — Digitally signed certificates that are used to authenticate IPsec on the device. Local certificates are signed by a CA using a certificate request. The local certificate is a personal certificate, installed on the device or remote device. Each device has a unique local certificate. Other devices that have imported the CA certificate that was used to sign a local certificate can authenticate this device.
- **Certificate Revocation List (CRL)** — List of certificates that have been revoked before their expiration dates by a certificate authority, along with the reasons for revocation and a proposed date for the next release. The certificate authority would revoke a certificate, for example, if there were a suspected compromise of the private part of a public/private key pair that invalidates the public part, or if there were a change in user details.

Configuring X.509 Certificates

To use X.509 certificates as a secure method of authentication for VPN access to the network, you must configure both local and CA certificates before you configure other VPN services. The sequence of tasks is as follows:

1. Import the CA certificate used to validate local certificates. For details, see [“CA Certificate Page” on page 287](#).
2. Create a certificate request and export it as a file that can be sent to the CA server. For details, see [“Certificate Requests Page” on page 291](#).

The CA server converts the request into a signed local certificate.

The local certificate is a personal certificate, installed on the X family device or remote device. Each device has a unique local certificate. The local certificate refers to the CA certificate for validation.



Note If you already have a local certificate with its own private key, you can import this certificate to the device from the Local Certificates page. It is not necessary to complete the certificate request process.

3. Import the signed local certificate retrieved from the CA server. For details, see [“Importing a signed local certificate” on page 294](#).
4. To maintain the integrity of the CA certificates on the X family device, you can also associate a CRL with each certificate and configure parameters to automatically update the CRL. For details, see [“Certificate Revocation List \(CRL\) for a CA Certificate” on page 289](#).

For more detailed information on X.509 certificates, see the *Concepts Guide*.

CA Certificate Page

CA certificates are digital certificates issued and signed by either a local certificate authority server or a certificate authority organization such as Verisign. You can create CA certificates and sign them yourself using tools such as OpenSSL.

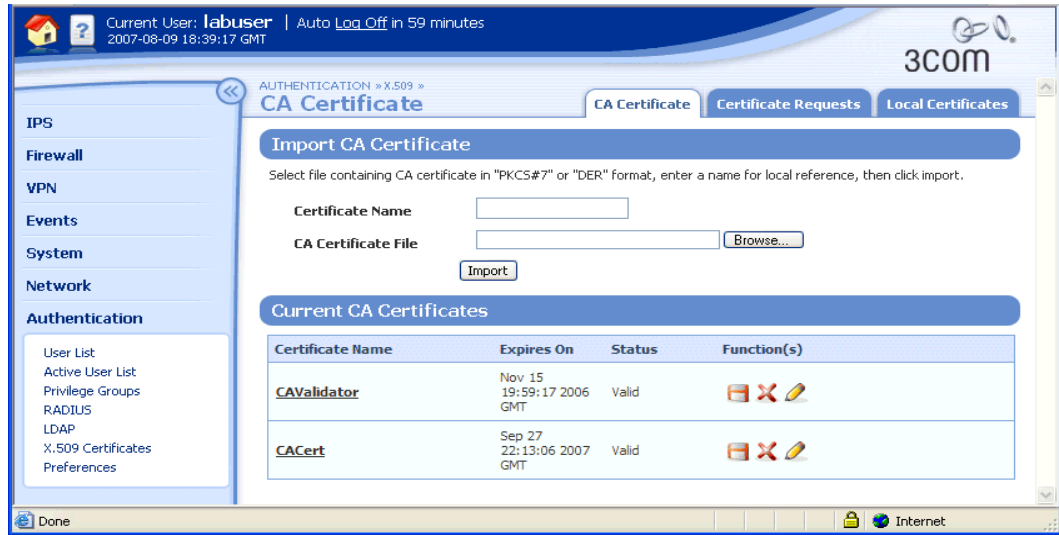
CA certificates are installed on the CA server for your organization and are used to verify local certificates by signing them. The X family device supports the PKCS#7 or DER format for CA certificates.

You can manage CA certificates for the device from the LSM. From the CA Certificates page, you can complete the following tasks:

- Importing the CA certificates used by your organization
- Viewing current CA certificates
- Maintaining a certificate revocation list to ensure that the CA certificates on the device are valid

The following figure shows the CA Certificate page:




Figure 9–6: CA Certificate Page



Current CA Certificates Parameter Details

The **Current CA Certificates** table provides the following information about existing CA certificates:

Table 9–6: Current CA Certificates Information

Column	Description
Certificate Name	Local name the device uses to reference the certificate, specified during the import process.
Expires On	Expiration date of the CA certificate.
Status	The status of the certificate: <ul style="list-style-type: none"> • Valid if the certificate can be used • Revoked if the certificate has been revoked by a certificate revocation list (CRL)
Function(s)	For each CA certificate listed in the table, you can: <ul style="list-style-type: none"> • Delete the certificate  • Export the certificate to a file  • Edit the CA certificate to view the certificate details, specify a CRL, and configure parameters to automatically update the CRL 
CRL Expiry	The expiration date of the certificate revocation list associated with the CA Certificate. This is set to No CRL loaded if the user has not configured a CRL for the CA.

Importing a CA certificate

STEP 1 From the navigation pane, select **Authentication > X.509 Certificates**.

The CA Certificate page opens.

STEP 2 In the **Import CA Certificate** section, type a unique **Certificate Name**. Use only the characters a–z, A–Z, and 0–9 (do not use spaces, symbols, or special characters).

This is the local name that the device uses to identify the CA certificate in the LSM.

STEP 3 Type the path and file for the CA certificate file, or click **Browse** and navigate to the file.

The CA certificate file must use the .DER format (PKCS#7).

STEP 4 Click **Import** to upload the CA certificate to the device.

After you import the CA certificate, you can view and manage it from the **Current CA Certificates** section. To configure a CRL for a certificate, click **Edit**.

Certificate Revocation List (CRL) for a CA Certificate

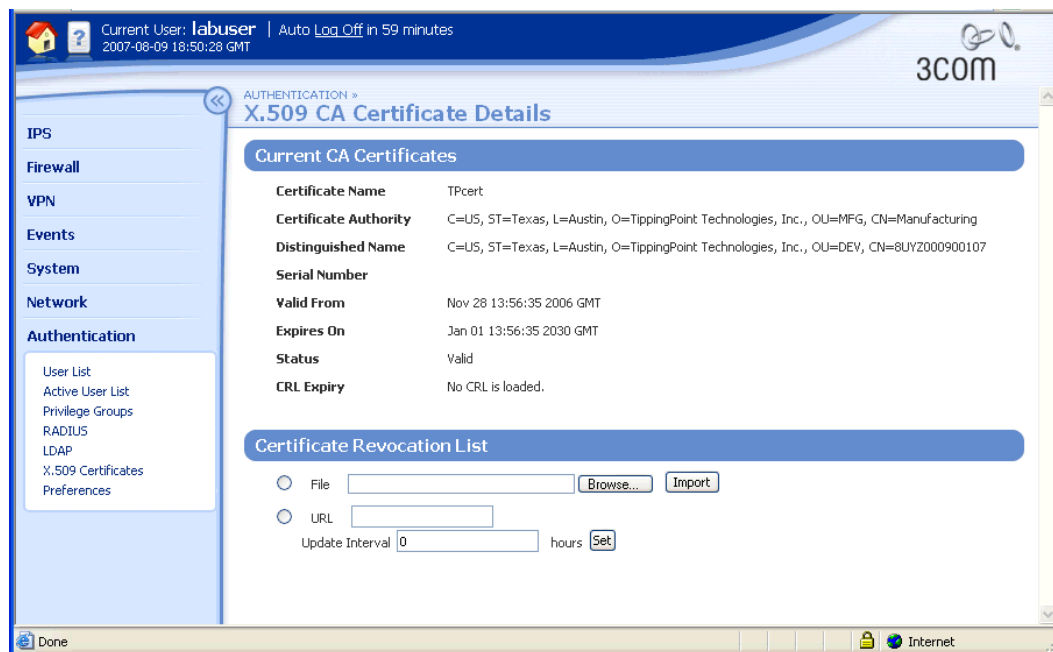
The **certificate revocation list (CRL)** is a list of CA certificates that have been revoked by a certificate authority before their expiration dates. The list includes the reasons for revocation and a proposed date for the next release. Certificates may be revoked because the private part of the public/private key pair has been compromised, invalidating the public key, or if the user details for the certificate have changed.

CRLs are continuously updated by the issuing certificate authority. To maintain the integrity of the CA certificates, use the X.509 CA Certificate Details page to import and maintain the CRL used to validate the CA certificate. From this page you can complete the following tasks:

- Viewing the certificate details
- Importing a CRL for the CA certificate
- Configuring automatic update of the CRL

The following figure shows the X.509 CA Certificate Details page:

Figure 9–7: X.509 CA Certificate Details Page



X.509 CA Certificates Parameter Details

The X.509 CA Certificate Details page provides the following information:

Table 9–7: CA Certificate Details

Detail	Description
Certificate Name	Name of the CA certificate.
Certificate Authority	The Distinguished Name of the certificate authority for this CA certificate.
Distinguished Name	The Subject Distinguished Name entered when creating the request for this certificate on the Create Certificate Requests page.
Serial Number	Serial number of this CA certificate, shown in upper-case hexadecimal format.
Valid From	The start date of this CA certificate, shown in the format <i>mmm dd hh:mm:ss yyyy timezone</i> .
Expires On	The end date of this CA certificate, shown in the format <i>mmm dd hh:mm:ss yyyy timezone</i> .
Status	Status of the certificate, either Valid or Not Valid with a reason.
CRL Expiry	Either the expiration date of the CRL associated with this CA certificate, shown in the format <i>mmm dd hh:mm:ss yyyy timezone</i> , or No CRL is loaded if the user has not configured a CRL for the CA certificate.

Configuring CRL parameters for a CA certificate

STEP 1 From the navigation pane, select **Authentication > X.509 Certificates**.

The CA Certificate page opens.

STEP 2 In the **Current CA Certificates** section, locate the CA certificate that you want configure.

Then, in the **Function(s)** field, click the **Edit** icon.

The X.509 CA Certificate Details page opens.

STEP 3 In the **Certificate Revocation List**, select **File**. Then, type the path and name for the CRL, or click **Browse** and navigate to the file.

STEP 4 Click **Import**.

STEP 5 To configure the CRL for automatic update, select the **URL** radio button. Then:

STEP A Type the **URL** used to retrieve the CRL from the Certificate Authority.

STEP B Type the **Update Interval** in hours. This specifies how often the device queries the CA Website to check for updates.

STEP C When you finish, click **Set**.

Certificate Requests Page

Certificate requests provide administrators with a form and encoding method to generate a signed local certificate from a CA server.

After generating the certificate request, the administrator has to export the request, and then provide it to the CA server. The CA server signs the request to generate a local certificate and returns the signed certificate to the administrator, who then imports it back into the device. Successfully importing the local certificate removes the corresponding certificate request, as the request has now been satisfied. After importing a local certificate, you can view and manage it from the Local Certificates page.

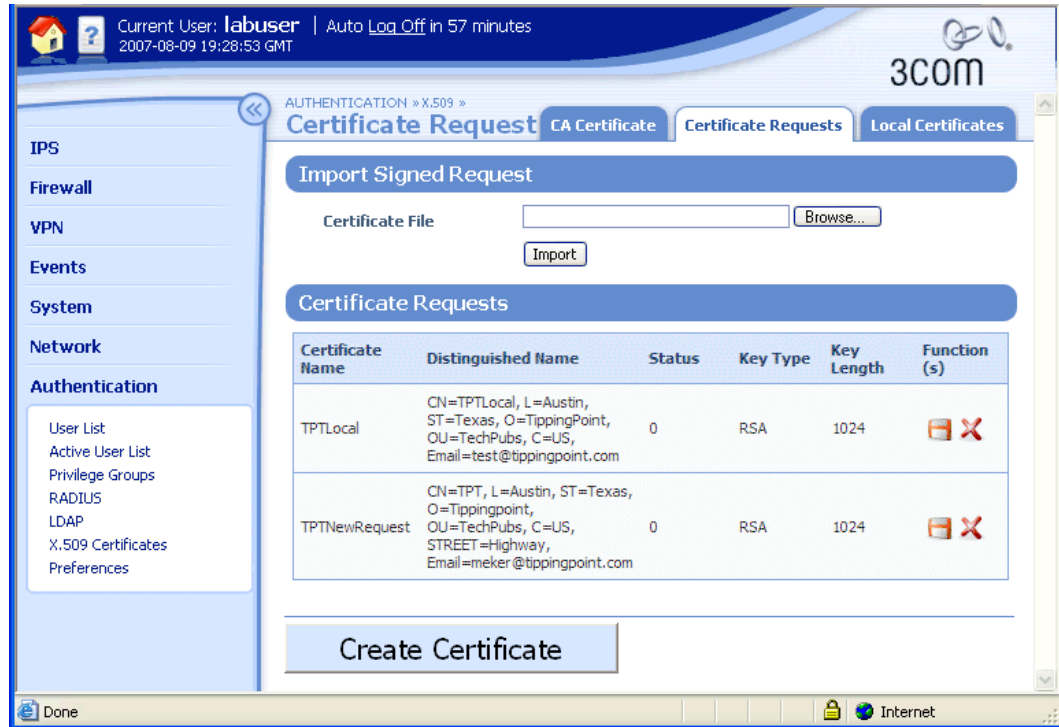
The device uses **PKCS#10 format** for certificate requests. When a request is created, a Distinguished Name (DN) and a public/private key pair is generated, and the public key is included in the PKCS#10 format.

You can manage certificate requests from the Certificates Request Page. From the Certificates Request page, you can complete the following tasks:

- Viewing certificate requests currently available.
- Creating a certificate request.
- Exporting the request so it can be submitted to the certificate authority.
- Importing a signed certificate request that has been returned by the certificate authority so it is available for use.

The following figure shows the Certificate Request page:

Figure 9–8: Certificate Request Page



For additional information, see the following topics:

- [“Certificate Requests Parameter Details” on page 293](#)
- [“Managing Certificate Requests” on page 293](#)
- [“Importing a signed local certificate” on page 294](#)

Certificate Requests Parameter Details

The Certificate Requests page provides the following information:



Table 9–8: Certificate Requests Details

Column	Description
Certificate Name	The name you gave to the local certificate when importing it.
Distinguished Name	The Distinguished Name of this local certificate. This is defined when you create the certificate Request. The Distinguished Name comprises a number of attributes including: CommonName, Locale, State or Province, Organization, Department, Country, and Street Address.
Status	The current status of the certificate request: <ul style="list-style-type: none"> • Not Valid if the certificate is valid in the future, or if authenticity cannot be verified using a CA certificate currently installed. • Valid if the certificate can be used. • Revoked if the certificate has been revoked by a CRL.
Key Type	Currently supports RSA as the type.
Key Length	Number of bits in the key: 1024 , 2048 , or 4096 .

Managing Certificate Requests

The following table shows the management functions you can perform from the Certificate Request page:

Table 9–9: Certificate Request Functions

Function	Icon/Field	Description
Import Signed Local Certificate	Import Signed Request section	When you receive a signed certificate from the certificate authority, you can import the certificate so that it is available on the device. When you import a signed certificate from the Certificate Requests page, the certificate request generated to obtain the signed certificate is automatically deleted.
Create a Certificate Request	Create Certificate button	Access the Create a Certificate Request page to specify the parameters and Distinguished Name attributes for the request, and generate the certificate request in PKCS#10 format.
Export		A certificate request must be exported to a file before it can be submitted to the CA (either by a Web-based service or by email). Certificate requests are exported in PKCS#10 format, which includes the Distinguished Name (DN) and the public key. A request is signed by the private key of the requester so that the CA can verify authenticity.
Delete		If a certificate request is no longer needed, use the Delete function to remove it from the device. The device automatically deletes certificate requests when you import the signed local certificate received from the certificate authority.

Creating a certificate request

- STEP 1** From the navigation pane, select **Authentication > X.509 Certificates**.
The CA Certificate page opens.
- STEP 2** Click the **Certificate Requests** tab.
The Certificate Request page opens.
- STEP 3** Click **Create Certificate**.
The Create Certificate Request page opens.
- STEP 4** Type a name for the Certificate Request in the **Certificate Name** field.
This is the name used by the local certificate when you later import the signed local certificate.
- STEP 5** Select the length in bits for the private key from the **Length** drop-down list, either **1024**, **1536**, or **2048**.
- STEP 6** In the **Distinguished Name** section, define the Distinguished Name attributes for the Certificate Request:
- STEP A** In the **DN Attribute** field, select an attribute from the drop-down list.
 - STEP B** Type the value in the data field.
 - STEP C** Click **Add to table below**.
The attribute and value are added to the Distinguished Name table. You can delete an attribute if required.
 - STEP D** Repeat this process until you have defined the necessary information for the certificate.
- STEP 7** Click **Create** to generate the certificate request in PKCS#10 format.
The Certificate Requests page opens, with the generated request listed in the **Certificate Request** table.
- STEP 8** Click **Export** to save the file so you can submit the request to a Certificate Authority to obtain a signed local certificate.

Importing a signed local certificate

Use this procedure to import the signed certificate that you received from the certificate authority in response to submitting a certificate request.

- STEP 1** From the navigation pane, select **Authentication > X.509 Certificates**.
The CA Certificate page opens.
- STEP 2** Click the **Certificate Requests** tab.
The Certificate Request page opens.
- STEP 3** In the **Import Signed Request** section, type the **Certificate File** path and filename for the certificate request to import, or click **Browse** and navigate to the file.

This is the name of the signed local certificate file returned from the CA to which you transferred the certificate request file.

STEP 4 Click **Import**.

If the device verifies that the certificate can be trusted and that it matches a current certificate request, the certificate is imported. The matching certificate request is deleted. After the local certificate is imported, you can view and manage it from the Local Certificates page.

If the import fails, its status is **Not Valid**, and a message explaining the failure is displayed.

Local Certificates Page

Local certificates are used by the X family device to authenticate IPsec on the device. Local certificates are signed using the private key of a CA certificate.

The local certificate is a personal certificate, installed on the X family device or a remote device. Each device has a unique local certificate. Because the local certificate has been signed by a CA, any other device that has imported and trusts the CA certificate can authenticate the X family device.

The device uses PKCS#12 format for importing local certificates with their private key. PKCS#12 format is a commonly used portable format for importing certificates into browsers. The imported file may also include the CA certificate, in which case the device adds the CA certificate to the CA list.

A local certificate can be installed using one of the following methods:

- Install the local certificate directly from the Local Certificate page with a private key. With this method, you must know the private key and have a CA certificate from the same CA that signed the local certificate installed on the device.
- Perform the certificate request procedure from the Certificate Requests page.

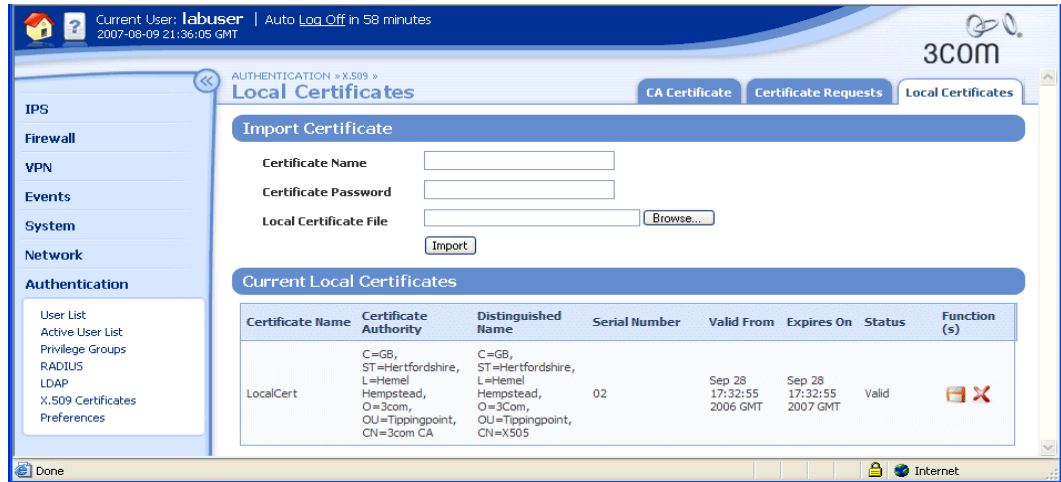
3Com recommends using the certificate request procedure because it is a more secure process. For details on the certificate request procedure, see [“Certificate Request Page” on page 292](#).

You can manage local certificates from the Local Certificates Request page (**Authentication** > **X.509 Certificates**, **Local Certificates** tab). From this page, you can complete the following tasks:

- Viewing local certificates currently available
- Importing a local certificate directly with a private key
- Exporting local certificates
- Deleting local certificates

The following figure shows the Local Certificates page:

Figure 9–9: Local Certificates Page





Local Certificate Parameter Details

The **Current Local Certificates** table provides the following information about existing certificates:

Table 9–10: Current Local Certificates Details

Column	Description
Certificate Name	The name of the certificate.
Certificate Authority	The Distinguished Name of the CA for this local certificate.
Distinguished Name	The Distinguished Name of this local certificate. See “Certificate Requests Page” on page 291 for information about Distinguished Names. These include CommonName, Locale, State or Province, Organization, Department, Country, and Street Address.
Serial Number	Serial number of this local certificate, in uppercase hexadecimal format.
Valid From	The start date of this local certificate, shown in the format <i>mmm dd hh:mm:ss yyyy timezone</i> .
Expires On	The end date of this local certificate, shown in the format <i>mmm dd hh:mm:ss yyyy timezone</i> .
Status	The current status of this local certificate: <ul style="list-style-type: none"> • Valid • Revoked by CA CRL • Not Valid — certificate valid in the future • Not Valid — certificate has expired • Not Valid — unable to verify certificate with current CAs

Table 9–10: Current Local Certificates Details (Continued)

Column	Description
Function(s)  	For each local certificate listed in the table, you can: <ul style="list-style-type: none"> • Delete the certificate. • Export the certificate to a file. You must provide the password for the certificate before you can export it.

Importing a local certificate

STEP 1 From the navigation pane, select **Authentication > X.509 Certificates**.

The CA Certificate page opens.

STEP 2 Click the **Local Certificates** tab.

The Local Certificates page opens.

STEP 3 In the **Import Certificate** section, type a unique **Certificate Name**. Use only the characters a–z, A–Z, and 0–9 (no spaces, symbols, or special characters).

This is the local name that the device uses to identify the local certificate.

STEP 4 Type the **Certificate Password** for the local certificate. This password is issued by the local certificate provider.

STEP 5 Type the **Local Certificate File** path and filename for the signed local certificate, or click **Browse** and navigate to the file.

The CA certificate file must use the PKCS#12 format. You can only import a local certificate that has been signed by a CA certificate available on the device. For details on importing CA certificates, see [“CA Certificate Page” on page 287](#).

STEP 6 Click **Import** to upload the local certificate onto the device.

If the import fails, an error message displays.

After you import the local certificate, view and manage it from the Current Local Certificates page.

Exporting a local certificate

STEP 1 From the navigation pane, select **Authentication > X.509 Certificates**.

The CA Certificate page opens.

STEP 2 Click the **Local Certificates** tab.

The Local Certificates page opens.

STEP 3 Click the Export icon for the certificate you want to export.

You must provide a valid password to export the local certificate.

STEP 4 At the prompt, type the certificate password in the **Please enter the certificate password** field. Then, click **OK**.

STEP 5 On the **File Download** dialog, click **Save**. Then, specify the path and filename to save the file.

Preferences Page

From the Preferences page (**Authentication > Preferences**), users with Administrative or Super-User access can configure preferences to manage the security settings that affect TOS and local user account access, session management, and device session management.



TIP Session timeouts and password expiration periods may be covered in your company's information security policy. Consult your security policy to be sure you configure these values appropriately.

The following figure shows the Preferences page:

Figure 9–10: Preferences Page

Current User: labuser | Auto Log Off in 59 minutes
2007-10-30 20:09:51 GMT

3COM

Authentication > Preferences

General User Preferences

Web Idle Timeout: 60 minute(s)

Page Refresh Time: 30 second(s)

TOS User Preferences

Security Level: No Security Checking

Password Expiration: 90 days

Password Expiration Action: Force User to Change Password

Max Login Attempts: 5

Failed Login Action: Lockout Account or IP address

Lockout Period: 5 minute(s)

Local User Preferences

Inactivity Timeout: 10 minute(s)

Maximum Session Time: 0 minute(s) Specify 0 (zero) for no limit

User Login Status Window:

Heartbeat Enable:

Heartbeat Interval: 30 Seconds

Maximum Heartbeat Loss: 2

Apply

Preferences Parameter Details

The following table provides information on the security preferences parameters:

Table 9–11: Authentication Preferences

Field	Description
General User Preferences	
Web Idle Timeout	Amount of time (in minutes) that can elapse with no user activity before the LSM logs out account access. This setting prevents unauthorized users from accessing the LSM or device services if the user is unexpectedly called away from the workstation or forgets to log out.
Page Refresh Time	Specify the time period for the Auto Refresh option available on pages that have dynamic content (such as the System Summary page, Log pages, and Health pages). If the option is enabled on a page, a countdown timer (starting with the value of Page Refresh Time) is started as soon as the page is opened. When the countdown expires, the page automatically refreshes.
TOS User Preferences	
Security Level	<p>Determines the length and complexity requirements for passwords. The following options are available:</p> <ul style="list-style-type: none"> • No Security Checking (Level 0) — Usernames cannot have any spaces. Passwords are not required. When this security level is selected, users must still enter a valid username to access the device or network services, but no password is required. • Basic Security Checking (Level 2) — User names must be between 6 and 32 characters long; passwords must be between 8 and 32 characters long. • Maximum Security Checking (Level 3) — User names must be between 6 and 32 characters long. <p>Passwords must be strong passwords, having 8 and 32 characters and containing at least one numeric character and one non-alphanumeric character (special characters such as !? and *). This is the default setting.</p>
Password Expiration	<p>Specifies how frequently users are required to change their passwords. You can disable this feature or select a time period (from 10 days up to 1 year) from the drop-down list.</p> <p>TIP Best practices for password security recommend that password expiration periods should be a minimum of 30 days and a maximum 90 days.</p>
Password Expiration Action	<p>Determines what action the device takes in response to a password expiration event. The following options are available:</p> <ul style="list-style-type: none"> • Force user to change the password when it expires. • Notify user of expiration. If this option is selected, the device notifies the user five days before the expiration occurs and at each subsequent login prompts the user to change the password before accessing the LSM. • Disable the account.
Max Login Attempts	Determines how many failed login attempts are allowed before the system takes the action specified in the Failed Login Action field.

Table 9–11: Authentication Preferences (Continued)

Field	Description
Failed Login Action	Determines what action the system takes when the Max Login Attempt count has been exceeded. The following options are available: <ul style="list-style-type: none"> • Disable the account and lock out the IP address. For this option, specify a Lockout Period. • Lock out the account or IP address. • Audit the event in the Audit log, documenting the failed login attempt.
Lockout Period	If the Lockout Account is selected as the Failed Login Action, this value determines the duration of the lockout. A value of 0 means no lockout.
Local User Preferences	
Inactivity Timeout	For local users, the amount of time (in minutes) that can elapse with no user activity before the device logs out account access. This setting prevents unauthorized users from accessing network services if the user is unexpectedly called away from the workstation or forgets to log out.
Maximum Session Time	For local users, this value determines the maximum amount of time that the user can have access to authorized network services during one session. A time of 0 means unlimited time.
User Login Status Window	If checked, a browser window is displayed for users who log in through the LSM, which allows user to log out of the LSM.
Heartbeat Enable	If checked, heartbeat function is enabled for all users. If the device does not receive heartbeats from a user session, the session is logged off.
Heartbeat Interval	An interval in seconds (default 30). An interval of 0 means unlimited time.
Maximum Heartbeat Loss	Number of missed heartbeats permitted before the device logs off a user session (the default is 2).

Setting user preferences

STEP 1 From the navigation pane, select **Authentication > Preferences**.

The Preferences page opens, displaying the current security settings.

If the fields are read-only, your account does not have the required security access to edit the preferences. You must have an account with Administrator or Super-User access.

STEP 2 Change values as desired. When you finish, click **Apply**.

Configuring session timeouts

1. Go to **Authentication > Preferences**.
2. Configure the following administration login timeouts:
 - **Web Idle Timeout.** This option defines the period of inactivity on a session after which an administrator must re-authenticate with the X family device.
 - **Maximum Session Time.** This option determines the maximum amount of time that the administrator can have access to authorized network services during one session. If set to 0, the session is unlimited.
 - **Lockout Period.** This option defines the period that a user is locked out of the Web Interface if they fail login too many times. This is a security feature to prevent hacker access.

Setting Up User Authentication

Complete the following procedures to set up user authentication:

1. Create a privilege group. See [“Creating or editing a privilege group” on page 279](#).
2. Add local users to the privilege group. See [“Adding local users to a privilege group” on page 280](#).
3. Enable authentication. See [“Configuring RADIUS” on page 281](#) or [“Configuring LDAP” on page 283](#).
4. Define a user session timeout. See [“Configuring session timeouts” on page 301](#).

A Browser Certificates

This appendix details creating browser certificates for use in Internet Explorer to ensure that notification messages are no longer reported to the user.

Overview

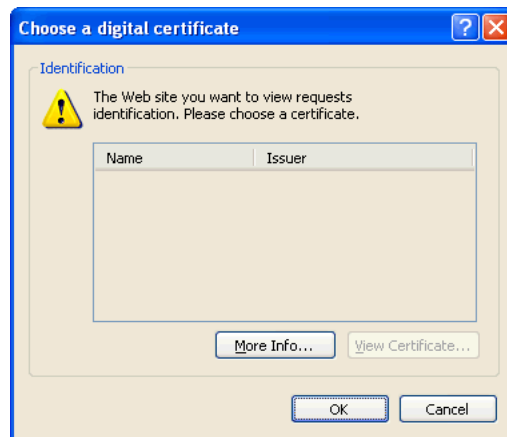
If you do not have a valid client certificate installed on your PC, Internet Explorer may display a Client Authentication message followed by a Security Alert message when you first establish an HTTPS session with the device. The following topics describe how to create certificates to remove these messages:

- [“Client Authentication Message” on page 304](#)
- [“Security Alert” on page 306](#)
- [“Example — Creating a Personal Certificate” on page 313](#)

Client Authentication Message

The X family device uses the same HTTPS channel to communicate with other products as it does to communicate with the LSM. During the SSL handshake, the device asks for a client certificate for validation. This is meant for other products; however, LSM users may also be prompted for a client certificate. You can safely ignore this dialog.

Figure A-1: Client Authentication Dialog Box



To remove this warning, you can create and install a personal certificate on your workstation.

The following procedures detail how to create and install the personal certificate:

- [“Creating a personal certificate” on page 304](#)
- [“Installing the personal certificate” on page 305](#)

Creating a personal certificate

The following command generates a self-signed certificate good for 10 years. The user must have access to a computer with OpenSSL installed on it. For the latest copy of OpenSSL, go to the OpenSSL web site: <http://www.openssl.org>.

STEP 1 Enter the following command:

```
openssl req -new -x509 -days 3650 -out cert.pem -keyout privkey.pem
```

This command creates two files: `cert.pem` and `privkey.pem`.

STEP 2 Enter the following command:

```
openssl pkcs12 -export -in cert.pem -inkey privkey.pem  
-out to_import.p12
```

This command creates the import file `to_import.p12`.

Installing the personal certificate

The following instructions detail how to import the personal certificate. During the procedure, you will import the file called `to_import.p12` created using the previous procedure.

- STEP 1** Open Microsoft Internet Explorer (version 6.0 or later).
- STEP 2** Select **Tools > Internet Options**.
The Internet Options window opens.
- STEP 3** Click on the **Content** tab. Then, click **Certificates**.
The Certificates window opens.
- STEP 4** Click **Import**.
The **Certificate Import Wizard** window opens.
- STEP 5** Click **Next**.
The File to Import window opens.
- STEP 6** Do the following:
 - STEP A** Click **Browse**.
 - STEP B** Locate and select the file `to_import.p12`.
 - STEP C** Click **Next**.
The Password window opens.
- STEP 7** Do the following:
 - STEP A** Enter your private key **Password**.
 - STEP B** Click the **Mark the private key as exportable** check box.
 - STEP C** Click **Next**.
The Certificate Store window opens.
- STEP 8** Select the option **Automatically select the certificate store based on the type of certificate**.
- STEP 9** Click **Next**.
The Completing the Certificate Import Wizard window opens.
- STEP 10** Click **Finish**.
When importation finishes, the message “The import was successful” appears.
- STEP 11** Click **OK**.

Security Alert

The Security Alert dialog in the following illustration shows two security alerts regarding certificates:

- [“Certificate Authority” on page 306](#) — The certificate is not from an trusted certifying authority
- [“Invalid Certificate Name” on page 311](#) — The name of the certificate is invalid

3Com creates a self-signed SSL device certificate for authentication with the browser. This allows X family devices to use SSL communication between the device and client Web browser. This certificate may cause browsers to display a warning dialog, or to otherwise indicate that the certificate is suspect. You can eliminate this warning by installing the certificate into the client certification trust list and placing an entry for the device in your local `HOSTS` or `LMHOSTS` file. The entry in the `HOSTS` file should name the host by its device serial number and then its IP address. This allows the SSL client to resolve the certificate common name.

Certificate Authority

The following dialog warning displays for a certificate authority security alert:

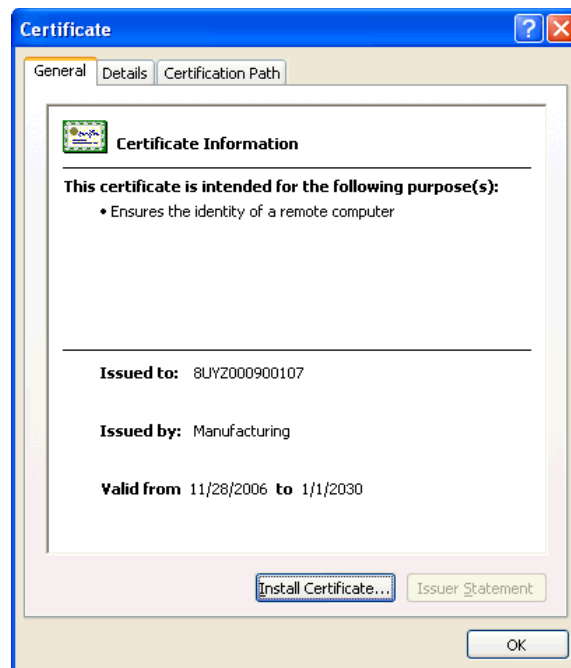
Figure A-2: Certificate Authority Security Alert



You can eliminate the Certificate Authority warning with the following procedure:

STEP 1 When the warning appears, click **View Certificate**. The **Certificate** dialog box opens.

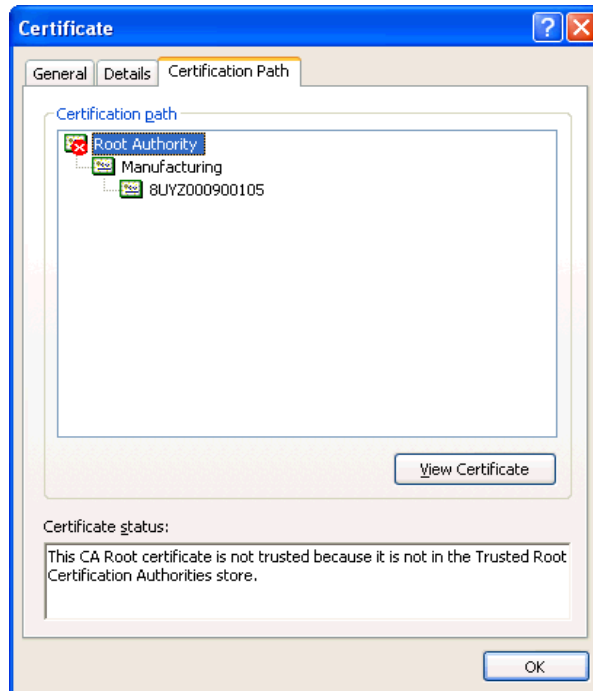
Figure A-3: Certificate Dialog Box



STEP 2 Select the **Certification Path** tab.

STEP 3 Select the **Root Authority**.

Figure A-4: Certification Path Tab — Root Authority



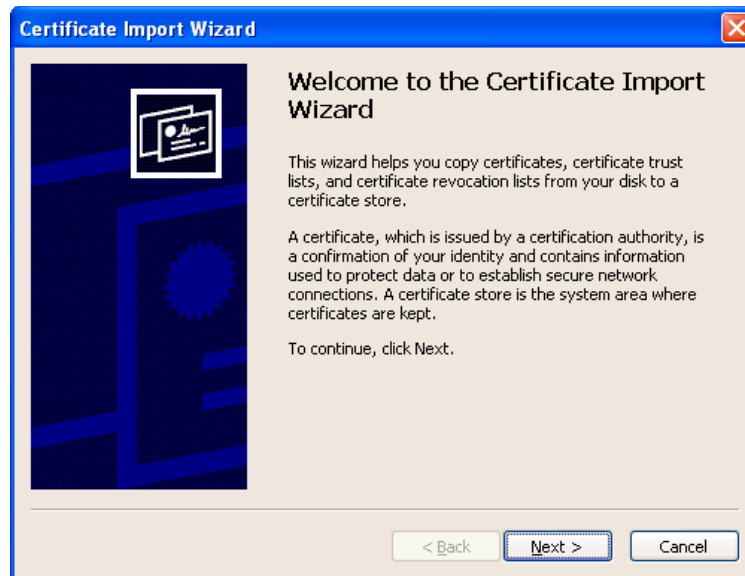
STEP 4 Click **View Certificate**.

Figure A-5: Certification Path Tab — Certificate Information



STEP 5 Click **Install Certificate**. The Certificate Import Wizard opens.

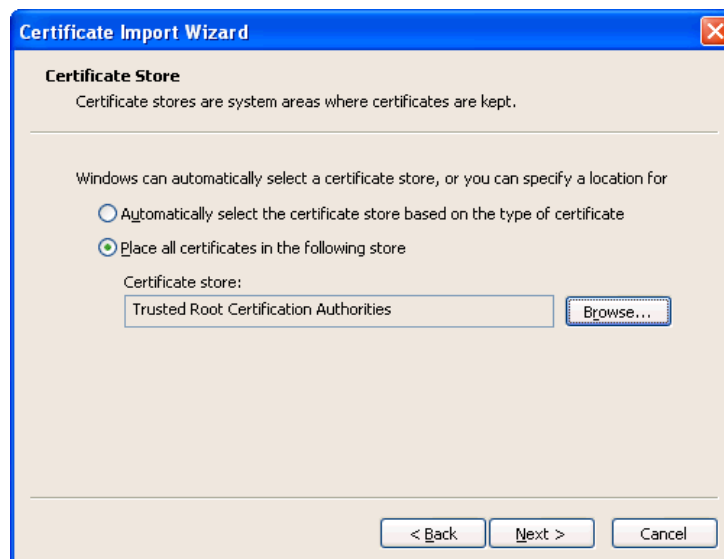
Figure A-6: Certificate Import Wizard



STEP 6 Click **Next**.

The **Certificate Store** dialog opens.

Figure A-7: Certificate Store Dialog



STEP 7 Do the following:

STEP A Select **Place all certificates in the following store**.

STEP B Click **Browse** and select the certificate store “Trusted Root Certificate Authorities.”

STEP C Click **OK**.

STEP 8 Click **Next**.

The Completing the Certificate Import Wizard window opens.

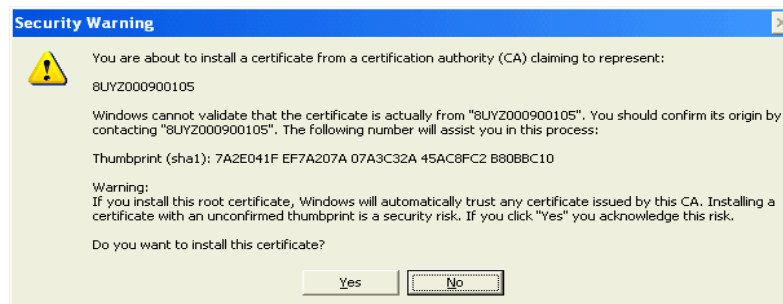
Figure A-8: Completing the Certificate Import Wizard Dialog



STEP 9 Click **Finish** to install the certificate.

The Root Certificate Store indicates the status of the import and displays the certificate information.

Figure A-9: Root Certificate Store Verification



STEP 10 Click **Yes**. The wizard displays the message “The import was successful.”

STEP 11 Click **OK**.

The LSM login page opens.

Invalid Certificate Name

The following warning appears for an invalid certificate name security alert:

Figure A-10: Invalid Certificate Name

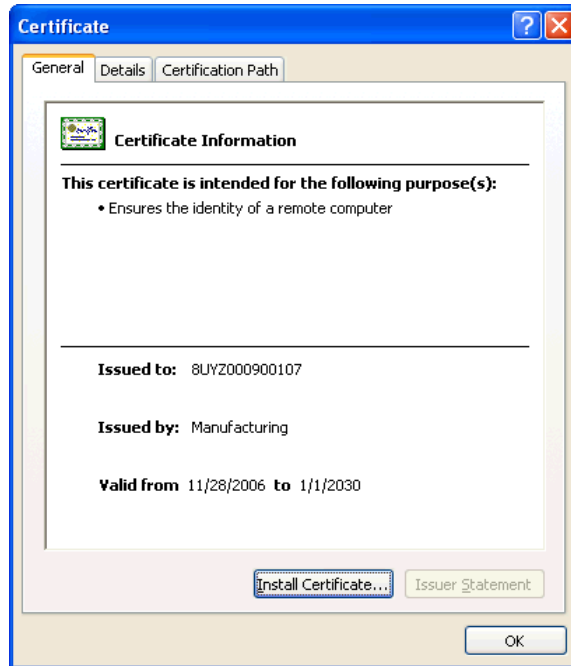


Perform the following steps to eliminate this warning:

STEP 1 When the warning displays, click **View Certificate**.

The **Certificate** window opens.

Figure A–11: Certificate Window

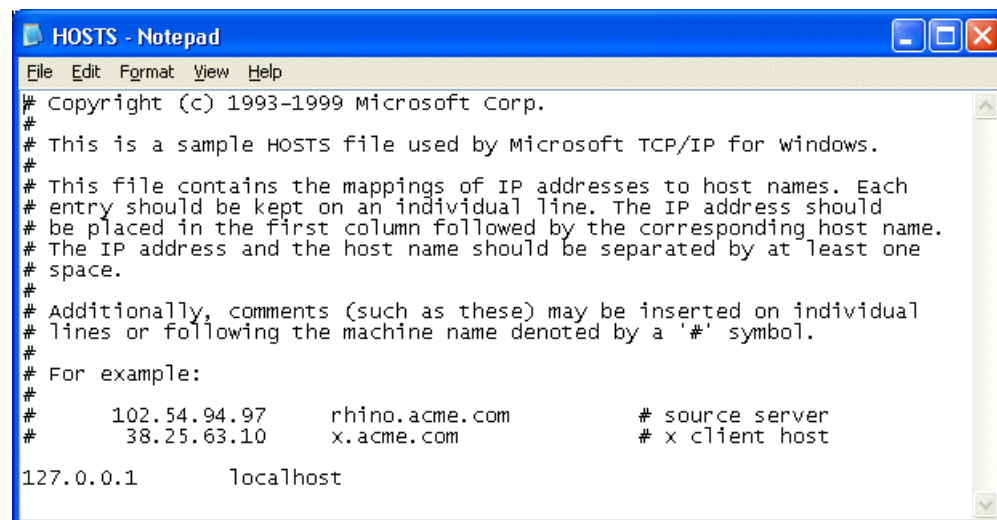


STEP 2 On the General tab, make note of the serial number.

STEP 3 Navigate to and open the local workstation's HOSTS file.

On a Windows XP system, this file is located in C:\WINDOWS\system32\drivers\etc.

Figure A–12: HOSTS File



- STEP 4** Add a line to the file with the device's IP address and serial number.
- STEP 5** When browsing to the device, enter the workstation name instead of the IP address in your Web browser. This name and certificate works only on that particular workstation.

Example — Creating a Personal Certificate

The following is an example of how to create you own personal certificate. User entries are in **bold** type. For security purposes, you should not use the sample passwords provided below.

```
[ ]# openssl req -new -x509 -days 3650 -out cert.pem
-keyout privkey.pem
Using configuration from /usr/share/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'privkey.pem'
Enter PEM pass phrase: DefaultPemPhrase
Verifying password - Enter PEM pass phrase: DefaultPemPhrase
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]: US
State or Province Name (full name) [Berkshire]: Texas
Locality Name (eg, city) [Newbury]: Austin
Organization Name (eg, company) [My Company Ltd]: 3Com
Corporation
Organizational Unit Name (eg, section) [ ]: TAC
Common Name (eg, your name or your server's hostname) [ ]: TPTI
Email Address [ ]: my_email@3com.com
[ ]# openssl pkcs12 -export -in cert.pem -inkey privkey.pem -out
to_import.p12
Enter PEM pass phrase: DefaultPemPhrase
Enter Export Password: exportPassCode
Verifying password - Enter Export Password: exportPassCode
[ ]#
```


B Log Formats and System Messages

Details the formats of the downloadable logs and system update status messages.

Overview

The following topics contain information on the formats of each of the LSM downloaded logs. This includes information on the remote syslog format and High Availability messages contained in the System Log. Also included are descriptions of messages received during the system update process.

The following topics are included:

- [“Log Formats” on page 316](#)
 - [“Alert and IPS Block Log Formats” on page 316](#)
 - [“Audit Log Format” on page 319](#)
 - [“Firewall Block Log Format” on page 320](#)
 - [“Firewall Session Log Format” on page 323](#)
 - [“VPN Log Format” on page 324](#)
 - [“System Log Format” on page 325](#)
- [“Remote Syslog Log Format” on page 326](#)
- [“High Availability Log Messages” on page 327](#)
- [“System Update Status Messages” on page 328](#)

Log Formats

You can view all the logs in the GUI. In addition, you can download a text-only version of the log and view it in a browser window or save it in a file. If you save a log in a file, you can then off load it to a remote syslog server. When downloading a log, the format is a stream of data separated by the delimiter specified in the GUI.

In the System Log, the fields displayed in the GUI are the same as the fields in the downloaded log. In the other logs, the fields that are shown in the GUI are only a subset of what is available in the downloaded log file.

This section documents the fields that are in the downloaded versions of these logs. These field definitions are helpful when reading the downloaded log file. They contain the description of the data so that you can format the desired fields in a reporting program such as Excel or Access, or send it to a remote syslog server.

Delimiters

On the Download Log page, you can specify one of the following delimiter formats:

- **tab** (default) — The field names do not appear in the tab delimited format
- **comma** (CSV)

For both types of delimiters, the sub-fields within the **Message** field are always tab delimited. If a Message sub-field is not used, a tab is inserted to move onto the next sub-field.

Alert and IPS Block Log Formats

An example of a tab-delimited IPS Block Log entry follows:

```
1, 2006-08-22 16:31:39,INFO,BLK,"Block v4 2 [3f937e55-31e9-11db-9452-0800179bd3a4] 1 [00000001-0001-0001-0001-000000000164] icmp 0
192.168.1.1:0 209.191.93.52:0 1 0 0 [cc2f252a-1a57-4d00-8dc8-a34e69992c46] ANY [cc2f252a-1a57-4d00-8dc8-a34e69992c46] ANY
1156260699 0000000000 1          pt0 0 0 0 0324"
```

The following table describes the downloadable format of the Alert Log and IPS Block Log:

Table B-1: Alert and IPS Block Log Formats

Field Name	Sub-Field Name	Description
Seq		Unique sequence number for this log file.
Entry_time		Date and time of event, in the format <i>yyyy-mm-dd 24H:mm:ss</i>

Table B-1: Alert and IPS Block Log Formats (Continued)

Field Name	Sub-Field Name	Description
Sev		Severity of the alert, from least to most severe: <ul style="list-style-type: none"> • INFO = for information only • WARN = warning • ERR = error • CRIT = critical
Comp		Software component that generated the message: <ul style="list-style-type: none"> • ALT = Alert Log • BLK = IPS Block Log
Message (contained within quotes)	Alert Action	<ul style="list-style-type: none"> • Alert = for Alert Log • Block = for IPS Block Log
	Policy Log Version	v4
	Alert Type	A bit field that identifies a message as traffic threshold, invalid, etc.
	Policy UUID	ID for the policy, enclosed within brackets ([]). Default policies begin with “[00000002-...”
	Message Severity	1 = low 2 = minor 3 = major 4 = critical
	Signature UUID	Signature ID from the DV, enclosed within brackets ([]). Can have multiple policies per signature. Default signatures begin with “[00000001-...”
	Protocol	Protocol of the alert. Examples: HTTP, IP, TCP, UDP, and ICMP.
	IP Protocol Numeric	Layer 2 protocol (uint). Only used in Firewall Block Logs. In all other logs, this field is 0.
	IP Protocol String	Layer 2 protocol (string). Only used in Firewall Block Logs. In all other logs, this field is blank.
	Source IP Address and Port	Packet’s source IP address and port. Format is <address>:<port>
Destination IP Address and Port	Packet’s destination IP address and port. Format is <address>:<port>	
Message (continued)	Hit Count	The aggregated number of messages received.
	In MPHY	Physical port number in which the packet arrived.

Table B-1: Alert and IPS Block Log Formats (Continued)

Field Name	Sub-Field Name	Description
	VLAN	(int)
	In Security Zone UUID	(uuid)
	In Security Zone NAME	(string) Example: ANY
	Out Security Zone UUID	(uuid)
	Out Security Zone NAME	(string) Example: ANY
	Date & Time (Seconds)	Beginning timestamp, in seconds, of the aggregation period.
	Date & Time (Nanoseconds)	Beginning timestamp, in microseconds, of the aggregation period.
	Period	Aggregation period, in minutes. 0 = no aggregation.
	Message Parameters	A string of values for special message formats used for traffic thresholds. This value is usually blank.
	Packet Trace Log Flag	Packet trace flag/version: <ul style="list-style-type: none"> • pt0 = off • pt1 = on
	Packet Trace Bucket ID	Packet trace aggregation bucket sequence number.
	Packet Trace Sequence Begin	Packet trace aggregation bucket beginning sequence number.
	Packet Trace Sequence End	Packet trace aggregation bucket ending sequence number.
	Number of characters in the line	Used for reverse parsing of the entry.

Audit Log Format

An example of a comma-delimited Audit Log entry follows:

```
48,2006-08-04 12:46:11,8,CLI,0.0.0.0,LCD,0,0,labuser,"Created policy
rule 100"
```

The following table describes the downloadable format of the Audit Log:

Table B-2: Audit Log Format

Field Name	Description
Seq	Unique sequence number for this log file.
Entry_time	Date and time of event, in the format <i>yyyy-mm-dd 24H:mm:ss</i> .
Access	The access level of the user performing the action.
Type	The interface from which the user logged in: <ul style="list-style-type: none"> • WEB for the LSM • CLI for the Command Line Interface
Address	The IP address from which the user connected to perform the action.
Cat	The area in which the use performed an action (LOGIN, LOGOUT, and Launch Bar tabs).
Result	<ul style="list-style-type: none"> • 0 = Pass • 1 = Fail
Flag	Not used.
User	The login name of the user performing the action. The user listed for an event may include SMS, SYS, HA, and CLI. These entries are automatically generated when one of these application performs an action.
Message (contained within quotes)	The message text associated with the event. The action performed as a result; for example, <i>Log Files Reset</i> .

Firewall Block Log Format

An example of a tab-delimited Firewall Block Log entry follows:

```
6,2006-10-05 17:12:31,INFO,BLK,"Block v4 2 [c52e3da9-23e0-11db-9cdd-00132055ccd2] 1 [00000001-0001-0001-0001-000000007400] firewall 17 UDP
152.67.137.49:137 152.67.140.3:137 1 0 0 [e3d4586b-67a6-4662-bc17-560455bedf54] LAN [08585a5d-23e1-11db-9cdd-00132055ccd2] MGMT
1160086351 0587833079 1 1 0| | | pt0 0 0 0 0344"
```

The following table describes the downloadable format of the Firewall Block Log:

Table B-3: Firewall Block Log Format

Field Name	Sub-Field Name	Description
Seq		Unique sequence number for this log file.
Entry_time		Date and time of event, in the format <i>yyyy-mm-dd 24H:mm:ss</i> .
Sev		Severity of the alert, from least to most severe: <ul style="list-style-type: none"> • INFO = for information only • WARN = warning • ERR = error • CRIT = critical
Comp		Software component that generated the message. Example: BLK.
Message (Contained within quotes.)	Action	
	Version	
	AlertType	
	Policy UUID	The UUID of the matched Firewall rule.
	Severity	Not used.
	Signature UUID	Not used.
	Protocol Type String	String name of the Protocol field (e.g. "tcp").
	Protocol Number	The IP protocol number used for the session by the starter.
	Protocol Name	String name of the Protocol (e.g. "http").

Table B–3: Firewall Block Log Format (Continued)

Field Name	Sub-Field Name	Description
Message (cont.)	Source IP	The source IP address and port for the session. This represents the “starter” of the session. Format is <i>ddd.ddd.ddd.ddd:port</i> .
	Destination IP	The destination IP address and port for the session. This represents the “target” of the session. Format is <i>ddd.ddd.ddd.ddd:port</i> .
	Packets Delta	Not used.
	Mphy	Ingress Port Number.
	Vlan	Ingress VLAN. Normally used to identify the security zone.
	Source Zone UUID	The UUID for the zone on which the source IP address appears.
	Source Zone Name	The zone on which the source IP address appears.
	Destination Zone UUID	The UUID for the zone on which the destination IP address appears.
	Destination Zone Name	The zone on which the destination IP address appears.
	Start time Secs	Unused by Firewall. UDM Log Aggregation.
	Start time Nanosecs	Unused by Firewall. UDM Log Aggregation.
	Period	Unused by Firewall. UDM Log Aggregation.

Table B-3: Firewall Block Log Format (Continued)

Field Name	Sub-Field Name	Description
Message (cont.)	Message Params	<p>The Message Params are further delimited as using the ‘ ’ character as follows:</p> <ul style="list-style-type: none"> • FirewallRuleId: The customer-visible firewall rule ID that matched (allowed) the session to go through. By definition this is a Permit rule. This should match the Policy UUID. • Category: For Web requests that were filtered by the Web Filter Subscription Service, the category that the URL field was matched to. • URLInfo: For Web requests, this is the extra information from Web filter engine for block decision. • URL For Web requests, the target URL. This field is filled in regardless of whether the request was filtered by the Web Filter Subscription Service. <p>When the log is being saved, the fields in Message Params are exported with tab separation (blanks for unused fields) to allow easy import into Excel.</p>
	Packet trace flag	Packet trace not supported by Firewall.
	Packet trace seq begin	Packet trace not supported by Firewall.
	Packet trace seq end	Packet trace not supported by Firewall.

The fields in this table are populated depending on the event being logged:

- **Block event** — This event represents a firewall block. The Category, URL, Session Start, and Bytes fields will be blank. The Firewall Rule field should be a hyperlink to the Firewall Rule edit page.
- **Web Filter Block Event** — This event is generated for a Web content request that is blocked. All specified fields are provided. The category field will be populated if the Web content request was blocked by the Web Filter Subscription service (not for a manual URL block).

Firewall Session Log Format

An example of a tab-delimited Firewall Session Log entry follows:

```
Aug 16 12:55:58 10.0.2.254 AUG 16 12:58:59 2007 device02 [fws]
10.0.2.1:52319 10.0.2.254:22 6 TCP(6) 0dc7c57b-4ff9-467f-8ef6-
d5069850a1c6 WAN f28c0bb7-c4be-11da-9598-00016cccb0cf this-device 1
4876 Session ended Sent Bytes:2472 Recv Bytes:2404 Sent Packets:17
Recv Packets:18
```

The following table describes the downloadable format of the Firewall Session Log:

Table B-4: Firewall Session Log Format

Field Name	Description
Seq	Unique sequence number for this log file.
Entry_time	Date and time of event, in the format <i>yyyy-mm-dd 24H:mm:ss</i> .
Sev	Severity of the alert, from least to most severe: <ul style="list-style-type: none"> • INFO = for information only • WARN = warning • ERR = error • CRIT = critical
Comp	Software component that generated the message. Examples: GEN, TNT
SrcIP	The source IP address and port for the session. This represents the “starter” of the session. Format is <i>ddd.ddd.ddd.ddd:port</i> .
DstIP	The destination IP address and port for the session. This represents the “target” of the session. Format is <i>ddd.ddd.ddd.ddd:port</i> .
Protocol Number	
Protocol	<i><protocol name> (<protocol number>)</i>
Source Zone UUID	The UUID for the zone on which the source IP address appears.
Source Zone Name	The zone on which the source IP address appears.
Destination Zone UUID	The UUID for the zone on which the destination IP address appears.
Destination Zone Name	The zone on which the destination IP address appears.
Firewall Rule ID	The firewall rule ID that matched (allowed) the session to go through. By definition this is a Permit rule.
Category	For Web requests that were filtered by the Web Filter Subscription Service, this is the category to which the URL field was matched.

Table B–4: Firewall Session Log Format (Continued)

Field Name	Description
URL	For Web requests, the target URL. This field is populated regardless of whether the request was filtered by the Web Filter Subscription Service.
Session Duration(s)	For Session End Events only, this field contains the duration of the session from its start time, in the format <i>dd:hh:mm.ss</i> .
Message	The message text associated with the event.
Bytes	For Session End Events only, this field contains the number of bytes sent and received during the session.
Packets	For Session End Events only, this field contains the number of packets sent and received during the session.

VPN Log Format

An example of a comma-delimited VPN Log entry follows:

```
17,2006-10-05 17:12:31,INFO,VPN,"152.67.137.49:500 10.171.2.254:500
Responder started IKE phase 1, main mode"
```

The following table describes the downloadable format of the VPN Log:

Table B–5: VPN Log Format

Field Name	Description
Seq	Unique sequence number for this log file.
Entry_time	Date and time of event, in the format <i>yyyy-mm-dd 24H:mm:ss</i> .
Sev	Severity of the alert, from least to most severe: <ul style="list-style-type: none"> • INFO = for information only • WARN = warning • ERR = error • CRIT = critical
Comp	Software component that generated the message: VPN.
Message (contained within quotes)	The message text associated with the event.

System Log Format

An example of a comma-delimited System Log entry follows:

```
21,2006-08-04 12:43:29,ERR ,DRV,"No cryptonet devices found."
```

The following table describes the downloadable format of the System Log:

Table B-6: System Log Format

Field Name	Description
Seq	Unique sequence number for this log file.
Entry_time	Date and time of event, in the format <i>yyyy-mm-dd 24H:mm:ss</i> .
Sev	Severity of the alert, from least to most severe: <ul style="list-style-type: none"> • INFO = for information only • WARN = warning • ERR = error • CRIT = critical
Comp	Software component that generated the message. Examples: SYS, UDM, and HTP.
Message (contained within quotes)	The message text associated with the event. For a list of High Availability messages, see “High Availability Log Messages” on page 327 .

Remote Syslog Log Format

The remote syslog format for the Alert, IPS Block, and Firewall Block Logs is described in this section.



Note For the System, Audit, VPN, and Firewall Session Logs, there is no specific format for the remote syslog. For these logs, the downloaded file is sent directly to the remote syslog server as a straight data dump without any manipulation of the data.

The following is an example of packet data sent to a collector. Collectors may display the header portion of the stream differently.

```
<13>Jan 13 12:55:01 192.168.65.22 ALT,v4,20050113T125501+0360,"i
robot"/192.168.65.22,1017,Alert,1,1,00000002-0002-0002-0002-
000000000164,"0164: ICMP: EchoRequest (Ping)","0164: ICMP: Echo
Request (Ping)",icmp,0,216.136.107.233:0,216.136.107.91:0,20
050113T125205+0360,199," ",1,3:1
```

In this example, the header follows the standard syslog format. Using the previous log entry as the example, the message is as follows:

```
ALT,v4,20050113T125501+0360,"i robot"/
192.168.65.22,1017,Permit,1,Low,00000002-0002-0002-0002-
000000000164,"0164: ICMP: EchoRequest (Ping)","0164: ICMP: Echo
Request (Ping)",icmp,0,216.136.107.233:0,216.136.107.91:0,20050113T1252
05+0360,199," ",1,3:1
```

The character located between each field is the configured delimiter, in this case a comma. The following table details the fields and their descriptions:

Table B–7: Remote Syslog Field Descriptions

Field	Description
1	Log type: ALT = alert, BLK = block, P2P = misuse and abuse.
2	Version of this message format.
3	ISO 8601 Date-Time-TZ when this alert was generated.
4	Host name/IP address that generated the alert. The quotes are required for this release because of a bug in the hostname validation (note the space in the name).
5	Sequence ID.
6	Reserved.
7	Action performed: “Block” or “Permit.”
8	Severity: “Low”, “Minor”, “Major,” or “Critical.”
9	Policy UUID.
10	Policy Name.

Table B–7: Remote Syslog Field Descriptions (Continued)

Field	Description
11	Signature Name.
12	Protocol name: “icmp,” “udp,” “tcp,” or “unknown.”
13	Firewall IP Protocol Numeric and String, in the format <code><uint> (<string>)</code> . Only used in Firewall Block Logs. In all other logs, this field will be 0.
14	Source address and port, colon delimited.
15	Destination address and port, colon delimited.
16	ISO 8601 Date-Time-TZ when the aggregation period started.
17	Number of events since start of aggregation period.
18	Traffic Threshold message parameters.
19	Traffic capture available on device: available = 1; none = 0.
20	Slot and segment of event.

High Availability Log Messages

The High Availability mechanism logs the following messages to the System Log. For details on the System Log, see [“System Log Format” on page 325](#).

Table B–8: High Availability Log Messages

Message	Type	Description
Changed to HA active state	Informational	Standby device has determined that active device is not responding to HA polling or has been manually forced to active state.
Changed to HA standby state	Informational	Active device has determined that it should return to standby state or has been manually forced to standby state.
Active HA device (ip-address) detected	Informational	Standby device has detected one of the HA management IP addresses of active device. This is logged for each of the IP interfaces that is configured with an HA management IP address.

Table B–8: High Availability Log Messages (Continued)

Message	Type	Description
Standby HA device (ip-address) detected	Informational	Active device has detected one of the HA management IP addresses of standby device. This should be logged for each of the IP interfaces that is configured with an HA management IP address.
Active HA device (ip-address) requesting pre-emption	Informational	Active device has detected that other device is also active (e.g. manually forced to active) and should return to standby state.
Active HA device (ip-address) no longer detected	Warning	Standby device has determined that active device is not responding to the HA heartbeat mechanism on one of the HA management IP addresses.
Standby HA device (ip-address) no longer detected	Warning	Active device has determined that standby device is no longer polling it on one of the HA management IP addresses.

System Update Status Messages

The LSM provides update status on the progress of the update. The messages include “<Update State>:<qualifier>”. The <Update State> indicates the state of the update. The <qualifier> provides information about the state. The following table details the messages that display on the LCD screen during an update of the TOS:

Table B–9: Update States

Update State	Description
Ready	Device is ready for an update.
Updating	Device is in the process of updating.
UpdateCommitting	Device has rebooted and is processing the final update steps.
UpdateFailure	Device failed Update. The screen displays the reason.
Rollback	Device is in the process of rollback.
RollbackCommitting	Device has rebooted and is processing the final rollback steps.
RollbackFailure	Device failed Rollback. The screen displays the reason.
Failsafe	Device was unable to load a valid image and is running a scaled-back image.

If an error occurs, the information changes. The state displays as “UpdateFailure:<state>,” where <state> is one of the listed states in the previous table. The listed state displays a qualifier and message regarding the state. The following table details the qualifier and messages:

Table B–10: Update Failure Messages

Update Failure Qualifier	Message
OK	Normal operation, no errors.
InvalidUpdateState	Current action is restricted while device is in this state. Fix problem and reset Update State.
InvalidLocation	Package file not found at that location.
RebootDuringUpdate	Device was rebooted during update. Check system log for recommendations.
TarChecksumError	Checksum error when extracting the archive: Corrupted package.
TarExtractError	File system error when extracting the archive.
ArchiveCreateFailure	File system error creating rollback archive.
SystemError	General error during update.
WrongPlatformType	Package is for a different platform. Make sure you have correct package.
PackageReadError	General error while reading package. Possible Truncated or Corrupted package, download new package from TMC and retry update.
WrongPackageType	Package is of unknown type, not an OS or DV package. Make sure you have correct package.
NotEnoughFreeSpace	Not enough available disk space. Remove older installed images.
UnsignedPackage	Package does not have proper digital signature.
MemoryError	Memory error when installing package. Reboot may be necessary.
BadCertificate	Package does not have proper digital certificate.
DowngradeRevisionNotSupported	Using update to install some older versions is not supported.
PackageOpenError	Unable to open package. Make sure you have a correct IPS package.
CannotUpdateDVWhenTSEIsBusy	Unable to update Threat Suppression Engine packages while the system is busy reloading filters. Retry operation later.



Device Maximum Values

Details the maximum values for X family devices.

The following table give the maximum values for configurable parameters of X family devices:

Table C-1: Device Maximum Values

Parameter	X5	X506
Action Sets		
Supported Rates	50, 100, 150, 200, 300, 400, 500, 600, 700, 900 Kbps	50, 100, 150, 200, 250, 300, 350, 400, 450, 500, 600, 700, 800, 900, 1000 Kbps 1.5, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 20, 25, 30, 35, 40, 50, 62, 83 Mbps
Firewall		
Rules	50 (25-user license) 100 (unlimited license)	500
Security Zones	16	32

Table C–1: Device Maximum Values (Continued)

Parameter	X5	X506
Services	125	200
Service Groups	25	50
Sessions	32,000 (25-user license) 60,000 (unlimited license)	131,072
VPN		
Security Associations	50	512
IKE Proposals	25	50
PPTP Sessions	50 (25-user license) 128 (unlimited license)	1,000
L2TP Sessions	50 (25-user license) 128 (unlimited license)	1,000
IPSec Tunnels (Phase 1) not Default SA	50	512
IPSec Tunnels (Phase 1) via Default SA	50	1,000
Network		
IP Address Groups	25	200
Entries per IP Address Group	50	200
Virtual Interfaces	6	32
GRE Virtual Interfaces	4	100
Static Routes	100	500
RIP Routes	5,000	8,000
OSPF Areas	20	50
OSPF Virtual Links	20	50
OSPF Adjacencies	100	300
OSPF Routes	50,000	200,000

Table C–1: Device Maximum Values (Continued)

Parameter	X5	X506
Schedules	25	100
Virtual Servers	25 (25-user license) 50 (unlimited license)	500
DHCP Static Mapping	50 (25-user license) 128 (unlimited license)	512
Certificates		
Local Certificates	5	25
Certificate Requests	5	5
CA Certificates	5	25
Web Content Filter		
URL Patterns	200	1,000
Web Filter Profiles	32	32
Content Filter Default Cache Size	2 MB	4 MB
Users and Privileges		
Local Users	25 (25-user license) 100 (unlimited license)	200
Privilege Groups	10 (25-user license) 50 (unlimited license)	100

Index

A

- access level, user 273
- action sets 42
 - Block 43
 - Block + Notify 43
 - Block + Notify + Trace 43
 - configure, create 45
 - create, quarantine 48
 - default 44
 - flow control 42
 - notification contacts 42
 - packet trace 42
 - Permit + Notify 43
 - Permit + Notify + Trace 43
 - quarantine 46
 - rate limit 46
 - Recommended 43
- Action Sets page 44
- Active User List page 277
- adaptive filter
 - configuration 32, 36
 - configuring 57
 - disabling settings 126
 - events 56, 125
- administrator 273
- aggregation period 50
- alert aggregation 49
- Alert log 316
- Anti-Spam page 95
- Anti-Spam Service 94
 - enabling or disabling 96
 - manual settings 97
 - tuning 96
- Application Protection
 - reconnaissance filters
 - filter tuning 35
 - port scans, host sweeps 35
 - settings 33
- Area ID 175
- Attack Reports page 123
- Audit log 101, 319
 - format 319
- authentication 271
 - OSPF 176
 - RIP 172
- Auto Log Off 11
- Auto Refresh 13, 299
- Auto Update, for Digital Vaccine 246
- AutoDV and High Availability 265
- automatic page refresh 299

B

- bandwidth management 67, 69
- black list 97
- Block 43
- Block + Notify 43
- Block + Notify + Trace 43

- blocked streams 112
 - flushing 113
 - searching for 113
- Blocked Streams page 112
- boot time 16
- bridge mode 132, 151
 - enabling 151
- browser certificates 303, 304, 306, 311, 313

C

- CA certificate
 - configuring CRL parameters 291
 - importing 289
- CA Certificate Page 288
- captive portal 69, 71
- category
 - action sets 42
 - settings, disable filter category, override 31
- certificate authority 306
- Certificate Import Wizard 309
- certificate revocation list (CRL) 289
- certificates 303
 - client authentication message 304
 - example 313
 - importing 294
 - request, creating 294
 - security alert 306
 - certificate authority 306
 - invalid certificate name 311
- client authentication message 304
- clients, local 4
- clock, setting 255
- Command Line Interface (CLI) 5
- configure
 - adaptive filter 56
 - client-to-site VPN 223
 - client-to-site VPNs for Windows
 - clients 232
 - DHCP server 187
 - firewall rules 69
 - high availability 260
 - IP address 143
 - IPSec 201
 - L2TP 225
 - L2TP over IPSec VPN 225
 - L2TP/IPSec VPN client 225
 - LDAP 283
 - management console contact 51
 - network 130
 - NMS 259
 - PAT 83
 - PPTP 236
 - PPTP server 238
 - PPTP VPN client 232
 - quarantine action set 48
 - RADIUS authentication 281
 - remote system log 50, 107, 267
 - segment 133
 - service groups 76
 - SMS 259
 - SNMP 259
 - TSE 56, 112, 114
 - URL Patterns 91
 - virtual servers 81
 - VPN 200
 - Web content filtering 84
 - Windows XP client for PPTP
 - connection 228
- Configure Adaptive Filter Events Report page 125
- Configure DHCP Server page 187
- connection table timeout 55
- content filtering. See Web filtering
- Core Categories filters, configuring 89
- create
 - action set 45
 - action sets 45
 - action sets, quarantine 48
 - black list 97
 - capture file 194
 - certificate request 294
 - filter level setting 21
 - firewall rule 70
 - firewall service 75
 - IKE proposal 221
 - IP interface 143
 - IPSec SA for site-to-site VPN 212
 - notification contact 50
 - OSPF area 178
 - OSPF virtual link 178
 - personal certificate 304
 - personal certificates 313
 - port 53
 - port configuration 52
 - privilege group 279
 - quarantine action set 48
 - schedule 79
 - security profile 20
 - security zone 139
 - service group 76
 - single Phase 2 SA for all traffic 221
 - snapshot 253
 - static route 171
 - TMC account 242
 - TOS software user account 276
 - traffic threshold filter 40, 41
 - URL pattern 91
 - user 274
 - virtual server 82
 - Web filter profile 89
 - white list 97
- Create OSPF Virtual Link page 178
- Create Security Zone page 138
- Create Traffic Capture page 194, 195
- Create Web Filtering Profile page 87
- critical thresholds 265

- current log file 100
- Custom Filter List Page 90
- custom filter list, configuring 90
- Custom Response Page 90
- custom response page, configuring 89
- custom Web filtering 84
- customer support xiv

D

- default gateway 159
- Default Gateway page 159
- default IP gateway 159
- default route 160
- delete
 - CA certificate 288
 - capture file 194
 - certificate request 293
 - days and times from schedule 79
 - filter override 34
 - global IP address limit or exception 34
 - IP address group 158
 - IP interface 143, 177
 - local certificate 297
 - local user account 275
 - notification contact 51
 - OSPF area 176
 - port 53
 - port configuration 52
 - previously installed TOS software
 - version 245
 - privilege group 277, 279
 - schedule 78
 - security association 205
 - security profile 20, 22
 - security zone 23, 136, 151
 - snapshot 254
 - static reservation 192
 - static route 170
 - user account 275
 - virtual server 81
 - Web filter profile 91

- DHCP
 - add static reservation 192
 - address pool 187
 - Default external interface
 - configuration 143
 - lease duration 187
 - lease, releasing 186
 - relay 189
 - configuring as central relay 190
 - configuring as remote VPN relay 191
 - server
 - disabling 188
 - enabling and configuring 187
 - lease duration, allow BOOTP clients 187
 - status summary 15
- DHCP Relay page 189
- DHCP server 185
 - configuration 185
 - configuring 187
- DHCP Server page 186
- DHCP status summary 15
- Digital Vaccine 17, 246
 - downloading update manually 247
 - enabling Auto Update 246

- installing update manually 247
 - update 246, 247
 - version 16
- disable filter category override 31
- disk usage default threshold 265
- DMZ, creating with a Virtual Server 60
- DNS
 - global settings, configuring 159
 - Lookup tool 193
 - name, finding IP address for 193
 - obtaining configuration 159
- DNS page 159
- download update signature 248
- DV. See Digital Vaccine
- dynamic DNS 160
 - enabling 163
 - providers (tbl.) 160
- Dynamic DNS page 161
- dynamic routing 167

E

- edit
 - action set 45
 - default action sets 44
 - default firewall rules 61
 - default SA for client-to-site VPN 211
 - default SA for site-to-site VPN 214
 - filter 28
 - firewall rule 70
 - IKE proposal 221
 - IP address group 158
 - IP interface 143, 144, 150
 - DHCP 146
 - IGMP 182
 - multicasting 156
 - OSPF 152, 177
 - PIM-DM 184
 - PPPoE client 149
 - PPTP client 147
 - RIP 154, 173
 - static IP address 145
 - IPSec SA for site-to-site VPN 212
 - notification contact 50
 - OSPF area 178
 - OSPF virtual link 178
 - port scan/host sweep filter 36
 - preferences 301
 - privilege group 279
 - quarantine action set 48
 - schedule 78, 79
 - security profile 20
 - security zone 139
 - service 76
 - traffic threshold filter 40, 41
 - URL pattern 90
 - virtual server configuration 82
 - Web filter profile 89
- Edit OSPF Virtual Link page 178
- Edit Security Profile page 30
- Edit Security Zone page 138
- email
 - failure 50
 - preferences 266
- email server
 - configuring 266
- Email Server page 266

- encryption 16
- events
 - adaptive filter 56, 125
 - blocked streams 112
 - rate limited streams 114
- exceptions
 - Application Protection 33
- expiration, password 298
- expired DHCP leases 188
- External Interface default configuration 143
- external IP interface, configuring
 - DHCP 146
 - L2TP client 148
 - PPPoE client 149
 - PPTP client 147
 - static IP address 145

F

- failover 164, 166
 - enabling 166
- filter action 17
- filter group, editing category settings 29
- filter override, deleting 34
- Filter Search page 25
- filters
 - action sets 42
 - adaptive filter configuration 32, 36
 - Application Protection reconnaissance filters
 - filter tuning 35
 - port scans, host sweeps 35
 - settings 33
 - category
 - disable override 31
 - create traffic threshold 41
 - editing individual settings 31
 - exceptions 33
 - Application Protection 33
 - limits 33
 - manage 24
 - notification contacts 49
 - rate-limiting 46
 - reset 34
 - search 25
 - traffic threshold 37
 - create 40
 - edit 40
 - update 246
 - view 28
 - View overrides and custom settings 28
 - Filters List page 26
 - Find Network Path tool 194
 - firewall 59
 - and anti-spam 60
 - and virtual servers 60
 - and Web filtering 60
 - block log 103, 320
 - block log format 320
 - control of secondary connections 59
 - schedules 77
 - service group 73
 - services 73
 - session log 104, 323
 - Firewall Reports page 126
 - firewall rule

- and IPS filtering 69
- and multicast routing 180
- and ping 195
- and security zones 69
- bandwidth management 69
- changing order 73
- creating 70
- default (tbl.) 61
- default configuration 69
- editing 70
- enabling or disabling 73
- logging options 68
- schedules 60
- user authentication 69
- Firewall Rules page 66
- firewall service
 - adding 75
 - editing 76
- Firewall Services page 74
- full routed/NAT mode 132

G

- Generic Route Encapsulation (GRE) 149
- global IP address
 - configuring limits/exceptions 33
 - deleting limit/exception settings 34
- GRE tunnel
 - and security zone 149
 - configuring 150

H

- health
 - Auto Refresh option 299
 - module 119
 - performance/throughput 121
 - system summary 14
- Health Monitor
 - default disk and memory thresholds 265
 - reset 266
- Hello Interval 175
- High Availability 241, 260
 - and bridge mode 151
 - configuration 260, 261
 - configuring with AutoDV 265
 - forcing state change 263
 - log 327
 - log messages 327
 - replacing a device 264
 - synchronizing 263
 - troubleshooting 265
 - tuning 264
- historical log file 100
- host
 - quarantine 117
 - sweeps filters 35
- Host Query Interval 181
- HOSTS file 312

I

- icons on launch bar 11, 12
- IGMP 180

- editing configuration 182
- enabling 182
- IGMP Setup page 181
- IKE (Internet Key Exchange) proposal 215
 - aggressive mode 217
 - configuring Phase 1 setup parameters 221
 - configuring Phase 2 setup parameters 223
 - main mode 217
- IKE Proposals page 216
- interface
 - launch bar 12
 - main pane 13
 - system summary 14
- internal clock, setting 255
- Internet Group Management Protocol (IGMP). See IGMP
- Internet Key Exchange (IKE) 215
 - see also IKE
- Intrusion Prevention System (IPS) 17
 - see also IPS
- invalid certificate name 311
- IP address
 - allocation 143
 - configuration 143
 - configuring static 144
 - quarantining 117
 - removing from quarantine 117
- IP Address Groups
 - add an IP address to 158
 - create 158
 - delete IP address from 158
 - edit 158
- IP Address Groups page 157
- IP Address Test page 98
- IP interface
 - bridge mode 151
 - creating, editing, or deleting 143
 - multicast routing 155
 - OSPF 152
 - RIP 153
- IP Interfaces page 142
- IP Security (IPSec) tunnel 149
- IPS 2
 - block log 316
 - filters, resetting 55
- IPS Preferences page 54
- IPS Services page 52
- IPSec 201
 - configuration 201
 - enable 204, 205, 245
 - enabling and configuring 205
 - security association 206
- IPSec Configuration page 204
- IPSec Status page 202

K

- keyword blocking 91

L

- L2TP Server Configuration page 230
- L2TP server, configuring and enabling 231

- L2TP Status page 229
- L2TP/IPSec
 - VPN configuration 225
- launch bar 12
 - icons 12
 - icons on 11
- Layer 2 Tunneling Protocol (L2TP) 225
- layout of LSM screen 10
- LDAP
 - configuring 283
 - testing 285
- LDAP Configuration page 283
- LDAP Schema Configuration page 285
- LDAP Test page 285
- leases, status of 15
- level, user access 273
- Lightweight Directory Access Protocol (LDAP). See LDAP
- link monitoring 165
 - configuring 165
- load balancing 166
 - configuring 166
- local certificate 295
 - exporting 297
 - importing 297
- local clients 4
- Local Security Manager (LSM) 4
- local user 272
- Log pages, Auto Refresh option 299
- logging in 8
- logging mode 56
 - disable if network is congested 56
- Logon Page 9
- logs
 - alert 316
 - audit 101, 319
 - delimiters 316
 - downloading 109
 - firewall block 103, 320
 - firewall session 104, 323
 - formats 316
 - high availability 327
 - IPS block 316
 - maintenance 100
 - managing 108
 - remote system log 326
 - reset 100
 - resetting 110
 - searching 110
 - system 106, 325
 - system summary 15
 - viewing 109
 - VPN 105, 324
- LSA (Link-State Advertisement) 178
- LSM
 - Auto Refresh 299
 - launch bar 12
 - login 8
 - main pane 13
 - overview 1
 - SMS configuration 5
 - system requirements 5
 - TippingPoint 2
 - packet statistics 15
 - screen layout 10
 - security notes 7
 - system summary 14
 - title bar 13

- web client
 - L2TP/IPSec VPN access 232
 - PPTP VPN access 232

M

- MAC address 192
- main menu bar 11
- main pane 13
- manage filters 24
- Managed Streams
 - Blocked Streams
 - find 113
 - flush 113
 - Quarantined Addresses
 - find 116
 - force quarantine 117
 - remove from quarantine 117
 - Rate-Limited Streams
 - find 115
 - flush 115
- management console 51
 - contact, configuring 51
- Max Query Response Time 181
- memory usage 118
 - default threshold 265
- Microsoft Networking 232
- Microsoft Point-to-Point Encryption 232, 239
- model number 16
- module
 - health 119
 - Ethernet Ports 121
- multicast 180
- multicast router 180

N

- NAT 144
- navigation
 - LSM 7
 - overview 10
- navigation pane 10
- network
 - congestion, modify the TSE global
 - configuration 56
 - deployment modes 131
 - path, finding 194
 - tools
 - DNS lookup 193
 - find network path 194
 - packet capture 194
 - ping 195
- Network Address Translation (NAT) 144
 - see also NAT
- Network DHCP status summary 15
- network management system (NMS) 5
- Network Ports page 133
- NMS 259
 - viewing or configuring information 259
- notification contacts 49
 - create 50
 - deleting 51
 - email failure 50
 - email preferences 266
 - nssa (Not So Stubby Area) 178

- NTP server, configuring for 256

O

- one-to-one NAT 80
 - configuring 82
- online help 11
- Open Shortest Path First (OSPF). See OSPF
- operator 273
- OSPF 152
 - diagnostic tools 174
 - editing configuration 177
 - enabling 177
 - enabling and configuring 152
 - LSA 178
 - NSSA 178
 - stub default cost 178
 - TSA 178
- OSPF Setup page 175

P

- Packet Capture 194
- packet capture file, viewing and
 - managing 194
- packet statistics 15
 - resetting 15
- packet, capturing 195
- password
 - changing 276
 - expiration 298
 - security requirement for 299
- performance 121
- Performance Wizard 121
- Permit + Notify 43
- Permit + Notify + Trace 43
- personal certificate
 - creating 304, 313
 - installing 305
- PIM-DM 180
 - editing configuration 184
 - enabling 183
- PIM-DM Setup page 183
- ping 195
- Ping page 196
- Ping tool 195
- Point-to-Point Protocol (PPP) 225
- Point-to-Point Tunnelling Protocol (PPTP) 236
- Poison Reverse 172
- policy rules 59
- port 52
 - add 53
 - configuration 52
 - delete 53
 - disabling 134
 - editing configuration 134
 - link-down error, correcting 135
 - restarting 134
- Port Address Translation (PAT) 81
 - configuration 83
- PPTP
 - VPN Configuration 232
- PPTP server
 - configuring and enabling 239
- PPTP Server Configuration page 238

- PPTP Status page 237
- preemption 264
- Preferences page 298
- preferences, setting 301
- Pre-shared Secret Key (PSK) 225
- privilege group 278
 - adding local users to 280
 - creating or editing 279
- Privilege Groups page 278
- product code 16
- product specification 16
- Productivity Categories filters,
 - configuring 89
- Protocol Independent Multicast-Dense Mode (PIM-DM). See PIM-DM

Q

- quarantine
 - action set 46
 - create action set 48
 - find quarantined hosts 116
 - force host into 117
 - remove hosts from 117
 - timeout 55
- Quarantine Reports page 125
- quarantined address, searching for 116
- Quarantined Addresses page 116
- quarantined streams 111
- Quary Timeout 181

R

- RADIUS page 281
- RADIUS, configuring 281
- Rate Limit Reports page 124
- rate limited streams 114
 - searching for 115
- Rate Limited Streams page 114
- rate limiting 46
- reboot 14, 15
- reconnaissance filters
 - port scan/host sweep 35
 - tuning 35
- refresh screen 13
- regular expression pattern matching 91
- Remote Authentication Dial-In User Service (RADIUS) 280
 - see also RADIUS
- remote system log 326
 - configuring 50, 107
 - format 326
- reports
 - Animate Charts option 123
 - firewall 126
 - quarantine 125
 - rate limit 124
 - Refresh Data option 123
 - top ten filters 123
 - traffic 124
 - traffic threshold 124
 - viewing 123
- requirements, system 5
- reset
 - filters 34
 - IPS filters 55

- log 100, 110
- packet counters 15
- packet statistics 15
- System Log indicator 14
- TCP 42, 43
- Traffic Threshold filter 39
- Retransmit Interval 176
- RIP 153, 171
 - editing configuration 173
 - enabling 173
- RIP Setup page 172
- role, user 273
- rollback 245
 - states, messages 328
- Router Dead Interval 175
- routing 167
 - multicast 180
 - OSPF 174
- Routing Information Protocol (RIP). See RIP
- routing table 167
- Routing Table page 168
- rules, firewall 59

S

- schedule
 - adding or editing 79
 - delete 78
 - edit 78, 79
- schedules
 - deleting days and times from 79
- Schedules page 77
- screen refresh 13
- Secure Management System (SMS) 5
- Security Access Level
 - default setting, changing 299
 - username and password requirements 299
- security alert 306
 - certificate authority 306
 - invalid certificate name 311
- security association 206
 - configuring 212
 - editing default 211
 - editing default for site-to-site VPN 214
- security level, user 273
- Security Management System (SMS) 258
- security profile 17, 19
 - change category settings 21
 - create 20
 - Default 18
 - delete 20
 - edit 20
 - editing a port scan/host sweep filter 36
 - override global filter settings 21
 - restore global category settings 21
 - view 20
- Security Profiles page 20, 35
- security zone
 - adding or removing 151
 - and security profile 17
 - configuring 139
 - creating or editing 139
 - edit configuration, delete 136
 - protected by security profile 22
- Security Zones page 136
- segment configuration 133
- service group 60
 - adding 76
 - editing 77
- Setup Wizard 268
- signature, update
 - download 248
- site-to-site multicasting 184
- SMS
 - configure 259
 - configuring 259
 - device under control of 258
 - disabling or enabling 260
- SMS & NMS page 258
- snapshot
 - creating 253
 - deleting 254
 - exporting 253
 - importing 253
 - restoring 253
- SNMP 258, 259
- software rollback 245
- software update 248
 - states, messages 328
- static reservation 191
 - adding 192
 - deleting 192
- Static Reservations page 192
- static route 169
 - creating 171
- Static Routes page 170
- static routing 167
- status
 - AutoDV 246
 - CA certificate 288
 - certificate request 293
 - device 118
 - DHCP client leases 186
 - dynamic DNS 161
 - interface 143
 - IPSec 202
 - L2TP 229
 - license 86
 - link 164
 - load balancing 165
 - local certificate 296
 - modules 119
 - OSPF interface 175
 - PPTP 236
 - routing table entry 169
 - system 14
 - system update 328
- Strong Encryption Service Pack 16, 200
- Stub Default Cost 178
- super-user 273
- syslog server, configuring contact 267
- Syslog Servers page 107
- system log 106
 - format 325
- system requirements 5
- System Snapshots page 252
- system status 14
- system summary
 - health 14
 - how to display 14
 - log summary 15
 - packet statistics 15
 - product specification 16

- system status 14
- versions 16
- System Summary page 14
 - Auto Refresh option 299

T

- TCP
 - Reset 45
 - Reset option 42
- TCP reset 43
- tech support xiv
- this-device zone 61
- Threat Management Center 242
- Threat Management Center (TMC) xiv
- Threat Suppression Engine (TSE). See TSE
- thresholds
 - critical 265
 - setting 265
- throughput 121
- Time Options page 255
- time zone, setting 257
- TippingPoint 2
- TOOLS page 193
- Top Ten Filters reports 123
- TOS software
 - changing password 276
 - creating user account 276
 - deleting a previously installed version 245
 - downloading update 249
 - installing update 250
 - rolling back to a previous version 244
 - user security level 273
 - version 16
- Traceroute page 197
- Traceroute tool 196
- traffic 122
- Traffic Capture page 195
- Traffic Capture tool 194
- traffic shaping. see bandwidth management
- Traffic Threshold filter 17, 37
 - configure, create, edit 41
- Traffic Threshold Filters page 38
- Transmit Delay 176
- transparent DMZ - NAT/Routed LAN mode 131
- transparent mode 131, 166
- troubleshooting 315
 - and system log 106
 - client-to-site configuration 224
 - email notification 50
 - High Availability 265
 - L2TP/IPSec connections 235
 - OSPF 179
 - PPTP connections 240
- TSA (Totally Stubby Area) 178
- TSE
 - blocked streams 112
 - configuration
 - blocked streams 112
 - rate limited streams 114
 - Configure timeouts 56
 - port configuration 52
 - adding 53
 - deleting 53

rate limited streams 114

U

update

Digital Vaccine

auto 246

manual 247

download signature 248

filter 246

software 248

states, messages 328

Update page 243

URL list

exporting 90

importing 90

URL pattern

regular expression syntax (tbl.) 91

user

access level 273

accounts

valid username and password, security access level 299

authentication 84

create 274

modify 274

username security requirements 299

User List page 274

V

version information 243

system summary 16

View Filter page 31

Virtual Private Network (VPN) 199

see also VPN

virtual server 80

configuring 82

delete 81, 82

edit 81, 82

Virtual Servers page 80

VPN

configuration

IPSec SA Phase 2 negotiation 221

interoperability with other vendors'

IPSec configuration 221

L2TP/IPSec configuration 225

PPTP configuration 232

VPN - IP Security/ IKE page 211

VPN log 105, 324

format 324

W

WAN failover 164

WAN Failover & Load Balancing page 164

warning thresholds 14

Web content filtering 84

Web Content Filtering Service

enabling or disabling 86

server 86

Web filter profile

creating or editing 89

delete 91

Web filtering 84

Web Filtering page 85

white list 97

Windows VPN client 239

WINS server 232, 239

X

X family device

client applications 4

environment 4

maximum values 331

system requirements 5

X.509 CA Certificate Details Page 290

X.509 certificate 286

configuring 286

X.509 Certificates page 215