Technical Support
Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR
Phone (Other Countries): See Support information card.

Product Updates
Product updates are available on the NETGEAR website at http://prosecure.netgear.com or http://kb.netgear.com/app/home.

ProSecure Forum
Go to http://prosecure.netgear.com/community/forum.php for information about the ProSecure forum and to become part of the ProSecure community.

Trademarks
NETGEAR, the NETGEAR logo, ReadyNAS, ProSafe, ProSecure, Smart Wizard, Auto Uplink, X-RAID2, and NeoTV are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT, and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions
To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

<table>
<thead>
<tr>
<th>Manual Part Number</th>
<th>Manual Version Number</th>
<th>Publication Date</th>
<th>Description</th>
</tr>
</thead>
</table>
| 202-10519-06       | 1.0                   | February 2011   | Made the following changes:  
  ▪ Upgraded the book to the new format.  
  ▪ Entirely revised Chapter 6, Monitoring System Access and Performance, to document the new Logs, Reports, and Alerts configuration menus that replaced the old Logs & Reports configuration menu.  
  ▪ Added Appendix A, Report Templates.  
  ▪ Separated the traffic logs into email traffic logs and Web traffic logs (see Configuring and Activating System, Email, and Syslog Logs and Querying Logs).  
  ▪ Under the Monitoring main navigation menu, replaced all screen shots that showed the old Logs & Reports configuration menu with screen shots that show the new Alerts, Logs, and Reports configuration menus. |
<table>
<thead>
<tr>
<th>Code</th>
<th>Version</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>202-10519-06</td>
<td>1.0</td>
<td>February 2011</td>
<td>(continued)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(continued)</td>
<td>- Revised the Setup Wizard update settings information (see <em>Setup Wizard Step 7 of 11: Update Settings</em>), software update information (see <em>Updating the Software</em>), and system status information (see <em>Viewing System Status</em>).</td>
</tr>
<tr>
<td>202-10519-05</td>
<td>1.0</td>
<td>July 2010</td>
<td>Added the following major new features:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Network refresh and permanent MAC address bindings (see <em>Configuring the Network Refresh and Permanent MAC Address Bindings</em>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Setting exceptions for custom groups and custom categories, and setting exceptions for file extensions and protocols (see <em>Setting Scanning Exclusions and Web Access Exceptions</em>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Creating custom groups (see <em>Creating Custom Groups for Web Access Exceptions</em>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Creating custom categories—see <em>Creating Custom Categories for Web Access Exceptions</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Using the DC Agent (see <em>Understanding the ProSecure DC Agent</em>, <em>Requirements for the ProSecure DC Agent Software and DC Agent Server</em>, and <em>Downloading ProSecure DC Agent Software, and Creating and Deleting DC Agents</em>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Also added the following minor features:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Requirement to accept terms of service agreement on the Real-Time Blacklist screen</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Capability to set the public host, IP address, and port on the Distributed Spam Analysis screen</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Capability to replace the content of a blocked page with custom text</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Capability to enable and disable SSLv2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Refinements in the active users search methods.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Domain information in the output screens that are accessible from the Monitoring menu</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Testing a URL as part of the diagnostics tools</td>
</tr>
<tr>
<td>202-10519-01</td>
<td>1.1</td>
<td>October 2009</td>
<td>Index update.</td>
</tr>
<tr>
<td>202-10519-01</td>
<td>1.0</td>
<td>September 2009</td>
<td>Initial publication of this reference manual.</td>
</tr>
</tbody>
</table>
Contents

Chapter 1  Introduction

What Is the ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600? ....................................................... 8
What Can You Do with an STM? ......................................................... 9
Key Features and Capabilities ......................................................... 9
  Stream Scanning for Content Filtering ........................................ 10
  Autosensing Ethernet Connections with Auto Uplink .................. 11
  Easy Installation and Management ............................................. 11
  Maintenance and Support ......................................................... 12
  STM Model Comparison ........................................................... 12
Service Registration Card with License Keys .................................. 12
Package Contents ........................................................................... 13
Hardware Features ......................................................................... 14
  Front Panel Ports and LEDs ...................................................... 14
  Rear Panel Features ................................................................... 20
  Bottom Panel with Product Label .............................................. 22
Choosing a Location for the STM .................................................. 23
Using the Rack-Mounting Kit ......................................................... 24

Chapter 2  Using the Setup Wizard to Provision the STM in Your Network

Choosing a Deployment Scenario .................................................. 25
  Gateway Deployment ............................................................... 25
  Server Group .......................................................................... 26
  Segmented LAN Deployment ................................................... 27
Understanding the Steps for Initial Connection ............................ 27
  Qualified Web Browsers .......................................................... 28
Logging In to the STM ................................................................. 28
  Understanding the Web Management Interface Menu Layout ....... 30
Using the Setup Wizard to Perform the Initial Configuration ......... 32
  Setup Wizard Step 1 of 10: Introduction ................................... 33
  Setup Wizard Step 2 of 11: Networking Settings ....................... 33
  Setup Wizard Step 3 of 11: Time Zone ...................................... 35
  Setup Wizard Step 4 of 11: Email Security ............................... 37
  Setup Wizard Step 5 of 11: Web Security ................................. 39
  Setup Wizard Step 6 of 11: Email Notification Server Settings .... 42
  Setup Wizard Step 7 of 11: Update Settings ............................. 43
  Setup Wizard Step 8 of 11: HTTP Proxy Settings ..................... 45
  Setup Wizard Step 9 of 11: Web Categories ............................. 46
Chapter 3 Performing Network and System Management

- Configuring Network Settings ........................................ 52
- Configuring Session Limits and Timeouts .......................... 56
- Configuring the Network Refresh and Permanent MAC Address Bindings .................................................. 57
  - Managing Permanent MAC Address Bindings ................. 59
- Configuring the HTTP Proxy Settings ............................... 60
- About Users with Administrative and Guest Privileges ........ 61
  - Changing Administrative Passwords and Timeouts ......... 62
- Configuring Remote Management Access ......................... 64
- Using an SNMP Manager .............................................. 65
  - Supported MIB Browsers ........................................... 67
- Managing the Configuration File ..................................... 67
  - Backing Up Settings ............................................... 68
  - Restoring Settings .................................................. 69
  - Reverting to Factory Default Settings .......................... 70
- Updating the Software .................................................. 71
  - Scheduling Updates .................................................. 71
  - Performing a Manual Update ..................................... 73
  - Critical Updates That Require a Restart ................. 74
- Configuring Date and Time Service ................................. 74
- Managing Digital Certificates ....................................... 76
  - Managing the Certificate for HTTPS Scans ................ 78
  - Managing Trusted Certificates ................................ 79
  - Managing Untrusted Certificates ............................... 80
- Managing the Quarantine Settings ................................ 81
- Managing the STM’s Performance .................................. 82

Chapter 4 Content Filtering and Optimizing Scans

- About Content Filtering and Scans ................................. 84
- Default Email and Web Scan Settings ......................... 85
- Configuring Email Protection ....................................... 87
  - Customizing Email Protocol Scan Settings ................ 87
  - Customizing Email Anti-Virus Settings ..................... 88
  - Email Content Filtering ........................................... 94
  - Protecting Against Email Spam ................................. 97
- Configuring Web and Services Protection ......................... 105
  - Customizing Web Protocol Scan Settings .................. 105
  - Configuring Web Malware Scans ............................... 107
ProSecure Web/Email Security Threat Management (STM) Appliance

Chapter 5  Managing Users, Groups, and Authentication

About Users, Groups, and Domains ........................................... 147
Configuring Groups ................................................................. 148
Creating and Deleting Groups by Name ...................................... 149
Editing Groups by Name ............................................................ 150
Creating and Deleting Groups by IP Address and Subnet .............. 151
Configuring User Accounts ....................................................... 152
Creating and Deleting User Accounts ....................................... 153
Editing User Accounts ............................................................... 154
Configuring Authentication ....................................................... 154
Understanding the STM’s Authentication Options ....................... 155
Understanding Active Directories and LDAP Configurations ......... 157
Creating and Deleting LDAP and Active Directory Domains ........ 161
Editing LDAP and Active Directory Domains ............................ 164
Understanding the ProSecure DC Agent .................................... 164
Requirements for the ProSecure DC Agent Software and DC Agent Server .................................................. 165
Downloading ProSecure DC Agent Software, and Creating and Deleting DC Agents ........................................... 165
Creating and Deleting RADIUS Domains .................................. 167
Editing RADIUS Domains and Configuring VLANs .................. 169
Global User Settings ................................................................. 170
Viewing and Logging Out Active Users ..................................... 172

Chapter 6  Monitoring System Access and Performance

Configuring Logging, Alerts, and Event Notifications .................. 175
Configuring the Email Notification Server .................................. 176
Configuring and Activating System, Email, and Syslog Logs ........ 177
Configuring Alerts ................................................................. 182
Understanding the Information on the Dashboard Screen ............ 184
Monitoring Web Usage .............................................................. 190
Viewing System Status ............................................................. 192
Querying Logs .................................................................. 194
Example: Using Logs to Identify Infected Clients ....................... 199
Log Management ..................................................... 199
Viewing, Scheduling, and Generating Reports ....................................... 200
Report Templates .................................................. 200
Generating Reports for Downloading ................................................. 202
Scheduling Automatic Generation and Emailing of Reports ...................... 203
Advanced Report Filtering Options .................................................. 204
Viewing and Managing the Quarantine Files ....................................... 208
Using Diagnostics Utilities .................................................. 215
Using the Network Diagnostic Tools ............................................... 216
Using the Realtime Traffic Diagnostics Tool ........................................ 217
Gathering Important Log Information and Generating a Network Statistics Report ................................................. 218
Restarting and Shutting Down the STM ............................................ 219

Chapter 7  Troubleshooting and Using Online Support

Basic Functioning ........................................................................ 223
Power LED Not On ...................................................................... 223
Test LED or Status LED Never Turns Off ........................................ 223
LAN or WAN Port LEDs Not On .................................................. 224
Troubleshooting the Web Management Interface ................................ 224
When You Enter a URL or IP Address a Time-Out Error Occurs .............. 225
Troubleshooting a TCP/IP Network Using a Ping Utility ....................... 225
Testing the LAN Path to Your STM ............................................... 226
Testing the Path from Your PC to a Remote Device ............................ 226
Restoring the Default Configuration and Password ............................ 227
Problems with Date and Time ..................................................... 228
Using Online Support ..................................................... 228
Enabling Remote Troubleshooting ................................................ 228
Installing Hot Fixes ....................................................................... 229
Sending Suspicious Files to NETGEAR for Analysis ............................ 230
Accessing the Knowledge Base and Documentation ............................ 231

Appendix A  Report Templates

Appendix B  Default Settings and Technical Specifications

Appendix C  Related Documents

Appendix D  Notification of Compliance

Index
Introduction

This chapter provides an overview of the features and capabilities of the ProSecure Web/Email Security Threat Management Appliance STM150, STM300, and STM600. It also identifies the physical features of the appliances and the contents of the product packages.

This chapter contains the following sections:

• What Is the ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600? on this page
• What Can You Do with an STM? on page 9
• Key Features and Capabilities on page 9
• Service Registration Card with License Keys on page 12
• Package Contents on page 13
• Hardware Features on page 14
• Choosing a Location for the STM on page 23

What Is the ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600?

The ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600, hereafter referred to as the STM, is an appliance-based, Web and email security solution that protects the network perimeter against Web-borne threats from spyware, viruses, email, and blended threats. Ideally deployed at the gateway, it serves as the network’s first line of defense against all types of threats, and complements firewalls, intrusion detection systems (IDS)/intrusion prevention systems (IPS), dedicated Intranet security products, and endpoint antivirus and antispyware software.

Powered by patent-pending Stream Scanning technology and backed by one of the most comprehensive malware databases in the industry, the STM can detect and stop all known spyware and viruses at the gateway, preventing them from reaching your desktops and servers, where cleanup would be much more difficult.

In addition to scanning HTTP, HTTPS, FTP, SMTP, POP3, and IMAP traffic, the STM protects networks against spam phishing attacks and unwanted Web use. The STM is a plug-and-play device that can be installed and configured within minutes.
What Can You Do with an STM?

The STM combines robust protection against malware threats with ease of use and advanced reporting and notification features to help you deploy and manage the device with minimal effort.

Here are some of the things that you can do with the STM:

• **Protect the network instantly.** The STM is a plug-and-play security solution that can be instantly added to networks without the need for network reconfiguration.

• **Scan network traffic for malware.** Using the Stream Scanning technology, you can configure the STM to scan HTTP, HTTPS, FTP, SMTP, POP3, and IMAP protocols. Unlike traditional batch-based scan engines that need to cache the entire file before they can scan, this scan engine checks traffic as it enters the network, ensuring unimpeded network performance.

• **Set access policies for individual users or groups.** You can configure Web and email access policies for individual users and groups based on the STM’s local database, on a group IP address, on a Lightweight Directory Access Protocol (LDAP) domain, group, or user, or on a RADIUS VLAN.

• **Receive real-time alerts and generate comprehensive reports.** You can configure the STM to send alerts when a malware attack or outbreak is detected on the network. Real-time alerts can be sent by email, allowing you to monitor malware events wherever you are.

By configuring the STM to send malware alerts, you can isolate and clean the infected computer before the malware incident can develop into a full-blown outbreak. The STM also provides comprehensive reports that you can use to analyze network and malware trends.

• **Manage through SNMP support.** You can enable and configure the STM’s Simple Network Management Protocol (SNMP) settings to receive SNMP traps through a supported management information base (MIB) browser.

• **Allow automated component updates.** Downloading components regularly is the key to ensuring updated protection against new threats. The STM makes this administrative task easier by supporting automatic malware pattern, program, and engine updates.

Key Features and Capabilities

The STM provides the following key features and capabilities:

• Up to two pairs of 10/100/1000 Mbps Gigabit Ethernet WAN ports (see STM Model Comparison on page 12).

• Scalable support (see STM Model Comparison on page 12) for:
  - Up to 600 concurrent users
  - Up to 6000 concurrently scanned HTTP sessions
- Up to 239 MB/s HTTP throughput
- Up to 960,000 emails per hour SMTP throughput

- Stream Scanning technology that enables scanning of real-time protocols such as HTTP.
- Comprehensive Web and email inbound and outbound security, covering six major network protocols: HTTP, HTTPS, FTP, SMTP, POP3, and IMAP.
- URL content filtering with 64 categories.
- Malware database containing hundreds of thousands of signatures of spyware, viruses, and other malware threats.
- Very frequently updated malware signatures, hourly if required. The STM can automatically check for new malware signatures as frequently as every 15 minutes.
- Multiple antispam technologies to provide extensive protection against unwanted emails.
- Spam and malware quarantine for easy analysis.
- Web application control, including access control for instant messaging, media applications, peer-to-peer applications, and Web-based tools and toolbars.
- User management with LDAP, Active Directory, and RADIUS integration, allowing you to configure access policies per user and per group.
- Easy, Web-based wizard setup for installation and management.
- SNMP-manageable.
- Dedicated management interface. (This feature is model dependent; see STM Model Comparison on page 12.)
- Hardware bypass port to prevent network disruption in case of failure. (This feature is model dependent; see STM Model Comparison on page 12.)
- Front panel LEDs for easy monitoring of status and activity.
- Internal universal switching power supply.

Stream Scanning for Content Filtering

Stream Scanning is based on the simple observation that network traffic travels in streams. The STM scan engine starts receiving and analyzing traffic as the stream enters the network. As soon as a number of bytes are available, scanning starts. The scan engine continues to scan more bytes as they become available, while at the same time another thread starts to deliver the bytes that have been scanned.

This multithreaded approach, in which the receiving, scanning, and delivering processes occur concurrently, ensures that network performance remains unimpeded. The result is file scanning that is up to five times faster than with traditional antivirus solutions—a performance advantage that you will notice.

Stream Scanning also enables organizations to withstand massive spikes in traffic, as in the event of a malware outbreak. The scan engine has the following capabilities:

- **Real-time protection.** The Stream Scanning technology enables scanning of previously undefended real-time protocols, such as HTTP. Network activities susceptible to latency (for example, Web browsing) are no longer brought to a standstill.
• **Comprehensive protection.** Provides both Web and email security, covering six major network protocols: HTTP, HTTPS, FTP, SMTP, POP3, and IMAP. The STM uses enterprise-class scan engines employing both signature-based and distributed spam analysis to stop both known and unknown threats. The malware database contains hundreds of thousands of signatures of spyware, viruses, and other malware.

• **Objectionable traffic protection.** The STM prevents objectionable content from reaching your computers. You can control access to the Internet content by screening for Web categories, Web addresses, and Web services. You can log and report attempts to access objectionable Internet sites.

• **Automatic signature updates.** Malware signatures are updated as frequently as every hour, and the STM can check automatically for new signatures as frequently as every 15 minutes.

**Autosensing Ethernet Connections with Auto Uplink**

With its internal 10/100/1000 ports, the STM can connect to either a 10 Mbps standard Ethernet network, a 100 Mbps Fast Ethernet network, or a 1000 Mbps Gigabit Ethernet network. The interfaces are autosensing and capable of full-duplex or half-duplex operation.

The STM incorporates Auto Uplink™ technology. Each Ethernet port automatically senses whether the Ethernet cable plugged into the port should have a “normal” connection such as to a PC or an “uplink” connection such as to a switch or hub. That port then configures itself correctly. This feature eliminates the need to think about crossover cables, as Auto Uplink accommodates either type of cable to make the right connection.

**Easy Installation and Management**

You can install, configure, and operate the STM within minutes after connecting it to the network. The following features simplify installation and management tasks:

• **Browser-based management.** Browser-based configuration allows you to easily configure the STM from almost any type of operating system, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided, and online help documentation is built into the browser-based Web Management Interface.

• **SNMP.** The STM supports SNMP to let you monitor and manage log resources from an SNMP-compliant system manager. The SNMP system configuration lets you change the system variables for MIB2.

• **Diagnostic functions.** The STM incorporates built-in diagnostic functions such as a ping utility, traceroute utility, DNS lookup utility, and remote restart.

• **Remote management.** The STM allows you to log in to the Web Management Interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses.

• **Visual monitoring.** The STM’s front panel LEDs provide an easy way to monitor its status and activity.
Maintenance and Support

NETGEAR offers technical support seven days a week, 24 hours a day. Information about support is available on the NETGEAR ProSecure website at http://prosecure.netgear.com/support/index.php.

STM Model Comparison

The following table compares the three STM models to show the differences:

Table 1. Differences between the STM Models

<table>
<thead>
<tr>
<th>Feature</th>
<th>STM150</th>
<th>STM300</th>
<th>STM600</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance and Sizing Guidelines</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Concurrent users</td>
<td>Up to 150</td>
<td>Up to 300</td>
<td>Up to 600</td>
</tr>
<tr>
<td>Web scan throughput</td>
<td>42 Mbps</td>
<td>136 Mbps</td>
<td>307 Mbps</td>
</tr>
<tr>
<td>Concurrent scanned HTTP connections</td>
<td>1500</td>
<td>3000</td>
<td>6000</td>
</tr>
<tr>
<td>SMTP throughput (emails per hour)</td>
<td>122,000</td>
<td>355,000</td>
<td>550,000</td>
</tr>
<tr>
<td><strong>Hardware</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Gigabit RJ-45 ports                         | Total of 5 ports:  
• 1 uplink
• 4 downlink | Total of 3 ports:  
• 1 pair of ports (1 uplink and 1 downlink)  
• 1 management | Total of 5 ports:  
• 2 pairs of ports\(^a\)  
(2 uplink and 2 downlink)  
• 1 management |
| Gigabit RJ-45 port pairs with failure bypass | 0       | 1 pair of ports  | 2 pairs of ports |
| Dedicated management VLAN RJ45 ports         | 0       | 1       | 1       |

\(^a\) The STM600 provides two pairs of ports, allowing for support of two separate networks or subnets with strict traffic separation.

Service Registration Card with License Keys

Be sure to store the license key card that came with your STM in a secure location. You do need these keys to activate your product during the initial setup.
Note: If you reset the STM to the original factory default settings after you have entered the license keys to activate the STM (see Registering the STM with NETGEAR on page 50), the license keys are erased. The license keys and the different types of licenses that are available for the STM are no longer displayed on the Registration screen. However, after you have reconfigured the STM to connect to the Internet and to the NETGEAR registration server, the STM retrieves and restores all registration information based on its MAC address and hardware serial number. You do not need to reenter the license keys and reactivate the STM.

Package Contents

The STM product package contains the following items:

- ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600
- One AC power cable
- Rubber feet (4) with adhesive backing
- One rack-mount kit
- Straight-through Category 5 Ethernet cable
Hardware Features

The front panel ports and LEDs, rear panel ports, and bottom label of the STM models are described in this section.

Front Panel Ports and LEDs

The front panels of the three STM models provide different components.

STM150 Front Panel

The following figure shows the front panel ports and status light-emitting diodes (LEDs) of the STM150:

Figure 2.

From left to right, the STM150’s front panel shows the following ports and LEDs:

1. Power LED.
2. Test LED.
3. One nonfunctioning USB port. This port is included for future management enhancements. The port is currently not operable on any STM model.
4. One uplink (WAN) Gigabit Ethernet port with an RJ-45 connector, left LED, and right LED.
5. Four downlink (LAN) Gigabit Ethernet ports with RJ-45 connectors, left LEDs, and right LEDs.
The function of each STM150 LED is described in the following table:

### Table 2. LED Descriptions for the STM150

<table>
<thead>
<tr>
<th>Object</th>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>On (green)</td>
<td>Power is supplied to the STM.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Power is not supplied to the STM.</td>
</tr>
<tr>
<td>Test</td>
<td>On (amber) during startup</td>
<td>The STM is initializing. After approximately 2 minutes, when the STM has</td>
</tr>
<tr>
<td></td>
<td></td>
<td>completed its initialization, the Test LED turns off. If the Test LED</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>remains on, the initialization has failed.</td>
</tr>
<tr>
<td></td>
<td>Blinking (amber)</td>
<td>The STM is shutting down.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Software is being updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A hotfix is being installed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>One of the three licenses has expired. To stop the Test LED from blinking,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>renew the license, or click the <strong>Stop LED Blinking</strong> button on the System</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Status screen (see <strong>Viewing System Status</strong> on page 192).</td>
</tr>
<tr>
<td>Uplink (WAN) Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Left LED</td>
<td>Off</td>
<td>The WAN port has no physical link, that is, no Ethernet cable is plugged</td>
</tr>
<tr>
<td></td>
<td>On (green)</td>
<td>into the STM.</td>
</tr>
<tr>
<td></td>
<td>Blink (green)</td>
<td>Data is being transmitted or received by the WAN port.</td>
</tr>
<tr>
<td>Right LED</td>
<td>Off</td>
<td>The WAN port is operating at 10 Mbps.</td>
</tr>
<tr>
<td></td>
<td>On (amber)</td>
<td>The WAN port is operating at 100 Mbps.</td>
</tr>
<tr>
<td></td>
<td>On (green)</td>
<td>The WAN port is operating at 1000 Mbps.</td>
</tr>
<tr>
<td>Downlink (LAN) Ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Left LED</td>
<td>Off</td>
<td>The LAN port has no link.</td>
</tr>
<tr>
<td></td>
<td>On (green)</td>
<td>The LAN port has detected a link with a connected Ethernet device.</td>
</tr>
<tr>
<td></td>
<td>Blink (green)</td>
<td>Data is being transmitted or received by the LAN port.</td>
</tr>
</tbody>
</table>
Table 2. LED Descriptions for the STM150 (Continued)

<table>
<thead>
<tr>
<th>Object</th>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right LED</td>
<td>Off</td>
<td>The LAN port is operating at 10 Mbps.</td>
</tr>
<tr>
<td></td>
<td>On (amber)</td>
<td>The LAN port is operating at 100 Mbps.</td>
</tr>
<tr>
<td></td>
<td>On (green)</td>
<td>The LAN port is operating at 1000 Mbps.</td>
</tr>
</tbody>
</table>

**Front Panel STM300**

The following figure shows the front panel ports and LEDs of the STM300:

![ STM300 Front Panel Diagram ]

**Figure 3.**

From left to right, the STM300’s front panel shows the following ports and LEDs:

1. Console port. Port for connecting to an optional console terminal. The port has a DB9 male connector. The default baud rate is 9600 K. The pinouts are (2) Tx, (3) Rx, (5) and (7) Gnd.
2. Power LED.
3. Status LED.
4. Hard drive (HDD) LED.
5. One nonfunctioning USB port. This port is included for future management enhancements. The port is currently not operable on any STM model.
6. Dedicated management (Mgmt) Gigabit Ethernet port with an RJ-45 connector.
7. One uplink (WAN) Gigabit Ethernet port with an RJ-45 connector, left LED, and right LED.
8. One downlink (LAN) Gigabit Ethernet port with RJ-45 connectors, left LED, and right LED.

**Note:** All Gigabit Ethernet ports provide switched N-way, automatic speed-negotiating, auto MDI/MDIX technology.
The function of each STM300 LED is described in the following table:

**Table 3. LED Descriptions for the STM300**

<table>
<thead>
<tr>
<th>Object</th>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>On (green)</td>
<td>Power is supplied to the STM.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Power is not supplied to the STM.</td>
</tr>
<tr>
<td>Status</td>
<td>On (amber) during startup</td>
<td>The STM is initializing. After approximately 2 minutes, when the STM has completed its initialization, the Status LED turns off. If the Status LED remains on, the initialization has failed.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>The system has completed its initialization successfully. The Status LED should be off during normal operation.</td>
</tr>
<tr>
<td></td>
<td>Blinking (amber)</td>
<td>The STM is shutting down. Software is being updated. A hotfix is being installed. One of the three licenses has expired. To stop the Status LED from blinking, renew the license, or click the Stop LED Blinking button on the System Status screen (see Viewing System Status on page 192).</td>
</tr>
<tr>
<td>HDD</td>
<td>On (Green)</td>
<td>Information is being written to the hard drive.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No hard drive activity.</td>
</tr>
</tbody>
</table>

**Uplink (WAN) Port**

<table>
<thead>
<tr>
<th>Left LED</th>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td></td>
<td>The WAN port has no physical link, that is, no Ethernet cable is plugged into the STM.</td>
</tr>
<tr>
<td>On (green)</td>
<td></td>
<td>The WAN port has a valid connection with a device that provides an Internet connection.</td>
</tr>
<tr>
<td>Blink (green)</td>
<td></td>
<td>Data is being transmitted or received by the WAN port.</td>
</tr>
<tr>
<td>Right LED</td>
<td>Off</td>
<td>The WAN port is operating at 10 Mbps.</td>
</tr>
<tr>
<td></td>
<td>On (green)</td>
<td>The WAN port is operating at 100 Mbps.</td>
</tr>
<tr>
<td></td>
<td>On (amber)</td>
<td>The WAN port is operating at 1000 Mbps.</td>
</tr>
</tbody>
</table>

**Downlink (LAN) Ports**

<table>
<thead>
<tr>
<th>Left LED</th>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td></td>
<td>The LAN port has no link.</td>
</tr>
<tr>
<td>On (green)</td>
<td></td>
<td>The LAN port has detected a link with a connected Ethernet device.</td>
</tr>
<tr>
<td>Blink (green)</td>
<td></td>
<td>Data is being transmitted or received by the LAN port.</td>
</tr>
<tr>
<td>Right LED</td>
<td>Off</td>
<td>The LAN port is operating at 10 Mbps.</td>
</tr>
<tr>
<td></td>
<td>On (green)</td>
<td>The LAN port is operating at 100 Mbps.</td>
</tr>
<tr>
<td></td>
<td>On (amber)</td>
<td>The LAN port is operating at 1000 Mbps.</td>
</tr>
</tbody>
</table>
Front Panel STM600

The following figure shows the front panel ports and LEDs of the STM600:

1. **Console port.** Port for connecting to an optional console terminal. The port has a DB9 male connector. The default baud rate is 9600 K. The pinouts are (2) Tx, (3) Rx, (5) and (7) Gnd.
2. **Power LED.**
3. **Status LED.**
4. **Hard drive (HDD) LED.**
5. One nonfunctioning USB port. This port is included for future management enhancements. The port is currently not operable on any STM model.
6. **Dedicated management (Mgmt) Gigabit Ethernet port with an RJ-45 connector.**
7. **Pair 1 uplink (WAN) and downlink (LAN) Gigabit Ethernet ports with RJ-45 connectors, left LEDs, and right LEDs.**
8. **Pair 2 uplink (WAN) and downlink (LAN) Gigabit Ethernet ports with RJ-45 connectors, left LEDs, and right LEDs.**

**Note:** All Gigabit Ethernet ports provide switched N-way, automatic speed-negotiating, auto MDI/MDIX technology.
The function of each STM600 LED is described in the following table:

Table 4. LED Descriptions for the STM600

<table>
<thead>
<tr>
<th>Object</th>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>On (green)</td>
<td>Power is supplied to the STM.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Power is not supplied to the STM.</td>
</tr>
<tr>
<td>Status</td>
<td>On (amber)</td>
<td>The STM is initializing. After approximately 2 minutes, when the STM has completed its initialization, the Status LED turns off. If the Status LED remains on, the initialization has failed.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>The system has completed its initialization successfully. The Status LED should be off during normal operation.</td>
</tr>
<tr>
<td></td>
<td>Blinking (amber)</td>
<td>The STM is shutting down. Software is being updated. A hotfix is being installed. One of the three licenses has expired. To stop the Status LED from blinking, renew the license, or click the Stop LED Blinking button on the System Status screen (see Viewing System Status on page 192).</td>
</tr>
<tr>
<td>HDD</td>
<td>On (green)</td>
<td>Information is being written to the hard drive.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No hard drive activity.</td>
</tr>
</tbody>
</table>

Uplink (WAN) Port

<table>
<thead>
<tr>
<th>Left LED</th>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Off</td>
<td>The WAN port has no physical link, that is, no Ethernet cable is plugged into the STM.</td>
</tr>
<tr>
<td></td>
<td>On (green)</td>
<td>The WAN port has a valid connection with a device that provides an Internet connection.</td>
</tr>
<tr>
<td></td>
<td>Blink (green)</td>
<td>Data is being transmitted or received by the WAN port.</td>
</tr>
<tr>
<td>Right LED</td>
<td>Off</td>
<td>The WAN port is operating at 10 Mbps.</td>
</tr>
<tr>
<td></td>
<td>On (green)</td>
<td>The WAN port is operating at 100 Mbps.</td>
</tr>
<tr>
<td></td>
<td>On (amber)</td>
<td>The WAN port is operating at 1000 Mbps.</td>
</tr>
</tbody>
</table>

Downlink (LAN) Ports

<table>
<thead>
<tr>
<th>Left LED</th>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Off</td>
<td>The LAN port has no link.</td>
</tr>
<tr>
<td></td>
<td>On (green)</td>
<td>The LAN port has detected a link with a connected Ethernet device.</td>
</tr>
<tr>
<td></td>
<td>Blink (green)</td>
<td>Data is being transmitted or received by the LAN port.</td>
</tr>
<tr>
<td>Right LED</td>
<td>Off</td>
<td>The LAN port is operating at 10 Mbps.</td>
</tr>
<tr>
<td></td>
<td>On (green)</td>
<td>The LAN port is operating at 100 Mbps.</td>
</tr>
<tr>
<td></td>
<td>On (amber)</td>
<td>The LAN port is operating at 1000 Mbps.</td>
</tr>
</tbody>
</table>
Rear Panel Features

The rear panel of the STM150 differs from the rear panels of the STM300 and STM600.

**Rear Panel STM150**

The following figure shows the rear panel components of the STM150:

![Rear Panel STM150](image)

1) Console port 2) Lock 3) Power button 4) Reset button 5) AC power socket

**Figure 5.**

From left to right, the STM150’s rear panel components are:

1. Console port. Port for connecting to an optional console terminal. The port has a DB9 male connector. The default baud rate is 9600 K. The pinouts are (2) Tx, (3) Rx, (5) and (7) Gnd.
2. Kensington lock. Attach an optional Kensington lock to prevent unauthorized removal of the STM150.
3. Power button. Press to restart the STM150. Restarting does not reset the STM150 to its factory defaults.
4. Reset button. Using a sharp object, press and hold this button for about 10 seconds until the front panel Test LED flashes and the STM150 returns to factory default settings.

**Note:** If you reset the STM150, all configuration settings are lost and the default passwords are restored.

5. AC power socket. Attach the power cord to this socket.
Rear Panel STM300 and STM600

The rear panels of the STM300 and STM600 are identical.

The following figure shows the rear panel components of the STM300 and STM600:

![Rear Panel STM300 and STM600](image)

**Figure 6.**

From left to right, the STM300’s and STM600’s rear panel components (excluding the four fan air outlets) are:

1. **Power switch.** Switch to turn the STM300 or STM600 on or off. Restarting does not reset the STM300 or STM600 to its factory defaults.

   **Note:** The STM300 and STM600 do not provide a Reset button. For information about how to reset the STM300 or STM600 to factory default settings using the Web Management Interface, see *Reverting to Factory Default Settings* on page 70.

2. **AC power socket.** Attach the power cord to this socket.
The product label on the bottom of the STM’s enclosure displays the STM’s default IP address, default user name, and default password, as well as regulatory compliance, input power, and other information.

**STM150 Product Label**

![STM150 Product Label](image)

Figure 7.

**STM300 Product Label**

![STM300 Product Label](image)

Figure 8.
STM600 Product Label

Choosing a Location for the STM

The STM is suitable for use in an office environment where it can be freestanding (on its runner feet) or mounted into a standard 19-inch equipment rack. Alternatively, you can rack-mount the STM in a wiring closet or equipment room. A mounting kit, containing two mounting brackets and four screws, is provided in the STM package.

Consider the following when deciding where to position the STM:

- The unit is accessible and cables can be connected easily.
- Cabling is away from sources of electrical noise. These include lift shafts, microwave ovens, and air-conditioning units.
- Water or moisture cannot enter the case of the unit.
- Airflow around the unit and through the vents in the side of the case is not restricted. Provide a minimum of 25 mm or 1 inch clearance.
- The air is as free of dust as possible.
- Temperature operating limits are not likely to be exceeded. Install the unit in a clean, air-conditioned environment. For information about the recommended operating temperatures for the STM, see Appendix B, Default Settings and Technical Specifications.
Using the Rack-Mounting Kit

Use the mounting kit for the STM to install the appliance in a rack. (A mounting kit is provided in the product package for the STM.) The mounting brackets that are supplied with the STM are usually installed before the unit is shipped out. If the brackets are not yet installed, attach them using the supplied hardware.

Figure 10.

Before mounting the STM in a rack, verify that:

- You have the correct screws (supplied with the installation kit).
- The rack onto which you will mount the STM is suitably located.
This chapter describes provisioning the STM in your network. This chapter contains the following sections:

- **Choosing a Deployment Scenario** on this page
- **Understanding the Steps for Initial Connection** on page 27
- **Logging In to the STM** on page 28
- **Using the Setup Wizard to Perform the Initial Configuration** on page 32
- **Verifying Correct Installation** on page 49
- **Registering the STM with NETGEAR** on page 50
- **What to Do Next** on page 51

## Choosing a Deployment Scenario

The STM is an inline transparent bridge appliance that can easily be deployed to any point on the network without the need for network reconfiguration or additional hardware.

The following are the most common deployment scenarios for the STM. Depending on your network environment and the areas that you want to protect, you can choose one or a combination of the deployment scenarios that are described in the following sections:

- **Gateway Deployment** on this page
- **Server Group** on page 26
- **Segmented LAN Deployment** on page 27

## Gateway Deployment

In a typical gateway deployment scenario, a single STM appliance is installed at the gateway—between the firewall and the LAN core switch—to protect the network against all malware threats entering and leaving the gateway. Installing the STM behind the firewall protects it from denial of service (DoS) attacks.
The following figure shows a typical gateway deployment scenario:

Figure 11.

**Server Group**

In a server group deployment, one STM appliance is installed at the gateway and another in front of the server group to help protect the email server from threats from internal as well as external clients. This type of deployment splits the network load and provides the email server with dedicated protection against malware threats, including email-borne viruses and spam. The following figure shows a typical server group deployment scenario:

Figure 12.
Segmented LAN Deployment

In a segmented LAN deployment, one STM appliance is installed in front of each network segment. VLAN traffic can pass through the STM and can be scanned by the STM. This type of deployment splits the network load and protects network segments from malware threats coming in through the gateway or originating from other segments. The following figure shows a typical segmented LAN deployment scenario:

![Segmented LAN Deployment Diagram](image)

**Figure 13.**

Understanding the Steps for Initial Connection

Generally, five steps are required to complete the basic and security configuration of your STM:

1. **Connect the STM physically to your network.** Connect the cables and restart your network according to the instructions in the installation guide. See the ProSecure™ Web/Email Security Threat Management Appliance STM150, STM300, or STM600 Installation Guide for complete steps. A PDF of the Installation Guide is on the NETGEAR ProSecure™ website at http://prosecure.netgear.com/resources/document-library.php.

2. **Log in to the STM.** After logging in, you are ready to set up and configure your STM. See Logging In to the STM on page 28.

3. **Use the Setup Wizard to configure basic connections and security.** During this phase, you connect the STM to your network. See Using the Setup Wizard to Perform the Initial Configuration on page 32.
4. **Verify the installation.** See *Verifying Correct Installation* on page 49.

5. **Register the STM.** See *Registering the STM with NETGEAR* on page 50.

Each of these tasks is described separately in this chapter.

## Qualified Web Browsers

To configure the STM, you need to use a Web browser such as Microsoft Internet Explorer 5.1 or later, Mozilla Firefox l.x or later, or Apple Safari 1.2 or later with JavaScript, cookies, and SSL enabled.

Although these Web browsers are qualified for use with the STM’s Web Management Interface, SSL VPN users should choose a browser that supports JavaScript, Java, cookies, SSL, and ActiveX to take advantage of the full suite of applications. Note that Java is required only for the SSL VPN portal, not for the Web Management Interface.

## Logging In to the STM

To connect to the STM, your computer needs to be configured to obtain an IP address automatically from the STM via DHCP. For instructions on how to configure your computer for DHCP, see the document that you can access from *Preparing Your Network* in Appendix C.

**To connect and log in to the STM:**

1. Start any of the qualified browsers, as explained in *Qualified Web Browsers* on this page.

2. Enter **https://192.168.1.201** in the address field.

   ![https://192.168.1.201](https://192.168.1.201)

   **Figure 14.**

   **Note:** The STM factory default IP address is 192.168.1.201. If you change the IP address, you need to use the IP address that you assigned to the STM to log in to the STM.

   The NETGEAR Configuration Manager Login screen displays in the browser (see the following figure, which shows the STM300).
3. In the User Name field, type admin. Use lowercase letters.
4. In the Password field, type password. Here, too, use lowercase letters.

**Note:** The STM user name and password are not the same as any user name or password you might use to log in to your Internet connection.

**Note:** The first time that you remotely connect to the STM with a browser via an SSL VPN connection, you might get a warning message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer 5.5 or later, simply click Yes to accept the certificate. Other browsers provide you with similar options to accept and install the SSL certificate. If you connect to the STM through the User Portal Login screen (see Figure 88 on page 156), you can import the STM’s root certificate by clicking the link at the bottom of the screen.
5. Click **Login**. The Web Management Interface displays, showing the Dashboard screen (see the following figure, which shows only the top part of the screen). For information about this screen, see *Understanding the Information on the Dashboard Screen* on page 184.

**Note:** During the initial setup, the Setup Wizard displays when you first log in; afterward the login takes you to the Dashboard screen.

![Dashboard screenshot](image)

**Figure 16.**

**Note:** After 5 minutes of inactivity (the default login time-out), you are automatically logged out.

### Understanding the Web Management Interface Menu Layout

The following figure shows the menu at the top of the STM300’s Web Management Interface. The Web Management Interface layouts of the STM150 and STM600 are identical to the STM300.
ProSecure Web/Email Security Threat Management (STM) Appliance

Chapter 2. Using the Setup Wizard to Provision the STM in Your Network

Figure 17.

The Web Management Interface menu consists of the following components:

- **1st Level: Main navigation menu links.** The main navigation menu in the orange bar across the top of the Web Management Interface provides access to all the configuration functions of the STM, and remains constant. When you select a main navigation menu link, the letters are displayed in white against an orange background.

- **2nd Level: Configuration menu links.** The configuration menu links in the gray bar (immediately below the main navigation menu bar) change according to the main navigation menu link that you select. When you select a configuration menu link, the letters are displayed in white against a gray background.

- **3rd Level: Submenu tabs.** Each configuration menu item has one or more submenu tabs that are listed below the gray menu bar. When you select a submenu tab, the text is displayed in white against a blue background.

The bottom of each screen provides action buttons. The nature of the screen determines which action buttons are shown. The following figure shows an example:

![Figure 18.](image)

Any of the following action buttons might be displayed on screen (this list might not be complete):

- **Apply.** Save and apply the configuration.
- **Reset.** Reset the configuration to default values.
- **Test.** Test the configuration before you decide whether or not to save and apply the configuration.
- **Auto Detect.** Enable the STM to detect the configuration automatically and suggest values for the configuration.
- **Next.** Go to the next screen (for wizards).
- **Back.** Go to the previous screen (for wizards).
- **Search.** Perform a search operation.
• **Cancel.** Cancel the operation.
• **Send Now.** Send a file or report.

When a screen includes a table, table buttons are displayed to let you configure the table entries. The nature of the screen determines which table buttons are shown. The following figure shows an example:

![Table Buttons](image)

**Figure 19.**

Any of the following table buttons might be displayed on screen:

• **Select All.** Select all entries in the table.
• **Delete.** Delete the selected entry or entries from the table.
• **Enable.** Enable the selected entry or entries in the table.
• **Disable.** Disable the selected entry or entries in the table.
• **Add.** Add an entry to the table.
• **Edit.** Edit the selected entry.
• **Up.** Move the selected entry up in the table.
• **Down.** Move the selected entry down in the table.

Almost all screens and sections of screens have an accompanying help screen. To open the help screen, click the question mark icon. ( )

### Using the Setup Wizard to Perform the Initial Configuration

The Setup Wizard facilitates the initial configuration of the STM by taking you through 11 screens, the last of which allows you to save the configuration.

**To start the Setup Wizard:**

1. Select **Global Settings > Network Settings** from the menu. The Network Settings submenu tabs display with the Network Settings screen in view.
2. From the Network Settings configuration menu, select **Setup Wizard.**

The following sections explain the 11 configuration screens of the Setup Wizard. On the 10th screen, you can save your configuration. The 11th screen is just an informational screen.

The tables in the following sections explain the buttons and fields of the Setup Wizard screens. Additional information about the settings in the Setup Wizard screens is provided in other chapters that explain manual configuration; each following section provides a specific link to a section in another chapter.
Setup Wizard Step 1 of 10: Introduction

The first Setup Wizard screen is just an introductory screen. Click **Next** to go to the following screen.

Setup Wizard Step 2 of 11: Networking Settings

Enter the settings as explained in the following table, and then click **Next** to go the following screen.

**Note:** After you have completed the steps in the Setup Wizard, you can make changes to the network settings by selecting **Global Settings > Network Settings**. For more information about these network settings, see **Configuring Network Settings** on page 52.
### Table 5. Setup Wizard Step 2: Network Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management Interface Settings</strong></td>
<td></td>
</tr>
<tr>
<td>System Name</td>
<td>The name for the STM for purposes of identification and management. The default name is the name of your model (STM150, STM300, or STM600).</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the STM through which you will access the Web Management Interface. The factory default IP address is 192.168.1.201. <strong>Note:</strong> If you change the IP address of the STM while being connected through the browser, you will be disconnected. You then need to open a new connection to the new IP address and log in again. For example, if you change the default IP address from 192.168.1.201 to 10.0.0.1, you need to enter <code>https://10.0.0.1</code> in your browser to reconnect to the Web Management Interface.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the IP subnet mask. The subnet mask specifies the network number portion of an IP address. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask.</td>
</tr>
<tr>
<td>Gateway Address</td>
<td>Enter the IP address of the gateway through which the STM is accessed.</td>
</tr>
<tr>
<td>Primary DNS</td>
<td>Specify the IP address for the primary DNS server.</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td>As an option, specify the IP address for the secondary DNS server.</td>
</tr>
<tr>
<td><strong>MTU Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Maximum Transmission Unit</td>
<td>The maximum transmission unit (MTU) is the largest physical packet size that a network can transmit. Packets that are larger than the MTU value are divided into smaller packets before they are sent, an action that prolongs the transmission process. For most Ethernet networks the MTU value is 1500 bytes, which is the default setting. <strong>Note:</strong> NETGEAR recommends synchronizing the STM’s MTU setting with that of your network to prevent delays in transmission.</td>
</tr>
</tbody>
</table>
Setup Wizard Step 3 of 11: Time Zone

![Figure 22](image)

Enter the settings as explained in the following table, and then click **Next** to go the following screen.

---

**Note:** After you have completed the steps in the Setup Wizard, you can make changes to the date and time by selecting **Administration > System Date & Time**. For more information about these settings, see **Configuring Date and Time Service** on page 74.

---

### Table 6. Setup Wizard Step 3: System Date and Time Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Date and Time</td>
<td>From the drop-down list, select an NTP server, or select to enter the time manually.</td>
</tr>
<tr>
<td><strong>Use Default NTP Servers</strong></td>
<td>The STM regularly updates its real-time clock (RTC), which it uses for scheduling, by contacting a default NETGEAR NTP server on the Internet. This is the default setting.</td>
</tr>
</tbody>
</table>
Use Custom NTP Servers

The STM regularly updates its RTC by contacting one of the two NTP servers (primary and backup), both of which you need to specify in the fields that become available when you select this option.

**Note:** If you select this option but leave either the Server 1 or Server 2 field blank, both fields are automatically set to the default NETGEAR NTP servers.

**Note:** A list of public NTP servers is available at [http://support.ntp.org/bin/view/Servers/WebHome](http://support.ntp.org/bin/view/Servers/WebHome).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
</table>
| Use Custom NTP Servers   | The STM regularly updates its RTC by contacting one of the two NTP servers (primary and backup), both of which you need to specify in the fields that become available when you select this option.  

**Note:** If you select this option but leave either the Server 1 or Server 2 field blank, both fields are automatically set to the default NETGEAR NTP servers.  

**Note:** A list of public NTP servers is available at [http://support.ntp.org/bin/view/Servers/WebHome](http://support.ntp.org/bin/view/Servers/WebHome). |
| Server 1 Name / IP Address | Enter the IP address or host name of the primary NTP server. |
| Server 2 Name / IP Address | Enter the IP address or host name of the secondary NTP server. |
| Manually Enter the Date and Time | Date | Enter the date in the yyyy-mm-dd (year-month-date) format. |
| Manually Enter the Date and Time | Time | Enter the time in the hh-mm-ss (hour-minutes-seconds) format. |

**Time Zone**

From the drop-down list, select the local time zone in which the STM operates. The correct time zone is required in order for scheduling to work correctly. You do not need to configure daylight savings time, which is applied automatically when applicable. Greenwich Mean Time (GMT) is the default setting.

**Note:** When you select a time zone that is not associated with a location, such as (GMT -08:00) GMT-8, daylight savings time is automatically disabled. When you select a time zone that is associated with a location, such as (GMT -08:00) Pacific Time (US & Canada), daylight savings time is automatically enabled.
Setup Wizard Step 4 of 11: Email Security

Enter the settings as explained in the following table, and then click Next to go the following screen.

**Note:** After you have completed the steps in the Setup Wizard, you can make changes to the email security settings by selecting Email Security > Policy or Email Security > Anti-Virus. The Email Anti-Virus screen also lets you specify notification settings and email alert settings. For more information about these settings, see Configuring Email Protection on page 87.

**Tip:** To enhance performance, you can disable scanning of any protocols that are seldom or never used. Be mindful of the difference between user- and server-generated traffic. For example, your mail server might not use IMAP, but some users might configure IMAP clients.
Table 7. Setup Wizard Step 4: Email Security Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Services to Scan</strong></td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>SMTP scanning is enabled by default on standard service port 25. To disable any of these services, clear the corresponding check box. You can change the standard service port or add another port in the corresponding Ports to Scan field.</td>
</tr>
<tr>
<td>POP3</td>
<td>POP3 scanning is enabled by default on standard service port 110.</td>
</tr>
<tr>
<td>IMAP</td>
<td>IMAP scanning is enabled by default on standard service port 143.</td>
</tr>
<tr>
<td><strong>Scan Action</strong></td>
<td></td>
</tr>
</tbody>
</table>
| SMTP | From the SMTP drop-down list, specify one of the following actions to be taken when an infected email is detected:  
  • Quarantine attachment. The email is not blocked, but the attachment is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry.  
  • Delete attachment. The email is not blocked, but the attachment is deleted, and a virus log entry or a spyware log entry is created.  
  • Block infected email. This is the default setting. The email is blocked, and a virus log entry or a spyware log entry is created.  
  • Quarantine infected email. The email is placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry.  
  • Log only. Only a virus log entry or a spyware log entry is created. The email is not blocked and the attachment is not deleted. |
| POP3 | From the POP3 drop-down list, specify one of the following actions to be taken when an infected email is detected:  
  • Quarantine attachment. The email is not blocked, but the attachment is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry.  
  • Delete attachment. This is the default setting. The email is not blocked, but the attachment is deleted, and a virus log entry or a spyware log entry is created.  
  • Log only. Only a virus log entry or a spyware log entry is created. The email is not blocked and the attachment is not deleted. |
| IMAP | From the IMAP drop-down list, specify one of the following actions to be taken when an infected email is detected:  
  • Quarantine attachment. The email is not blocked, but the attachment is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry.  
  • Delete attachment. This is the default setting. The email is not blocked, but the attachment is deleted, and a virus log entry or a spyware log entry is created.  
  • Log only. Only a virus log entry or a spyware log entry is created. The email is not blocked and the attachment is not deleted. |
Table 7. Setup Wizard Step 4: Email Security Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Exceptions</strong></td>
<td></td>
</tr>
<tr>
<td>From the drop-down list, specify one of the following actions to be taken when an email attachment exceeds the size that you specify in the file size field:</td>
<td></td>
</tr>
<tr>
<td>• <strong>Skip</strong>. The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Block</strong>. The file is blocked and does not reach the end user.</td>
<td></td>
</tr>
<tr>
<td>The default and maximum file sizes are as follows:</td>
<td></td>
</tr>
<tr>
<td>• For the STM600, the default setting is to block any attachment larger than 10240 KB. The maximum file size that you can specify is 51200 KB.</td>
<td></td>
</tr>
<tr>
<td>• For the STM300, the default setting is to block any attachment larger than 10240 KB. The maximum file size that you can specify is 25600 KB.</td>
<td></td>
</tr>
<tr>
<td>• For the STM150, the default setting is to block any attachment larger than 8192 KB. The maximum file size that you can specify is 25600 KB.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong>: Setting the maximum file size to a high value might affect the STM's performance. NETGEAR recommends the default value, which is sufficient to detect the vast majority of threats.</td>
<td></td>
</tr>
</tbody>
</table>

Setup Wizard Step 5 of 11: Web Security

![Step 5 of 11: Web Security](image)

Figure 24.

Enter the settings as explained in the following table, and then click **Next** to go the following screen.
Note: After you have completed the steps in the Setup Wizard, you can make changes to the Web security settings by selecting **Web Security > Policy** or **Web Security > HTTP/HTTPS > Malware Scan**. The Malware Scan screen also lets you specify HTML scanning and notification settings. For more information about these settings, see *Configuring Web and Services Protection* on page 105.

Table 8. Setup Wizard Step 5: Web Security Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Services to Scan</strong></td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>HTTP scanning is enabled by default on standard service port 80.</td>
</tr>
<tr>
<td></td>
<td>To disable Hypertext Transfer Protocol (HTTP) scanning, clear the corresponding check box. You can change the standard service port or add another port in the corresponding Ports to Scan field.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>HTTPS scanning is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>To enable Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) scanning, select the corresponding check box. You can change the standard service port (number 443) or add another port in the corresponding Ports to Scan field.</td>
</tr>
<tr>
<td>FTP</td>
<td>FTP scanning is enabled by default on standard service port 21.</td>
</tr>
<tr>
<td></td>
<td>To disable File Transfer Protocol (FTP) scanning, clear the corresponding check box. You can change the standard service port or add another port in the corresponding Ports to Scan field.</td>
</tr>
<tr>
<td><strong>Scan Action</strong></td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>From the HTTP drop-down list, specify one of the following actions to be taken when an infected Web file or object is detected:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Quarantine file</strong>. The Web file or object is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or spyware log entry.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Delete file</strong>. This is the default setting. The Web file or object is deleted, and a virus log entry or spyware log entry is created.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Log only</strong>. Only a virus log entry or spyware log entry is created. The Web file or object is not deleted.</td>
</tr>
<tr>
<td></td>
<td>Select the <strong>Streaming</strong> check box to enable streaming of partially downloaded and scanned HTTP file parts to the end user. This method allows the user to experience more transparent Web downloading. Streaming is enabled by default.</td>
</tr>
</tbody>
</table>
Table 8. Setup Wizard Step 5: Web Security Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
</table>
| HTTPS   | From the HTTPS drop-down list, specify one of the following actions to be taken when an infected Web file or object is detected:  
  • **Quarantine file.** The Web file or object is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or spyware log entry.  
  • **Delete file.** This is the default setting. The Web file or object is deleted, and a virus log entry or spyware log entry is created.  
  • **Log only.** Only a virus log entry or spyware log entry is created. The Web file or object is not deleted.  
  Select the **Streaming** check box to enable streaming of partially downloaded and scanned HTTPS file parts to the end user. This method allows the user to experience more transparent Web downloading. Streaming is enabled by default. |
| FTP     | From the FTP drop-down list, specify one of the following actions to be taken when an infected Web file or object is detected:  
  • **Quarantine file.** The Web file or object is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or spyware log entry.  
  • **Delete file.** This is the default setting. The Web file or object is deleted, and a virus log entry or spyware log entry is created.  
  • **Log only.** Only a virus log entry or spyware log entry is created. The Web file or object is not deleted. |
| Scan Exceptions | From the drop-down list, specify one of the following actions to be taken when a Web file or object exceeds the size that you specify in the file size field:  
  • **Skip.** The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting.  
  • **Block.** The file is blocked and does not reach the end user.  
  The default and maximum file sizes are as follows:  
  • For the STM600 and STM300, the default setting is to block any attachment larger than 10240 KB. The maximum file size that you can specify is 51200 KB.  
  • For the STM150, the default setting is to block any attachment larger than 8192 KB. The maximum file size that you can specify is 25600 KB.  
  **Note:** Setting the maximum file size to a high value might affect the STM’s performance. NETGEAR recommends the default value, which is sufficient to detect the vast majority of threats. |
Setup Wizard Step 6 of 11: Email Notification Server Settings

![Image of the Email Notification Server step in the Setup Wizard]

Figure 25.

Enter the settings as explained in the following table, and then click **Next** to go to the following screen.

**Note:** After you have completed the steps in the Setup Wizard, you can make changes to the administrator email notification settings by selecting **Global Settings > Email Notification Server**. For more information about these settings, see *Configuring the Email Notification Server* on page 176.

Table 9. Setup Wizard Step 6: Email Notification Server Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email Notification Server Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Show as Mail Sender</td>
<td>A descriptive name of the sender for email identification purposes. For example, enter <a href="mailto:stm600notification@netgear.com">stm600notification@netgear.com</a>.</td>
</tr>
<tr>
<td>Send Notifications to</td>
<td>The email address to which the notifications should be sent. Typically, this is the email address of a user with administrative privileges.</td>
</tr>
<tr>
<td>SMTP Server</td>
<td>The IP address and port number or Internet name and port number of your ISP’s outgoing email SMTP server. The default port number is 25.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you leave this field blank, the STM cannot send email notifications.</td>
</tr>
<tr>
<td>Mail Server Requires Authentication</td>
<td>If the SMTP server requires authentication, select the <strong>Mail Server Requires Authentication</strong> check box and enter the following settings:</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name for SMTP server authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for SMTP server authentication.</td>
</tr>
</tbody>
</table>
Setup Wizard Step 7 of 11: Update Settings

Figure 26.

Enter the settings as explained in the following table, and then click Next to go the following screen.

Note: After you have completed the steps in the Setup Wizard, you can make changes to the security subscription update settings by selecting Administration > Software Update. For more information about these settings, see Updating the Software on page 71.
Table 10. Setup Wizard Step 7: Update Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Information</strong></td>
<td>You cannot configure this section; it is shown for information only. For the software, scan engine, (signature) pattern file, and operating system (OS), the current version and the date of the last update are displayed. Click + More to display the versions and most recent downloads for the antispam engine, applications engine, applications pattern file, stream engine, stream pattern file, mini engine, mini pattern file, policyd, scand, urld, update client, and rescue software.</td>
</tr>
<tr>
<td><strong>Update Settings</strong></td>
<td>Select one of the following radio buttons:</td>
</tr>
<tr>
<td>Update From</td>
<td>• Default Update Server. The scan engine and signatures are updated from the NETGEAR default update server.</td>
</tr>
<tr>
<td></td>
<td>• Another Update Server. The scan engine and signatures are updated from a server that you specify by entering the server IP address or host name in the Server Address field.</td>
</tr>
<tr>
<td>Server Address</td>
<td>The update server IP address or host name.</td>
</tr>
<tr>
<td>Update Component</td>
<td>Make one of the following selections from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• Update Signature Patterns only. Only the (signature) pattern file is updated. The software, scan engine, and OS are not updated.</td>
</tr>
<tr>
<td></td>
<td>• Update all Software and Signature Patterns. The software, scan engine, (signature) pattern file, and OS are updated. This is the default setting.</td>
</tr>
<tr>
<td>Update Frequency</td>
<td>Make one of the following selections:</td>
</tr>
<tr>
<td></td>
<td>• Weekly. From the drop-down lists, specify the day, hour, and minutes that the update should occur.</td>
</tr>
<tr>
<td></td>
<td>• Daily. From the drop-down lists, specify the hour and minutes that the update should occur.</td>
</tr>
<tr>
<td></td>
<td>• Every. From the drop-down list, specify the frequency with which the update should occur.</td>
</tr>
</tbody>
</table>
Setup Wizard Step 8 of 11: HTTP Proxy Settings

Figure 27.

Enter the settings as explained in the following table, and then click Next to go the following screen.

Note: After you have completed the steps in the Setup Wizard, you can make changes to the security subscription update settings by selecting Global Settings > HTTP Proxy. For more information about these settings, see Configuring the HTTP Proxy Settings on page 60.

Table 11. Setup Wizard Step 8: HTTP Proxy Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS Proxy Settings</td>
<td>If computers on the network connect to the Internet via a proxy server, select the Use a Proxy Server to Connect to the Internet check box to specify and enable a proxy server. Enter the following settings:</td>
</tr>
<tr>
<td>Use a Proxy Server to Connect to the Internet</td>
<td>Proxy Server: The IP address and port number of the proxy server.</td>
</tr>
<tr>
<td></td>
<td>User Name: The user name for proxy server authentication.</td>
</tr>
<tr>
<td></td>
<td>Password: The password for proxy server authentication.</td>
</tr>
</tbody>
</table>
Setup Wizard Step 9 of 11: Web Categories

Figure 28.

Enter the settings as explained in the following table, and then click **Next** to go the following screen.
Note: After you have completed the steps in the Setup Wizard, you can make changes to the content filtering settings by selecting **Web Security > HTTP/HTTPS > Content Filtering**. The Content Filtering screen lets you specify additional filtering tasks and notification settings. For more information about these settings, see *Configuring Web Content Filtering* on page 109.

Table 12. Setup Wizard Step 9: Web Categories Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the Web Categories You Wish to Block</td>
<td></td>
</tr>
</tbody>
</table>

Select the **Enable Blocking** check box to enable blocking of Web categories, which is the default setting. Select the check boxes of any Web categories that you want to block. Use the action buttons in the following way:

- **Allow All.** All Web categories are allowed.
- **Block All.** All Web categories are blocked.
- **Set to Defaults.** Blocking and allowing of Web categories are returned to their default settings. See *Table 24* on page 85 for information about the Web categories that are blocked by default. Categories that are preceded by a green rectangle are allowed by default; categories that are preceded by a pink rectangle are blocked by default.
Setup Wizard Step 10 of 11: Configuration Summary

![Configuration Summary Screen](image)

- **Network Settings**
  - System Name: STM001
  - IP Address: 192.168.1.100
  - Subnet Mask: 255.255.255.0
  - Gateway (IP Address): 192.168.1.254
  - Primary DNS: 192.168.1.254
  - Secondary DNS: 4.2.2.2
  - Maximum Transmission Unit: 1500

- **System Date and Time**
  - Use NTP Server: time.g-netgear.com
  - Time Zone: GMT, Greenwich Mean Time

- **SMTP Security**
  - Status: Enable
  - Service: SMTP
  - Ports to Scan: 25
  - Action: Block infected email

- **Web Security**
  - Status: Enable
  - Service: HTTP
  - Ports to Scan: 80
  - Action: Block (streaming)

- **Email Notification Server**
  - Email Server: smtp.g-netgear.com
  - SMTP Server: 223.456.789.0
  - Mail Recipients: admin@yourdomain.com

- **Update Settings**
  - Update Server Address: update.g-netgear.com
  - Update Component: Software and pattern
  - Frequency: 1d

- **HTTP Proxy Settings**
  - HTTP Proxy: Enable
  - Proxy Server: 

- **Blocked Website Categories**
  - Alcohol, Tobacco, Gambling
  - Adult Images, Gambling Activities
  - Music, Video, Movies, Games
  - Sports, Travel, Weather
  - News, Politics, Sports

Click **Apply** to save your settings and automatically restart the system, or click **Back** to make changes to the configuration.
Setup Wizard Step 11 of 11:Restarting the System

![Wizard screen 11](image)

Wizard screen 11 is just an informational screen to let you know that the system restarts automatically with the new configuration.

**Verifying Correct Installation**

Test the STM before deploying it in a live production environment. The following instructions walk you through a couple of quick tests designed to ensure that your STM is functioning correctly.

**Testing Connectivity**

Verify that network traffic can pass through the STM:

- Test an Internet URL (see *Testing a URL* on page 217).
- Ping the IP address of a device on either side of the STM.

**Testing HTTP Scanning**

If client computers have direct access to the Internet through your LAN, try to download the eicar.com test file from [http://www.eicar.org/download/eicar.com](http://www.eicar.org/download/eicar.com).

The eicar.com test file is a legitimate DoS program and is safe to use because it is not a malware threat and does not include any fragments of malware code. The test file is provided by EICAR, an organization that unites efforts against computer crime, fraud, and misuse of computers or networks.

Verify that the STM correctly scans HTTP traffic:

1. Log in to the STM Web Management Interface, and then verify that HTTP scanning is enabled. For information about how to enable HTTP scanning, see *Customizing Web Protocol Scan Settings* on page 105.
2. Check the downloaded eicar.com test file, and note the attached malware information file.
Registering the STM with NETGEAR

To receive threat management component updates and technical support, you need to register your STM with NETGEAR. The support registration keys are provided with the product package (see Service Registration Card with License Keys on page 12).

The STM supports a bundle key, which is a single support registration key that provides all three licenses: Web protection, Email protection, and Support & Maintenance.

**Note:** Activating the service licenses initiates their terms of use. Activate the licenses only when you are ready to start using this unit. If your unit has never been registered before, you can use the 30-day trial period for all three types of licenses to perform the initial testing and configuration. To use the trial period, do not click **Register** in step 5 of the following procedure but click **Trial** instead.

**To activate the service licenses:**

1. Ensure that your STM is connected to the Internet.
2. Select **Support > Registration** from the menu. The Registration screen displays:

![Registration Screen](image)

**Figure 31.**
3. In the Registration Key field, enter the license key.
4. Fill out the customer and VAR fields.
5. Click **Register**.
6. Repeat **step 3** and **step 5** for additional license keys.

The STM activates the licenses and registers the unit with the NETGEAR registration server.

---

**Note:** If you reset the STM to the original factory default settings after you have entered the license keys to activate the STM (see **Registering the STM with NETGEAR** on page 50), the license keys are erased. The license keys and the different types of licenses that are available for the STM are no longer displayed on the Registration screen. However, after you have reconfigured the STM to connect to the Internet and to the NETGEAR registration server, the STM retrieves and restores all registration information based on its MAC address and hardware serial number. You do not need to reenter the license keys or reactivate the STM.

---

**What to Do Next**

You have completed setting up and deploying the STM to the network. The STM is now set up to scan the protocols and services that you specified for malware threats and to perform updates based on the configured update source and frequency.

If you need to change the settings, or to view reports or logs, log in to the STM Web Management Interface, using the default IP address or the IP address that you assigned to the STM in **Setup Wizard Step 1 of 10: Introduction** on page 33.

The STM is ready for use. However, the following sections describe some important tasks that you might want to address before you deploy the STM in your network:

- **Changing Administrative Passwords and Timeouts** on page 62
- **Managing Digital Certificates** on page 76
- **Configuring Groups** on page 148
- **Configuring User Accounts** on page 152
- **Configuring Authentication** on page 154
- **Setting Scanning Exclusions and Web Access Exceptions** on page 130
This chapter describes the network settings, the system management features, and ways to improve the performance of the STM. If you have used the Setup Wizard, you have already configured some of these settings, but there are situations in which you might want to modify them. This chapter contains the following sections:

- Configuring Network Settings on this page
- Configuring Session Limits and Timeouts on page 56
- Configuring the Network Refresh and Permanent MAC Address Bindings on page 57
- Configuring the HTTP Proxy Settings on page 60
- About Users with Administrative and Guest Privileges on page 61
- Configuring Remote Management Access on page 64
- Using an SNMP Manager on page 65
- Managing the Configuration File on page 67
- Updating the Software on page 71
- Configuring Date and Time Service on page 74
- Managing Digital Certificates on page 76
- Managing the Quarantine Settings on page 81
- Managing the STM’s Performance on page 82

### Configuring Network Settings

If you have used the Setup Wizard, you might already have configured the Web Management Interface and maximum transmission unit (MTU) settings; the Network Settings screen allows you to modify these settings and to specify the interface speed and duplex settings.

The STM requires a valid IP address to retrieve online updates and to enable access to its Web Management Interface. If you have used the Setup Wizard to configure the STM, you have already specified the management interface name and address settings and the size of the MTU. In addition to modifying these settings, the Network Settings screen also allows you to specify the interface speed and duplex settings for the management interface, for the
STM600 or STM300 uplink and downlink interfaces, or for the STM150’s WAN and LAN interfaces.

To configure the STM’s network settings:

1. Select Global Settings > Network Settings from the menu. The Network Settings submenu tabs display with the Network Settings screen in view. (The following figure shows the STM600.)

![STM600 Network Settings](image1)

The following figure shows the Interface Speed & Duplex Settings section of the Network Settings screen of the STM300:

![STM300 Interface Speed & Duplex Settings](image2)
The following figure shows the Interface Speed & Duplex Settings section of the Network Settings screen of the STM150:

![Interface Speed & Duplex Settings](image)

**Figure 34. STM150**

2. Complete the fields and make your selections from the drop-down lists as explained in the following table:

**Table 13. Network Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management Interface Settings</strong></td>
<td></td>
</tr>
<tr>
<td>System Name</td>
<td>The name for the STM for purposes of identification and management. The default name is the name of your model (STM150, STM300, or STM600).</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the STM through which you will access the Web Management Interface. The factory default IP address is 192.168.1.201.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If you change the IP address of the STM while being connected through the browser, you will be disconnected. You then need to open a new connection to the new IP address and log in again. For example, if you change the default IP address from 192.168.1.201 to 10.0.0.1, you need to enter <a href="https://10.0.0.1">https://10.0.0.1</a> in your browser to reconnect to the Web Management Interface.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the IP subnet mask. The subnet mask specifies the network number portion of an IP address. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask.</td>
</tr>
<tr>
<td>Gateway Address</td>
<td>Enter the IP address of the gateway through which the STM is accessed.</td>
</tr>
<tr>
<td>Primary DNS</td>
<td>Specify the IP address for the primary DNS server IP address.</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td>As an option, specify the IP address for the secondary DNS server IP address.</td>
</tr>
<tr>
<td><strong>Interface Speed &amp; Duplex Settings</strong></td>
<td></td>
</tr>
<tr>
<td>These sections show the MAC address and assigned speed and duplex setting for each active interface. The Set Speed/Duplex drop-down list allows you to select the speed and duplex setting for each active interface. To set the speed to 1000baseT duplex (“full”), select <strong>auto</strong> to let the STM sense the speed automatically.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>MGMT stands for management interface.</td>
</tr>
</tbody>
</table>
### Table 13. Network Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>STM600</td>
<td>From the Set Speed/Duplex drop-down list, make one of the following selections:</td>
</tr>
<tr>
<td></td>
<td>• <strong>auto</strong>. Speed autosensing. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• <strong>10baseT/Half</strong>. Ethernet speed at half duplex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>10baseT/Full</strong>. Ethernet speed at full duplex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>100baseT/Half</strong>. Fast Ethernet speed at half duplex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>100baseT/Full</strong>. Fast Ethernet speed at full duplex.</td>
</tr>
<tr>
<td>STM300</td>
<td>From the Set Speed/Duplex drop-down list, make one of the following selections:</td>
</tr>
<tr>
<td></td>
<td>• <strong>auto</strong>. Speed autosensing. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• <strong>10baseT/Half</strong>. Ethernet speed at half duplex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>10baseT/Full</strong>. Ethernet speed at full duplex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>100baseT/Half</strong>. Fast Ethernet speed at half duplex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>100baseT/Full</strong>. Fast Ethernet speed at full duplex.</td>
</tr>
<tr>
<td>STM150</td>
<td>From the Set Speed/Duplex drop-down list, make one of the following selections:</td>
</tr>
<tr>
<td></td>
<td>• <strong>auto</strong>. Speed autosensing. This is the default setting, which can sense 1000BaseT speed at full duplex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>10baseT/Half</strong>. Ethernet speed at half duplex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>10baseT/Full</strong>. Ethernet speed at full duplex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>100baseT/Half</strong>. Fast Ethernet speed at half duplex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>100baseT/Full</strong>. Fast Ethernet speed at full duplex.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> All LAN interfaces share the same MAC address, speed, and duplex mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The STM150 does not provide a dedicated management interface.</td>
</tr>
<tr>
<td>MTU Settings</td>
<td>The maximum transmission unit (MTU) is the largest physical packet size that a network can transmit. Packets that are larger than the MTU value are divided into smaller packets before they are sent, an action that prolongs the transmission process. For most Ethernet networks the MTU value is 1500 bytes, which is the default setting.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> NETGEAR recommends synchronizing the STM’s MTU setting with that of your network to prevent delays in transmission.</td>
</tr>
</tbody>
</table>

3. Click **Apply** to save your settings. (If you click **Reset**, the STM restarts to restore the default network settings.) Changing the network settings has the following consequences:

- Changing any of the settings in the Management Interface Settings section of the screen causes the STM to restart.
- Changing any of the settings in the Interface Speed & Duplex Settings section of the screen causes the network to restart.
- Changing the MTU setting causes services such as HTTP and SMTP to restart.
Configuring Session Limits and Timeouts

The Session Limits screen allows you to specify the total number of sessions per user (that is, per IP address or single source machine) that are allowed on the STM. Session limiting is disabled by default. When session limiting is enabled, you can specify the maximum number of sessions per user either as an absolute number or as a percentage of the STM’s total connection capacity per user, which is 10000 sessions. (You cannot change the total connection capacity per user.) If a user exceeds the number of allocated sessions, packets might be dropped.

Note: Some protocols such as FTP and RSTP create two sessions per connection.

To configure session limits and timeouts:

1. Select **Global Settings > Network Settings** from the menu. The Network Settings submenu tabs display with the Network Settings screen in view.
2. Click the **Session Limits** submenu tab. The Session Limits screen displays:

![Session Limits Screen](image)

Figure 35.
3. Select the radio buttons, make your selections from the drop-down list, and complete the fields as explained in the following table:

Table 14. Session Limits Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Limits</td>
<td>Do You Want to Enable per-user Session Limits?</td>
</tr>
<tr>
<td>Limit Type</td>
<td>From the Limit Type drop-down list, make one of the following selections:</td>
</tr>
<tr>
<td>Limit Value</td>
<td>Depending on the selection in the Limit Type field, this value is a percentage or an absolute number.</td>
</tr>
<tr>
<td>The Total Number of Packets Dropped</td>
<td></td>
</tr>
<tr>
<td>Session Timeouts</td>
<td>If a session goes without data flow longer than the configured values, the session is terminated.</td>
</tr>
<tr>
<td>TCP Timeout</td>
<td>The time in seconds after which a TCP session without data flow is terminated. The default time is 1200 seconds.</td>
</tr>
<tr>
<td>UDP Timeout</td>
<td>The time in seconds after which an UDP session without data flow is terminated. The default time is 180 seconds.</td>
</tr>
<tr>
<td>ICMP Timeout</td>
<td>The time in seconds after which an ICMP session without data flow is terminated. The default time is 8 seconds.</td>
</tr>
</tbody>
</table>

4. Click **Apply** to save your settings. Changing any settings in the Session Timeouts section of the screen requires the STM to restart. If you click **Reset**, the STM restarts to restore the default network settings.

**Configuring the Network Refresh and Permanent MAC Address Bindings**

The STM integrates smart virtual MAC address detection to automatically detect virtual MAC addresses and bind these to an interface. When the network topology changes, a virtual MAC address might no longer be bound to the original interface. If this situation occurs, the host to which the virtual MAC address is assigned is no longer able to communicate with others through the STM. Therefore, the network need to be refreshed to enable the STM to redetect the virtual MAC address on the correct interface.
To refresh the network and view the MAC Address Bindings table:

1. Select **Global Settings > Network Settings** from the menu. The Network Settings submenu tabs display with the Network Settings screen in view.

2. Click the **Network Refresh** submenu tab. The Network Refresh screen displays. (The following figure shows the STM150.)

![Network Refresh Screen](image-url)
3. Select the check boxes and radio buttons and make your selections from the drop-down list as explained in the following table:

**Table 15. Network Refresh Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatically Refresh the Network</strong></td>
<td></td>
</tr>
<tr>
<td>Periodically refresh the MAC address bindings</td>
<td>Select this check box to enable the periodic refresh of the dynamic MAC address bindings. Specify if the refresh occurs either weekly or daily.</td>
</tr>
<tr>
<td>Weekly</td>
<td>Select the <strong>Weekly</strong> radio button to enable a weekly refresh of the network, and then specify when the refresh needs to occur by selecting the day, hour, and minutes from the drop-down lists.</td>
</tr>
<tr>
<td>Daily</td>
<td>Select the <strong>Daily</strong> radio button to enable a daily refresh of the network, and then specify when the refresh needs to occur by selecting the hour and minutes from the drop-down lists.</td>
</tr>
</tbody>
</table>

Click **Apply** to schedule the automatic refresh of the network, or click **Reset** to return to the default settings.

**Manually Refresh the Network**

Click **Refresh** to immediately refresh the network.

*Note:* When you click **Refresh**, the network restarts.

*Note:* The Advanced Settings button is described in the following section.

**Managing Permanent MAC Address Bindings**

You can permanently bind a MAC address to an interface. Such a binding does not change when the network topology changes and does not need to be redetected by the STM.

**To create a permanent MAC binding:**

1. Select **Global Settings > Network Settings** from the menu. The Network Settings submenu tabs display with the Network Settings screen in view.
2. Click the **Network Refresh** submenu tab. The Network Refresh screen displays (see the previous figure, which shows the STM150). Locate the Manually Refresh the Network section.
3. Click the **Advanced Settings** button. The screen expands to display the MAC Address Bindings section.
4. Complete the fields and make your selections from the drop-down lists as explained in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Enter the MAC address that you want to bind permanently.</td>
</tr>
<tr>
<td>Port (STM150) or Interface</td>
<td>From the drop-down list, select the interface to which the MAC address needs</td>
</tr>
<tr>
<td>(STM300 and STM600)</td>
<td>to be bound.</td>
</tr>
<tr>
<td>Type</td>
<td>This field is automatically determined: it displays Permanent or Dynamic.</td>
</tr>
</tbody>
</table>

5. To add the newly configured MAC address binding to the MAC Address Bindings table, click the **Add** table button in the Action column.

The MAC Address Bindings table displays both the dynamic bindings that are automatically detected by the STM and the permanent bindings that you have created.

**Changing a Dynamic MAC Address Binding to a Permanent Binding**

**To change a dynamic binding to a permanent binding:**

1. Locate the dynamic MAC address binding that you want bind permanently, and select an interface from the Port drop-down list (STM150) or Interface drop-down list (STM300 and STM600).
2. Click the corresponding **Add** table button in the Action column.

**Activating, Editing, or Deleting a Permanent MAC Address Binding**

For each permanent binding in the MAC Address Bindings table, the Action column provides two table buttons:

- **Apply.** Activates the permanent MAC address binding.
- **Delete.** Deletes the permanent MAC address binding from the table.

**To assign another interface to a permanent MAC address binding:**

1. Locate the dynamic MAC address binding that you want to edit, and select another interface from the Port drop-down list (STM150) or Interface drop-down list (STM300 and STM600).
2. Click **Apply** to save your changes.

**Configuring the HTTP Proxy Settings**

If you have used the Setup Wizard, you might have already configured an HTTP proxy; the HTTP Proxy screen allows you to modify these settings. If the STM is installed behind an HTTP proxy, you might need to specify the HTTP proxy settings for the STM to connect to the...
Internet. The settings on the HTTP Proxy screen affect Web category filtering, distributed spam analysis, and software updates.

To configure the HTTP proxy:

1. Select Global Settings > HTTP Proxy from the menu. The HTTP Proxy screen displays:

   ![HTTP Proxy Screen](image)

2. Select the check box and complete the fields as explained in the following table:

   Table 17. HTTP Proxy Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS Proxy Settings</td>
<td></td>
</tr>
<tr>
<td>Use a Proxy Server to Connect to</td>
<td>If computers on the network connect to</td>
</tr>
<tr>
<td>the Internet</td>
<td>the Internet via a proxy server, select</td>
</tr>
<tr>
<td></td>
<td>the Use a Proxy Server to Connect to the</td>
</tr>
<tr>
<td></td>
<td>Internet check box to specify and enable</td>
</tr>
<tr>
<td></td>
<td>a proxy server. Enter the following</td>
</tr>
<tr>
<td></td>
<td>settings:</td>
</tr>
<tr>
<td></td>
<td>Proxy Server: The IP address and port</td>
</tr>
<tr>
<td></td>
<td>number of the proxy server.</td>
</tr>
<tr>
<td></td>
<td>User Name: The user name for proxy</td>
</tr>
<tr>
<td></td>
<td>server authentication.</td>
</tr>
<tr>
<td></td>
<td>Password: The password for proxy server</td>
</tr>
<tr>
<td></td>
<td>authentication.</td>
</tr>
</tbody>
</table>

3. Click Apply to save your settings.

About Users with Administrative and Guest Privileges

There are two predefined user types that can access the STM’s Web Management Interface:

- **Administrator.** A user who has full access and the capacity to change the STM configuration (that is, read/write access). The default user name for an administrator is admin, and the default password for an administrator is password.
• **Guest user.** A user who can only view the STM configuration (that is, read-only access). The default user name for a guest is guest, and the default password for a guest is guest.

NETGEAR recommends that you change these passwords to more secure passwords.

The login window that is presented to the administrator and guest user is the NETGEAR Configuration Manager Login screen (see Figure 87 on page 155).

**Changing Administrative Passwords and Timeouts**

In addition to changing the default password for the administrator and guest user, you can use the Set Password screen to change the account names, and modify the Web Management Interface timeout setting.

---

**Note:** The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both uppercase and lowercase), numbers, and symbols. The password can be up to 64 characters.

---

**To modify the administrator and guest accounts, and to modify the Web Management Interface timeout setting:**

1. Select **Administration > Set Password** from the menu. The Set Password screen displays:

![Figure 38](image-url)

---

**Figure 38.**
2. To modify the administrator or guest settings, select the check box and complete the fields as explained in the following table:

Table 18. Set Password Settings Screen: Administrator and Guest Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Selection</strong></td>
<td></td>
</tr>
<tr>
<td>Select one of the following radio buttons:</td>
<td></td>
</tr>
<tr>
<td>• <strong>Edit Administrator Settings</strong>. Allows you to modify the administrator settings, while the guest settings are masked out.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Edit Guest Settings</strong>. Allows you to modify the guest settings, while the administrator settings are masked out.</td>
<td></td>
</tr>
<tr>
<td><strong>Administrator Settings/Guest Setting</strong></td>
<td></td>
</tr>
<tr>
<td>New User Name</td>
<td>The default user name. For the administrator account, the default name is admin; for the guest account, the default name is guest.</td>
</tr>
<tr>
<td>Old Password</td>
<td>The current (factory default) password.</td>
</tr>
<tr>
<td>New Password</td>
<td>Enter the new password.</td>
</tr>
<tr>
<td>Retype New Password</td>
<td>Confirm the new password.</td>
</tr>
</tbody>
</table>

3. Under the Administrator Settings and Guest Settings sections of the screen, click **Apply** to save your settings.

4. If you modified the administrator settings and now want to modify the guest settings, or the other way around, repeat **step 2** and **step 3** for the other settings.

5. To modify the Web Management Interface timeout settings, complete the field as explained in the following table:

Table 19. Set Password Settings Screen: Web Interface Timeout Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web Interface Timeout</strong></td>
<td></td>
</tr>
<tr>
<td>Session Timeout</td>
<td>Enter the period in seconds after which the Web Management Interface is automatically logged off if no activity is detected. The default is 600 seconds. You can configure a session timeout from 30 seconds to 9999 seconds.</td>
</tr>
</tbody>
</table>

6. Under the Web Interface Timeout section of the screen, click **Apply** to save your settings.

**Note:** After a factory default reset, the password and timeout values are changed back to password and 600 seconds (5 minutes), respectively.
Configuring Remote Management Access

An administrator can configure, upgrade, and check the status of the STM over the Internet via a Secure Sockets Layer (SSL) VPN connection.

You need to use an SSL VPN connection to access the STM from the Internet: type **https://** (not http://) followed by the STM’s WAN IP address into your browser. For example, if the STM’s WAN IP address is 172.16.0.123, type the following in your browser: **https://172.16.0.123**.

The STM’s remote login URL is:

https://<IP_address> or https://<FullyQualifiedDomainName>

**Note:** The STM is accessible to anyone who knows its IP address and default password. Because a malicious WAN user can reconfigure the STM and misuse it in many ways, NETGEAR highly recommends that you change the admin and guest default passwords before continuing (see Changing Administrative Passwords and Timeouts on page 62).

To configure remote management:

1. Select **Administration > Remote Management** from the menu. The Remote Management screen displays:

   ![](image)

   **Figure 39.**
2. In the Secure HTTPS Management section of the screen, enter number of the port that you want to use to access Web Management Interface of the STM. The default setting is port 443, but you can enter a port ranging from 1024 to 65535. You cannot use some ports such as 2080 and 8088 that might be used by the STM.

This section of the screen also displays the HTTPS hyperlink through which you can access the Web Management Interface of the STM. The hyperlink consists of the IP address or fully qualified domain name (FQDN) for the STM and the port number that you have assigned.

3. In the Access Control List section of the screen, you can specify IP addresses or IP address ranges that you want to grant access to the Web Management Interface for increased security. To specify a range, separate the beginning IP address and the ending IP address by a hyphen (-). To allow access from all IP addresses and IP address ranges, leave this field blank.

4. Click **Apply** to save your changes.

---

**Note:** To maintain security, the STM rejects a login that uses http://address rather than the SSL https://address.

---

**Note:** The first time that you remotely connect to the STM with a browser via an SSL VPN connection, you might get a warning message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer 5.5 or later, simply click **Yes** to accept the certificate.

---

**Using an SNMP Manager**

Simple Network Management Protocol (SNMP) forms part of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

SNMP lets you monitor and manage your STM from an SNMP manager. It provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. The STM provides support for report aggregation through SNMP version 1 (SNMPv1) and version 2 (SNMPv2).
To enable SNMP and to configure the SNMP settings:

1. Select **Administration > SNMP** from the menu. The SNMP screen displays:

   ![SNMP Screen Screenshot](image)

   **Figure 40.**

2. Select the radio buttons and complete the fields as explained in the following table:

   **Table 20. SNMP Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SNMP Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Do You Want to Enable SNMP?</td>
<td>Select one of the following radio buttons:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Yes.</strong> Enable SNMP.</td>
</tr>
<tr>
<td></td>
<td>• <strong>No.</strong> Disable SNMP. This is the default setting.</td>
</tr>
<tr>
<td>Read Community</td>
<td>The community string to allow an SNMP manager access to the MIB objects of the STM for the purpose of reading only. The default setting is public.</td>
</tr>
<tr>
<td>Set Community</td>
<td>The community string to allow an SNMP manager access to the MIB objects of the STM for the purpose of reading and writing. The default setting is private.</td>
</tr>
</tbody>
</table>
ProSecure Web/Email Security Threat Management (STM) Appliance

Table 20. SNMP Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do You Want to Enable SNMP?</td>
<td>Contact</td>
</tr>
<tr>
<td>(continued)</td>
<td>The SNMP system contact information that is available to the SNMP manager. This setting is optional.</td>
</tr>
<tr>
<td>Location</td>
<td>Location</td>
</tr>
<tr>
<td></td>
<td>The physical location of the STM. This setting is optional.</td>
</tr>
</tbody>
</table>

**Trusted SNMP Hosts**

Enter the IP addresses of the computers and devices to which you want to grant read-only (GET) or write (SET) privileges on the STM. Separate IP addresses by a comma. To allow any trusted SNMP host access, leave the field blank, which is the default setting.

**SNMP Traps**

Enter the IP addresses of the SNMP management stations that are allowed to receive the STM’s SNMP traps. Separate IP addresses by a comma. If you leave the field blank, which is the default setting, no SNMP management station can receive the STM’s SNMP traps.

3. Click **Apply** to save your settings.

**Supported MIB Browsers**

After you have configured the SNMP settings, you need to enter the IP address of the STM in the Management Information Base (MIB) browsers through which you want to query or configure the STM. See the documentation of your MIB browser for instructions.

NETGEAR recommends the following MIB browsers for receiving the STM SNMP notifications:

- MG-Soft
- SNMP
- Net-SNMP (Linux Text)
- SNMP Browser for KDE

The STM MIB structure is automatically downloaded by management stations. You should start receiving notifications after you have enabled SNMP on the STM and added its IP address into your MIB browsers.

**Managing the Configuration File**

The configuration settings of the STM are stored in a configuration file on the STM. This file can be saved (backed up) to a PC, retrieved (restored) from the PC, or cleared to factory default settings.

Once the STM is installed and works correctly, make a backup of the configuration file to a computer. If necessary, you can later restore the STM settings from this file.
The Backup and Restore Settings screen lets you:

- Back up and save a copy of the current settings
- Restore saved settings from the backed-up file
- Revert to the factory default settings.

To display the Backup and Restore Settings screen, select Administration > Backup and Restore Settings from the menu:

```
Figure 41.
```

**Backing Up Settings**

The backup feature saves all STM settings to a file. These settings include:

- **Network settings.** IP address, subnet mask, gateway, and so on.
- **Scan settings.** Services to scan, primary and secondary actions, and so on.
- **Update settings.** Update source, update frequency, and so on.
- **Antispam settings.** Whitelist, blacklist, content filtering settings, and so on.

Back up your STM settings periodically, and store the backup file in a safe place.

**Tip:** You can use a backup file to export all settings to another STM that has the same language and management software versions. Remember to change the IP address of the second STM before deploying it to eliminate IP address conflicts on the network.
To back up settings:

1. On the Backup and Restore Settings screen (see the previous figure), next to Save a copy of current settings, click the **Backup** button to save a copy of your current settings. A dialog box displays, showing the file name of the backup file.

   **Note:** The backup file has the following format:
   
   `backup_$hostname_$productversion_$yyyymmdd.gpg`

   - `$hostname`: The host name of the STM that is configured on the Network Settings screen, for example, STM600.
   - `$productversion`: The software version of the STM, for example, 2.0.0-39.
   - `$yyyymmdd`: The time when the backup is performed, for example, 20100617.

   Using these examples, the backup file name would be `backup_STM600_2.0.0-39_20100617.gpg`.

2. Select **Save file**, and then click **OK**.
3. Open the folder where you have saved the backup file, and then verify that it has been saved successfully.

   **Note the following:**
   
   - If your browser is not configured to save downloaded files automatically, locate the folder in which you want to save the file, specify the file name, and save the file.
   - If you have your browser configured to save downloaded files automatically, the file is saved to your browser’s download location on the hard disk.

### Restoring Settings

**WARNING!**

Restore only settings that were backed up from the same software version. Restoring settings from a different software version can corrupt your backup file or the STM system software.
To restore settings from a backup file:

1. On the Backup and Restore Settings screen (see Figure 41 on page 68), next to Restore save settings from file, click Browse.
2. Locate and select the previously saved backup file.
3. When you have located the file, click the Restore button. A warning screen might appear, and you might have to confirm that you want to restore the configuration.

The STM restarts. During the reboot process, the Backup and Restore Settings screen remains visible. The reboot process is complete after several minutes when the Test LED on the front panel goes off.

**WARNING!**

Once you start restoring settings, do not interrupt the process. Do not try to go online, turn off the STM, shut down the computer, or do anything else to the STM until the settings have been fully restored.

Reverting to Factory Default Settings

To reset the STM to the original factory default settings, click the Default button next to Revert to factory default settings on the Backup and Restore Settings screen (see Figure 41 on page 68).

The STM restarts. The Backup and Restore Settings screen remains visible during the reboot process. The reboot process is complete after several minutes when the Test LED (STM150) or Status LED (STM300 and STM600) on the front panel goes off.

**WARNING!**

When you restore the factory default settings, the STM settings are erased. All content settings and scan settings are lost. Back up your settings if you intend on using them.

**Note:** After rebooting with factory default settings, the STM administrator account password is password, the guest account password is guest, and the LAN IP address is 192.168.1.201.
Note: For the STM150 only, there is an alternate way to return the settings to factory defaults: Using a sharp object, press and hold the Reset button on the rear panel of the STM150 (see Rear Panel STM150 on page 20) for about 10 seconds until the front panel Test LED flashes and the STM150 returns to factory default settings.

Updating the Software

If you have used the Setup Wizard, you might have already configured the software update settings; the Software Update screen allows you to modify these settings.

The STM has four main software components:

• The application software that includes the network protocols, security services, Web Management Interface, and other components.

• A scan engine that enables the STM to scan emails, attachments, Web files, and applications, and that functions in conjunction with the pattern file.

• A pattern file that contains the virus signature files and virus database.

• An operating system (OS) that includes the kernel modules and hardware drives.

The STM provides two methods for updating components:

• Scheduled, automatic update

• Manual update

Because new virus threats can appear any hour of the day, it is very important to keep both the pattern file and scan engine firmware as current as possible. The STM can automatically check for updates, as often as every 15 minutes, to ensure that your network protection is current.

Scheduling Updates

Enabling scheduled updates ensures that the STM automatically downloads the latest components from the NETGEAR update server.
To configure scheduled updates:

1. Select Administration > Software Update from the menu. The Software Update screen displays:

![Software Update Screen](image)

2. Select the radio buttons, complete the field, and make your selections from the drop-down lists as explained in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Information</strong></td>
<td>You cannot configure this section; it is shown for information only. For the software, scan engine, (signature) pattern file, and operating system (OS), the current version and the date of the last update are displayed. Click + More to display the versions and most recent downloads for the antispam engine, applications engine, applications pattern file, stream engine, stream pattern file, mini engine, mini pattern file, policyd, scand, urld, update client, and rescue software.</td>
</tr>
</tbody>
</table>
Table 21. Software Update Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Update From</td>
<td>Select one of the following radio buttons:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default Update Server.</strong> The scan engine and signatures are updated from the NETGEAR default update server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Another Update Server.</strong> The scan engine and signatures are updated from a server that you specify by entering the server IP address or host name in the Server Address field.</td>
</tr>
<tr>
<td>Server Address</td>
<td>The update server IP address or host name.</td>
</tr>
<tr>
<td>Update Component</td>
<td>Make one of the following selections from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Update Signature Patterns only.</strong> Only the (signature) pattern file is updated. The software, scan engine, and OS are not updated.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Update all Software and Signature Patterns.</strong> The software, scan engine, (signature) pattern file, and OS are updated. This is the default setting.</td>
</tr>
<tr>
<td><strong>Update Frequency</strong></td>
<td>Make one of the following selections:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Weekly.</strong> From the drop-down lists, specify the day, hour, and minutes that the update should occur.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Daily.</strong> From the drop-down lists, specify the hour and minutes that the update should occur.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Every.</strong> From the drop-down list, specify the frequency with which the update should occur.</td>
</tr>
</tbody>
</table>

3. Click **Apply** to save your settings.

**Performing a Manual Update**

If you want to immediately check for and download available updates, perform a manual update:

1. Select **Administration > Software Update** from the menu. The Software Update screen displays (see the previous figure).
2. At the bottom of the screen, click **Update Now**. The STM contacts the update server and checks for available updates. If updates are available, the Update Progress screen displays to show the progress of the update:

![Update Progress](image-url)

Figure 43.
3. After the update has finished, click **Apply** to activate the newly updated software.

**Critical Updates That Require a Restart**

If a downloaded update requires a restart, you are prompted to perform the update when you log in to the STM. The following figure shows an example of a Critical Update screen, which provides information about the update and allows you to install it immediately or at a later time. To install the update immediately, click **Install Now**. To install the update at a later time, click **Later**.

![Critical Update Screen](image)

**Figure 44.**

**Configuring Date and Time Service**

If you have used the Setup Wizard, you might have already configured the system date and time settings; the System Date and Time screen allows you to modify these settings.

Configure date, time, and NTP server designations on the System Date and Time screen. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers. Setting the correct system time and time zone ensures that the date and time recorded in the STM logs and reports are accurate. Changing the time zone requires the STM to restart to apply the updated settings.
To set time, date, and NTP servers:

1. Select **Administration > System Date and Time** from the menu. The System Date and Time screen displays:

![System Date and Time screen](image)

The top of the screen displays the current weekday, date, time, time zone, and year (in the example in the previous figure: Current Time: 2009-08-02 00:19:30).

2. Select the radio buttons, complete the fields, and make your selections from the drop-down list as explained in the following table:

**Table 22. System Date and Time Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Date and Time</td>
<td>From the drop-down list, select an NTP server, or select to enter the time manually.</td>
</tr>
<tr>
<td>Use Default NTP Servers</td>
<td>The STM regularly updates its real-time clock (RTC), which it uses for scheduling, by contacting a default NETGEAR NTP server on the Internet. This is the default setting.</td>
</tr>
</tbody>
</table>
3. Click **Apply** to save your settings. Changing the time zone requires the STM to restart.

---

**Note:** If you select the default NTP servers or if you enter a custom server FQDN, the STM determines the IP address of the NTP server by performing a DNS lookup. You need to configure a DNS server address on the Network Settings screen (see Configuring Network Settings on page 52) before the STM can perform this lookup.

---

### Managing Digital Certificates

The STM uses digital certificates (also known as X509 certificates) for secure Web access connections over HTTPS (that is, SSL VPN connections).

Digital certificates can be either self-signed or can be issued by Certification Authorities (CAs) such as an internal Windows server or an external organizations such as Verisign or Thawte. On the STM, the uploaded digital certificate is checked for validity and purpose. The digital certificate is accepted when it passes the validity test and the purpose matches its use.
The STM uses digital certificates to authenticate connecting HTTPS servers, and to allow HTTPS clients to be authenticated by remote entities. A digital certificate that authenticates a server, for example, is a file that contains the following elements:

- A public encryption key to be used by clients for encrypting messages to the server.
- Information identifying the operator of the server.
- A digital signature confirming the identity of the operator of the server. Ideally, the signature is from a trusted third party whose identity can be verified.

When a security alert is generated, the user can decide whether or not to trust the host.

![Security Alert]

**Figure 46.**

You can obtain a digital certificate from a well-known commercial Certificate Authority (CA) such as Verisign or Thawte. Because a commercial CA takes steps to verify the identity of an applicant, a digital certificate from a commercial CA provides a strong assurance of the server's identity.

The STM contains a self-signed digital certificate from NETGEAR. This certificate can be downloaded from the STM login screen or from the Certificate Management screen for browser import. However, NETGEAR recommends that you replace this digital certificate with a digital certificate from a well-known commercial CA prior to deploying the STM in your network.

The STM's Certificate Management screen lets you to view the currently loaded digital certificate for HTTPS scans, upload a new digital certificate, manage the trusted CA authorities list, and manage the untrusted certificates list.

To display the Certificate Management screen, select **Web Security > Certificate Management** from the menu. Because of the size of this screen, and because of the way the information is presented, the Certificate Management screen is divided and presented in this manual in three figures (the following figure, **Figure 48** on page 79, and **Figure 49** on page 80).
Managing the Certificate for HTTPS Scans

To manage the STM’s active certificate that is used for HTTPS scans, select Web Security > Certificate Management from the menu. The Certificate Management screen displays. The following figure shows only the Certificate Used for HTTPS Scans section of the screen:

![Certificate Management Screen](image)

The top part of the Certificate Used for HTTPS Scans section displays information about the current certificate that is used for HTTPS scans.

**Note:** For information about the HTTPS scanning process, HTTPS Scan Settings on page 119.

**To download the current certificate into your browser:**

1. Click Download for browser import.
2. Follow the instructions of your browser to save the RootCA.crt file on your computer.

**To reload the default NETGEAR certificate:**

1. Select the Use NETGEAR default certificate radio button.
2. Click Apply to save your settings.
To import a new certificate:

1. Select the **Use imported certificate (PKCS12 format)** radio button.
2. Click **Browse** next to the Import from File field.
3. Navigate to a trusted certificate file on your computer. Follow the instructions of your browser to place the certificate file in the Import from File field.
4. If required, enter the appropriate password in the Certificate password field.
5. Click the **Upload** button.

---

**Note:** If the certificate file is not in the pkcs12 format, the upload fails. Importing a new certificate overwrites any previously imported certificates.

6. Click **Apply** to save your settings.

Managing Trusted Certificates

**To manage trusted certificates:**

Select **Web Security > Certificate Management** from the menu. The Certificate Management screen displays. The following figure shows only the Trusted Certificate Authorities section of the screen:

![Certificate Management, screen 2 of 3](image)

The Trusted Certificate Authorities table contains the trusted certificates from third-party websites that are signed by the Certificate Authorities.
To view details of a trusted certificate:

1. From the Trusted Certificate Authorities table, select the certificate.
2. Click View Details. A new screen opens that displays the details of the certificate.

To delete a trusted certificate:

1. From the Trusted Certificate Authorities table, select the certificate.
2. Click Delete Selected.

To import a trusted certificate:

1. Click Browse next to the Import from File field.
2. Navigate to a trusted certificate file on your computer. Follow the instructions of your browser to place the certificate file in the Import from File field.
3. Click the Upload button. The newly imported trusted certificate is added to the Trusted Certificate Authorities table.

Managing Untrusted Certificates

To manage untrusted certificates:

Select Web Security > Certificate Management from the menu. The Certificate Management screen displays. The following figure shows only the Untrusted Certificates section of the screen:

![Figure 49. Certificate Management, screen 3 of 3](image)

When the STM detects an untrusted or invalid certificate, it automatically places the certificate in the Untrusted Certificates table.

To view details of an untrusted certificate:

1. From the Untrusted Certificates table, select the certificate.
2. Click View Details. A new screen opens that displays the details of the certificate.
To delete an untrusted certificate:

1. From the Untrusted Certificates table, select the certificate.
2. Click Delete Selected.

To move an untrusted certificate to the Trusted Certificate Authorities table:

1. From the Untrusted Certificates table, select the certificate.
2. Click Add to Trusted List. The previously untrusted certificate is added to the Trusted Certificate Authorities table.

Managing the Quarantine Settings

You can specify how much memory the STM reserves for quarantined items, and how long these items remain in memory. In general, the default settings work well for most situations.

To change the quarantine settings:

1. Select Global Settings > Quarantine from the menu. The Quarantine screen displays:

![Quarantine Screen]

Figure 50.
2. Select the radio buttons, complete the field, and make your selections from the drop-down lists as explained in the following table:

**Table 23. Quarantine Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Quarantine Area Size</td>
<td>Specify the maximum amount of memory in MB that is allocated to malware quarantine. This limit is cumulative for all users. For the STM600, the default setting is 200 MB, and the maximum setting is 512 MB. For the STM150 and STM300, the default setting is 100 MB, and the maximum setting is 512 MB. <strong>Note:</strong> After the limit has been exceeded, old items are automatically purged from the malware quarantine to make space for new items.</td>
</tr>
<tr>
<td>Spam Quarantine Area Size</td>
<td>Specify the maximum amount of memory in MB that is allocated to spam quarantine. This limit is cumulative for all users. For the STM600, the default setting is 1024 MB, and the maximum setting is 2048 MB. For the STM150 and STM300, the default setting is 512 MB, and the maximum setting is 1024 MB. <strong>Note:</strong> After the limit has been exceeded, old items are automatically purged from the malware quarantine to make space for new items.</td>
</tr>
<tr>
<td>Quarantine Lifetime</td>
<td>Specify how long items remain in quarantine before being automatically purged. The default setting is 15 days. The maximum setting is 30 days.</td>
</tr>
</tbody>
</table>

3. Click **Apply** to save your settings.

**Note:** For information about how to view and manage the quarantine files, see **Viewing and Managing the Quarantine Files** on page 208.

**Managing the STM’s Performance**

Performance management consists of controlling the traffic through the STM so that the necessary traffic gets through when there is a bottleneck and either reducing unnecessary traffic or rescheduling some traffic to low-peak times to prevent bottlenecks from occurring in the first place.

If you want to reduce traffic by preventing unwanted emails from reaching their destinations or by preventing access to certain sites on the Internet, you can use the STM’s content filtering feature. By default, this feature is disabled; all requested traffic from any website is allowed with the exception of Web content categories that are mentioned in **Default Email and Web Scan Settings** on page 85.
You can adjust the following features of the STM in such a way that the traffic load on the WAN side decreases.

- **Email content filtering.** To reduce incoming email traffic, you can block emails with large attachments, reject emails based on keywords, file extensions, or file names, and set spam protection rules. There are several ways you can reduce unwanted email traffic:
  - Setting the size of email files to be scanned. Scanning large email files requires network resources and might slow down traffic. You can specify the maximum file or message size that is scanned, and whether files that exceed the maximum size are skipped (which might compromise security) or blocked. For more information, see Exception Settings on page 90.
  - Keyword, file extension, and file name blocking. You can reject emails based on keywords in the subject line, file type of the attachment, and file name of the attachment. For more information, see Email Content Filtering on page 94.
  - Protecting against spam. Set up spam protection to prevent spam from using up valuable bandwidth. For more information, see Protecting Against Email Spam on page 97.

- **Web content filtering.** The STM provides extensive methods to filter Web content in order to reduce traffic:
  - Web category blocking. You can block entire Web categories because their content is unwanted, offensive, or not relevant, or simply to reduce traffic. For more information, see Configuring Web Content Filtering on page 109.
  - File extension blocking. You can block files based on their extension. Such files can include executable files, audio and video files, and compressed files. For more information, see Configuring Web Content Filtering on page 109.
  - URL blocking. You can specify URLs that are blocked by the STM. For more information, see Configuring Web URL Filtering on page 116.
  - Web services blocking. You can block Web applications such as instant messaging, media, peer-to-peer, and tools. For more information, see Configuring Application Control on page 127.
  - Web object blocking. You can block the following Web component types: embedded objects (ActiveX, Java, Flash), proxies, and cookies; and you can disable Java scripts. For more information, see Configuring Web Content Filtering on page 109.
  - Setting the size of Web files to be scanned. Scanning large Web files requires network resources and might slow down traffic. You can specify the maximum file size that is scanned, and whether files that exceed the maximum size are skipped (which might compromise security) or blocked. For more information, see Configuring Web Malware Scans on page 107.

For these features (with the exception of Web object blocking and setting the size of files to be scanned), you can set schedules to specify when Web content is filtered (see Configuring Web Content Filtering on page 109) and configure scanning exclusions and access exceptions (see Setting Scanning Exclusions and Web Access Exceptions on page 130). You can use the STM’s monitoring functions to assist you with performance management (see Monitoring Real-Time Traffic, Security, Statistics, and Web Usage on page 184).
This chapter describes how to apply the content filtering features of the STM and how to optimize scans to protect your network. This chapter contains the following sections:

- About Content Filtering and Scans on this page
- Configuring Email Protection on page 87
- Configuring Web and Services Protection on page 105
- Configuring Application Control on page 127
- Setting Scanning Exclusions and Web Access Exceptions on page 130

### About Content Filtering and Scans

The STM provides very extensive Web content and email content filtering options, Web browsing activity reporting, email antivirus and antispam options, and instant alerts via email. You can establish restricted Web access policies that are based on the time of day, Web addresses, and Web address keywords. You can also block Internet access by applications and services, such as instant messaging and peer-to-peer file sharing clients.

**Note:** For information about how to monitor blocked content and malware threats in realtime, see *Monitoring Real-Time Traffic, Security, Statistics, and Web Usage* on page 184. For information about how to view blocked content and malware threats in the logs, see *Querying Logs* on page 194. For information about how to view quarantined content, see *Viewing and Managing the Quarantine Files* on page 208.
Default Email and Web Scan Settings

For most network environments, the default scan settings and actions that are shown in the following table work well, but you can adjust these to meet the needs of your specific environment.

Table 24. Default Email and Web Scan Settings

<table>
<thead>
<tr>
<th>Scan Type</th>
<th>Default Scan Setting</th>
<th>Default Action (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email Server Protocols</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>Enabled</td>
<td>Block infected email</td>
</tr>
<tr>
<td>POP3</td>
<td>Enabled</td>
<td>Delete attachment if infected</td>
</tr>
<tr>
<td>IMAP</td>
<td>Enabled</td>
<td>Delete attachment if infected</td>
</tr>
<tr>
<td><strong>Web Server Protocols</strong>a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>Enabled</td>
<td>Delete file if malware threat detected</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Disabled</td>
<td>No action (scan disabled)</td>
</tr>
<tr>
<td>FTP</td>
<td>Enabled</td>
<td>Delete file if malware threat detected</td>
</tr>
<tr>
<td><strong>Instant Messaging Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Talk</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>ICQ</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>miRC</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>MSN Messenger</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>QQ</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Yahoo Messenger</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td><strong>Media Applications</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iTunes (music store, update)</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Quicktime (update)</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Real Player (guide)</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Rhapsody (guide, music store)</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Winamp (Internet radio/TV)</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td><strong>Peer-to-Peer (P2P) Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BitTorrent</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>eDonkey</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Gnutella</td>
<td>Allowed</td>
<td></td>
</tr>
</tbody>
</table>
### Table 24. Default Email and Web Scan Settings (Continued)

<table>
<thead>
<tr>
<th>Scan Type</th>
<th>Default Scan Setting</th>
<th>Default Action (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tools</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alexa Toolbar</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>GoToMyPC</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Weatherbug</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Yahoo Toolbar</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td><strong>Web Objects</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Embedded Objects (ActiveX/Java/Flash)</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Javascript</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Proxy</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Cookies</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td><strong>Web Content Categories</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commerce</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Drugs and Violence</td>
<td>Blocked</td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td>Allowed with the exception of School Cheating</td>
<td></td>
</tr>
<tr>
<td>Gaming</td>
<td>Blocked</td>
<td></td>
</tr>
<tr>
<td>Inactive Sites</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Internet Communication and Search</td>
<td>Allowed with the exception of Anonymizers</td>
<td></td>
</tr>
<tr>
<td>Leisure and News</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Malicious</td>
<td>Blocked</td>
<td></td>
</tr>
<tr>
<td>Politics and Religion</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Sexual Content</td>
<td>Blocked</td>
<td></td>
</tr>
<tr>
<td>Technology</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td>Uncategorized</td>
<td>Allowed</td>
<td></td>
</tr>
</tbody>
</table>

*a. For the STM300 and STM600, files and messages that are larger than 10240 KB are skipped by default. For the STM150, files and messages that are larger than 8192 KB are skipped by default.*
Configuring Email Protection

The STM lets you configure the following settings to protect the network’s email communication:

- The email protocols that are scanned for malware threats
- Actions that are taken when infected emails are detected
- The maximum file sizes that are scanned
- Keywords, file types, and file names in emails that are filtered to block objectionable or high-risk content
- Customer notifications and email alerts that are sent when events are detected
- Rules and policies for spam detection

Customizing Email Protocol Scan Settings

If you have used the Setup Wizard, you might have already configured the email policies; the (email) Policy screen allows you to modify these settings.

To configure the email protocols and ports to scan:

1. Select Email Security > Policy from the menu. The (email) Policy screen displays:

Figure 51.
2. Select the check boxes and complete the fields and as explained in the following table:

Table 25. Email Policy Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP</td>
<td>Select the SMTP check box to enable Simple Mail Transfer Protocol (SMTP) scanning. This service is enabled by default and uses default port 25.</td>
</tr>
<tr>
<td>POP3</td>
<td>Select the POP3 check box to enable Post Office Protocol 3 (POP3). This service is enabled by default and uses default port 110.</td>
</tr>
<tr>
<td>IMAP</td>
<td>Select the IMAP check box to enable Internet Message Access Protocol (IMAP). This service is enabled by default and uses default port 143.</td>
</tr>
</tbody>
</table>

**Note:** If a protocol uses a port other than the standard service port (for example, port 25 for SMTP), enter this nonstandard port in the Ports to Scan field. For example, if the SMTP service on your network uses both port 25 and port 2525, enter both port numbers in the Ports to Scan field and separate them by a comma.

**Note:** The following protocols are not supported by the STM: SMTP over SSL using port number 465, POP3 over SSL using port number 995, and IMAP over SSL using port number 993.

3. Click **Apply** to save your settings.

**Customizing Email Anti-Virus Settings**

If you have used the Setup Wizard, you might have already configured the email antivirus action and exception settings; the Action and Exception screens allows you to modify these settings. The Notification screen allows you to specify the email antivirus notification settings.

Whether or not the STM detects an email virus, you can configure it to take a variety of actions (some of the default actions are listed in Table 24 on page 85), set exceptions for file sizes, and specify which notifications, emails, or both need to be sent to the end users.
**Action Settings**

**To configure the email antivirus action settings:**

1. Select **Email Security > Anti-Virus** from the menu. The Anti-Virus submenu tabs display with the Action screen in view:

![Action Settings Screen](image)

Figure 52.

2. Make your selections from the drop-down lists as explained in the following table:

**Table 26. Email Anti-Virus Action Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>From the SMTP drop-down list, specify one of the following actions to be taken when an infected email is detected:</td>
</tr>
<tr>
<td>• Quarantine attachment. The email is not blocked, but the attachment is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry.</td>
<td></td>
</tr>
<tr>
<td>• Delete attachment. The email is not blocked, but the attachment is deleted, and a virus log entry or a spyware log entry is created.</td>
<td></td>
</tr>
<tr>
<td>• Block infected email. This is the default setting. The email is blocked, and a virus log entry or a spyware log entry is created.</td>
<td></td>
</tr>
<tr>
<td>• Quarantine infected email. The email is placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry.</td>
<td></td>
</tr>
<tr>
<td>• Log only. Only a virus log entry or a spyware log entry is created. The email is not blocked and the attachment is not deleted.</td>
<td></td>
</tr>
</tbody>
</table>
To configure the email antivirus exception settings:

1. Select Email Security > Anti-Virus from the menu. The Anti-Virus submenu tabs display with the Action screen in view.

2. Click the Exceptions submenu tab. The Exceptions screen displays:

![Figure 53.](image)

3. Click Apply to save your settings.

**Exception Settings**

**To configure the email antivirus exception settings:**

1. Select Email Security > Anti-Virus from the menu. The Anti-Virus submenu tabs display with the Action screen in view.

2. Click the Exceptions submenu tab. The Exceptions screen displays:

![Figure 53.](image)

**Table 26. Email Anti-Virus Action Settings (Continued)**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| POP3    | From the POP3 drop-down list, specify one of the following actions to be taken when an infected email is detected:  
  - **Quarantine attachment.** The email is not blocked, but the attachment is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry.  
  - **Delete attachment.** This is the default setting. The email is not blocked, but the attachment is deleted, and a virus log entry or a spyware log entry is created.  
  - **Log only.** Only a virus log entry or a spyware log entry is created. The email is not blocked and the attachment is not deleted. |
| IMAP    | From the IMAP drop-down list, specify one of the following actions to be taken when an infected email is detected:  
  - **Quarantine attachment.** The email is not blocked, but the attachment is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry.  
  - **Delete attachment.** This is the default setting. The email is not blocked, but the attachment is deleted, and a virus log entry or a spyware log entry is created.  
  - **Log only.** Only a virus log entry or a spyware log entry is created. The email is not blocked and the attachment is not deleted. |
3. Make your selection from the drop-down list and complete the field as explained in the following table:

**Table 27. Email Anti-Virus Exception Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Exceptions</strong></td>
<td>From the drop-down list, specify one of the following actions to be taken when an email attachment exceeds the size that you specify in the file size field:</td>
</tr>
<tr>
<td>• <strong>Skip</strong>. The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Block</strong>. The file is blocked and does not reach the end user.</td>
<td></td>
</tr>
</tbody>
</table>

The default and maximum file sizes are:

- For the STM600 and STM300, the default setting is to block any attachment larger than 10240 KB. The maximum file size that you can specify is 51200 KB.
- For the STM150, the default setting is to block any attachment larger than 8192 KB. The maximum file size that you can specify is 25600 KB.

**Note:** Setting the maximum file size to a high value might affect the STM’s performance. NETGEAR recommends the default value, which is sufficient to detect the vast majority of threats.

4. Click **Apply** to save your settings.
Notification Settings

To configure the email antivirus notification settings:

1. Select Email Security > Anti-Virus from the menu. The Anti-Virus submenu tabs display with the Action screen in view.
2. Click the Notifications submenu tab. The Notifications screen displays:

![Notification Settings](image)

Figure 54.
3. Complete the fields, select the check boxes, and make your selections from the drop-down lists as explained in the following table:

Table 28. Email Anti-Virus Notification Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Notification Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Insert Warning into Email Subject</td>
<td>For SMTP email messages, select this check box to insert a warning into the email subject line:</td>
</tr>
<tr>
<td>(SMTP)</td>
<td>• <strong>Malware Found.</strong> If a malware threat is found, a [MALWARE INFECTED] message is inserted. You can change this default message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>No Malware Found.</strong> If no malware threat is found, a [MALWARE FREE] message is inserted. You can change this default message.</td>
</tr>
<tr>
<td></td>
<td>By default, this check box is cleared and no warnings are inserted.</td>
</tr>
<tr>
<td>Append Safe Stamp (SMTP and POP3)</td>
<td>For SMTP and POP3 email messages, select this check box to insert a default safe stamp message at the end of an email. The safe stamp insertion serves as a security confirmation to the end user. You can change the default message. By default, this check box is cleared and no safe stamp is inserted.</td>
</tr>
<tr>
<td>Append Warning if Attachment</td>
<td>For SMTP and POP3 email messages, select this check box to append a default warning message to an email if the message or an attachment to the message exceeds the scan size limit. The warning message informs the end user that the attachment was skipped and might not be safe to open. You can change the default message. By default, this check box is selected and a warning message is appended to the email.</td>
</tr>
<tr>
<td>Exceeds Scan Size Limit (SMTP and POP3)</td>
<td></td>
</tr>
<tr>
<td>Replace Infected Attachments with</td>
<td>Select this check box to replace an email that is infected with a default warning message. The warning message informs the end user about the name of the malware threat. You can change the default message to include the action that the STM has taken (see the following example). By default, this check box is selected, and a warning message replaces an infected email.</td>
</tr>
<tr>
<td>the Following Warning Message</td>
<td>The following is a sample message where the %VIRUSINFO% metaword is replaced with the EICAR test virus:</td>
</tr>
<tr>
<td></td>
<td>This attachment contains malware: File 1.exe contains malware EICAR. Action: Delete.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Make sure that you keep the %VIRUSINFO% metaword in a message to enable the STM to insert the correct malware threat information.</td>
</tr>
<tr>
<td><strong>Email Alert Settings</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Ensure that the email notification server (see Configuring the Email Notification Server on page 176) is configured before you specify the email alert settings.</td>
</tr>
<tr>
<td>Send alert to</td>
<td>In addition to inserting a warning message to replace an infected email, you can configure the STM to send a notification email to the sender, the recipient, or both by selecting the corresponding check box or check boxes. By default, both check boxes are cleared and no notification email is sent.</td>
</tr>
</tbody>
</table>
Email Content Filtering

The STM provides several options to filter unwanted content from emails. You can filter content from emails based on keywords in the subject line, file type of the attachment, and file name of the attachment. You can also set an action to perform on emails with password-protected attachments.

Several types of email blocking are available:

- **Keyword blocking.** You can specify words that, should they appear in the email subject line, cause that email to be blocked by the STM.
- **Password-protected attachments.** You can block emails based on password-protected attachments such as .zip or .rar attachments.
- **File extension blocking.** You can block emails based on the extensions of attached files. Such files can include executable files, audio and video files, and compressed files.
- **File name blocking.** You can block emails based on the names of attached files. Such names can include, for example, names of known malware threats such as the Netsky worm (which normally arrives as netsky.exe).

4. Click **Apply** to save your settings.

### Table 28. Email Anti-Virus Notification Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subject</strong></td>
<td>The default subject line for the notification email is “Malware detected!” You can change this subject line.</td>
</tr>
<tr>
<td><strong>Message</strong></td>
<td>The warning message informs the sender, the recipient, or both about the name of the malware threat. You can change the default message to include more information. Make sure that you keep the %VIRUSINFO% metaword in a message to enable the STM to insert the correct malware threat information. In addition to the %VIRUSINFO% metaword, you can insert the following metawords in your customized message: %TIME%, %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%.</td>
</tr>
</tbody>
</table>
To configure email content filtering:

1. Select **Email Security > Filters** from the menu. The Filters screen displays:

   ![Filters Screen](image)

   **Figure 55.**
2. Complete the fields and make your selections from the drop-down lists as explained in the following table:

Table 29. Email Filter Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter by Subject Keywords</strong></td>
<td></td>
</tr>
<tr>
<td>Keywords</td>
<td>Enter keywords that are detected in the email subject line. Use commas to separate different keywords. The total maximum length of this field is 2048 characters, excluding duplicate words and delimiter commas.</td>
</tr>
<tr>
<td>Action SMTP</td>
<td>From the SMTP drop-down list, specify one of the following actions to be taken when a keyword that is defined in the Keywords field is detected:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Block email &amp; Log.</strong> The email is blocked, and a log entry is created.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Log.</strong> This is the default setting. Only a log entry is created. The email is not blocked.</td>
</tr>
<tr>
<td>Action POP3</td>
<td>From the POP3 drop-down list, specify one of the following actions to be taken when a keyword that is defined in the Keywords field is detected:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Block email &amp; Log.</strong> The email is blocked, and a log entry is created.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Log.</strong> This is the default setting. Only a log entry is created. The email is not blocked.</td>
</tr>
<tr>
<td><strong>Filter by Password-Protected Attachments (ZIP, RAR, etc.)</strong></td>
<td></td>
</tr>
<tr>
<td>Action SMTP</td>
<td>From the SMTP drop-down list, specify one of the following actions to be taken when a password-protected attachment to an email is detected:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Block attachment &amp; Log.</strong> The email is not blocked, the attachment is blocked, and a log entry is created.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Block email &amp; Log.</strong> The email is blocked, and a log entry is created.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Log.</strong> This is the default setting. Only a log entry is created. The email and attachment are not blocked.</td>
</tr>
<tr>
<td>Action POP3</td>
<td>From the POP3 drop-down list, specify one of the following actions to be taken when a password-protected attachment to an email is detected:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Block attachment &amp; Log.</strong> The email is not blocked, the attachment is blocked, and a log entry is created.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Log.</strong> This is the default setting. Only a log entry is created. The email and attachment are not blocked.</td>
</tr>
<tr>
<td>Action IMAP</td>
<td>From the IMAP drop-down list, specify one of the following actions to be taken when a password-protected attachment to an email is detected:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Block attachment &amp; Log.</strong> The email is not blocked, the attachment is blocked, and a log entry is created.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Log.</strong> This is the default setting. Only a log entry is created. The email and attachment are not blocked.</td>
</tr>
</tbody>
</table>
3. Click **Apply** to save your settings.

## Protecting Against Email Spam

The STM integrates multiple antispam technologies to provide comprehensive protection against unwanted email. You can enable all or a combination of these antispam technologies. The STM implements these spam prevention technologies in the following order:

1. **Whitelist.** Emails from the specified sources or to the specified recipients are not considered spam and are accepted.
2. **Blacklist.** Emails from the specified sources are considered spam and are blocked.
3. **Real-time blacklist.** Emails from known spam sources that are collected by blacklist providers are blocked.
4. **Distributed spam analysis.** Emails that are detected as spam by the NETGEAR Spam Classification Center are either tagged, blocked, or quarantined.
This order of implementation ensures the optimum balance between spam prevention and system performance. For example, if an email originates from a whitelisted source, the STM delivers the email immediately to its destination inbox without implementing the other spam prevention technologies, thereby speeding up mail delivery and conserving the STM system resources. However, regardless of whether or not an email is whitelisted, it is still scanned by the STM’s antimalware engines.

You can configure these antispam options in conjunction with content filtering to optimize blocking of unwanted mails.

---

**Note:** Emails that are sent through the STM over an authenticated connection between a client and an SMTP mail server are not checked for spam.

---

**Note:** An email that has been checked for spam by the STM contains an “X-STM-SMTP” (for SMTP emails) or “X-STM-POP3” (for POP-3 emails) tag in its header.

---

**Setting Up the Whitelist and Blacklist**

You can specify emails that are accepted or blocked based on the originating IP address, domain, and email address by setting up the whitelist and blacklist. You can also specify emails that are accepted based on the destination domain and email address.

The whitelist ensures that email from listed (that is, trusted) sources and recipients is not mistakenly tagged as spam. Emails going to and from these sources and recipients are delivered to their destinations immediately, without being scanned by the antispam engines. This can help to speed up the system and network performance. The blacklist, on the other hand, lists sources from which all email messages are blocked. You can enter up to 200 entries per list, separated by commas.

---

**Note:** The whitelist takes precedence over the blacklist, which means that if an email source is on both the blacklist and the whitelist, the email is not scanned by the antispam engines.
To configure the whitelist and blacklist:

1. Select **Email Security > Anti-Spam** from the menu. The Anti-Spam submenu tabs display, with the Whitelist/Blacklist screen in view.

![Image of Whitelist/Blacklist screen](image-url)

Figure 56.
Complete the fields as explained in the following table:

Table 30. Whitelist/Blacklist Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sender IP Address (SMTP)</strong></td>
<td></td>
</tr>
<tr>
<td>Whitelist</td>
<td>Enter the source IP addresses from which emails can be trusted.</td>
</tr>
<tr>
<td>Blacklist</td>
<td>Enter the source IP addresses from which emails are blocked.</td>
</tr>
<tr>
<td>Click Apply to save settings</td>
<td>or click Reset to clear all entries from these fields.</td>
</tr>
<tr>
<td><strong>Sender Domain (SMTP and POP3)</strong></td>
<td></td>
</tr>
<tr>
<td>Whitelist</td>
<td>Enter the sender email domains from which emails can be trusted.</td>
</tr>
<tr>
<td>Blacklist</td>
<td>Enter the sender email domains from which emails are blocked.</td>
</tr>
<tr>
<td>Click Apply to save settings</td>
<td>or click Reset to clear all entries from these fields.</td>
</tr>
<tr>
<td><strong>Sender Email Address (SMTP and POP3)</strong></td>
<td></td>
</tr>
<tr>
<td>Whitelist</td>
<td>Enter the email addresses from which emails can be trusted.</td>
</tr>
<tr>
<td>Blacklist</td>
<td>Enter the email addresses from which emails are blocked.</td>
</tr>
<tr>
<td>Click Apply to save settings</td>
<td>or click Reset to clear all entries from these fields.</td>
</tr>
<tr>
<td><strong>Recipients Domain (SMTP and POP3)</strong></td>
<td></td>
</tr>
<tr>
<td>Whitelist</td>
<td>Enter the email domains of the recipients to which emails can be safely delivered.</td>
</tr>
<tr>
<td>Click Apply to save settings</td>
<td>or click Reset to clear all entries from this field.</td>
</tr>
<tr>
<td><strong>Recipients Email Address (SMTP and POP3)</strong></td>
<td></td>
</tr>
<tr>
<td>Whitelist</td>
<td>Enter the email addresses of the recipients to which emails can be safely delivered.</td>
</tr>
<tr>
<td>Click Apply to save settings</td>
<td>or click Reset to clear all entries from this field.</td>
</tr>
</tbody>
</table>

**Note:** In the fields of the Whitelist/Blacklist screen, use commas to separate multiple entries. For IP addresses, use a hyphen to indicate a range (for example, 192.168.32.2-192.168.32.8.)

**Configuring the Real-Time Blacklist**

Blacklist providers are organizations that collect IP addresses of verified open SMTP relays that might be used by spammers as media for sending spam. These known spam relays are compiled by blacklist providers and are made available to the public in the form of real-time blacklists (RBLs). By accessing these RBLs, the STM can block spam originating from known spam sources.
To enable the real-time blacklist:

1. Select **Email Security > Anti-Spam** from the menu. The Anti-Spam submenu tabs display, with the Whitelist/Blacklist screen in view.

2. Click the **Real-Time Blacklist** submenu tab. The Real-Time Blacklist screen displays:

   ![Real-Time Blacklist Screen](image)

   **Figure 57.**

3. Select the **Enable** check box to enable the Real-Time Blacklist function.

4. Select the **Active** check boxes to the left of the default blacklist providers (Spamhaus and Spamcop) that you want to activate. A Terms of Service popup window displays.

5. Read the terms of service in the Terms of Service field. If you agree with these terms, click **OK**.

6. Click **Apply** to save your settings.
To add a blacklist provider to the real-time blacklist:

1. In the Add Real-time Blacklist section, add the following information:
   • In the Provider field, add the name of the blacklist provider.
   • In the RBL Domain Suffix field, enter the domain suffix of the blacklist provider.

2. Click the Add table button in the Add column. The new blacklist provider is added to the Real-Time Blacklist (SMTP) table, and it is disabled by default.

To delete a blacklist provider from the real-time blacklist, click the Delete table button next to the blacklist provider that you want to delete.

Configuring Distributed Spam Analysis

Spam, phishing, and other email-borne threats consist of millions of messages intentionally composed differently to evade commonly used filters. Nonetheless, all messages within the same outbreak share at least one unique, identifiable value that can be used to distinguish the outbreak.

With distributed spam analysis, message patterns are extracted from the message envelope, headers, and body with no reference to the content itself. Pattern analysis can then be applied to identify outbreaks in any language, message format, or encoding type. Message patterns can be divided into distribution patterns and structure patterns. The STM uses distribution patterns to determine if the message is legitimate or a potential threat by analyzing the way it is distributed to the recipients. The STM uses structure patterns to determine the volume of the distribution.

The STM uses a distributed spam analysis architecture to determine whether or not an email is spam for SMTP and POP3 emails. Any email that is identified as spam is tagged as spam (an option for both SMTP and POP3), blocked, or quarantined (the latter two are options possible only for SMTP).

Note: Unlike other scans, you do not need to configure the spam score because the NETGEAR Spam Classification Center performs the scoring automatically as long as the STM is connected to the Internet. However, this does mean that the STM needs to be connected to the Internet for the spam analysis to be performed correctly.
To configure distributed spam analysis and the antispam engine settings:

1. Select **Email Security > Anti-Spam** from the menu. The Anti-Spam submenu tabs display, with the Whitelist/Blacklist screen in view.

2. Click the **Distributed Spam Analysis** submenu tab. The Distributed Spam Analysis screen displays:

![Distributed Spam Analysis](image)

3. Complete the fields, select the check boxes, and make your selections from the drop-down lists as explained in the following table:

**Table 31. Distributed Spam Analysis Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed Spam Analysis</td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>Select the <strong>SMTP</strong> check box to enable distributed spam analysis for the SMTP protocol. (You can enable distributed spam analysis for both SMTP and POP3.)</td>
</tr>
<tr>
<td>POP3</td>
<td>Select the <strong>POP3</strong> check box to enable distributed spam analysis for the POP3 protocol. (You can enable distributed spam analysis for both SMTP and POP3.)</td>
</tr>
</tbody>
</table>
### Action

SMTP

From the SMTP drop-down list, select the action that is taken when spam is detected by the antispam engine:

- **Tag spam email.** This is the default setting. The email is tagged as spam, and a spam log entry is created.
- **Block spam email.** The email is blocked, and a spam log entry is created.
- **Quarantine spam email.** The email is quarantined, a spam log entry is created, and a spam quarantine log entry is created.

POP3

The only option is to tag spam email. A spam log entry is also created.

### Tag

**Add tag to mail subject**

When you select the Tag spam email option from the Action drop-down list (see earlier in this table), select this check box to add a tag to the email subject line. The default tag is [SPAM], but you can customize this tag. The default setting is to add the default tag to the subject line.

**Add tag X-NETGEAR-SPAM to mail header**

When you select the Tag spam email option from the Action drop-down list (see earlier in this table), select this check box to add the X-NETGEAR-SPAM tag to the email header. The default setting is to add the default tag to the email header.

### Send Quarantine Spam Report

**Note:** Ensure that the email notification server (see *Configuring the Email Notification Server* on page 176) is configured before you specify the quarantine spam report settings.

**Enable**

Select this check box to enable the STM to send a quarantine spam report to the recipient that you have specified on the Email Notification Server screen (see *Configuring the Email Notification Server* on page 176).

Select one of the following radio buttons to specify the frequency with which the report is sent:

- **Weekly.** Reports are sent weekly at the day and time that you specify from the drop-down lists (weekday, hours, and minutes).
- **Daily.** Reports are sent daily at the time that you specify from the drop-down lists (hours and minutes).
Click Apply to save your settings. The Distributed Spam Analysis section and the Send Quarantine Spam Report section each have their own Apply and Reset buttons to enable you to make changes to these sections separately.

### Configuring Web and Services Protection

The STM lets you configure the following settings to protect the network’s Internet communication:

- The Web protocols that are scanned for malware threats
- Actions that are taken when infected Web files or objects are detected
- The maximum file sizes that are scanned
- Web objects that are blocked
- Web categories, keywords, and file types that are filtered to block objectionable or high-risk content
- Domains and URLs that are blocked for objectionable or high-risk content
- Customer notifications and email alerts that are sent when events are detected
- Schedules that determine when content filtering is active

### Customizing Web Protocol Scan Settings

If you have used the Setup Wizard, you might have already configured the Web protocol scan settings; the (Web) Policy screen allows you to modify these settings.

Scanning all protocols enhances network security, but might affect the performance of the STM. For an optimum balance between security and performance, enable scanning only of the most commonly used protocols on your network. For example, you can scan FTP and HTTP, but not HTTPS (if this last protocol is not often used). For more information about performance, see Managing the STM’s Performance on page 82.
To specify the Web protocols and ports that are scanned for malware threats.

1. Select **Web Security > Policies** from the menu. The (Web) Policy screen displays:

![Web Policy Screen](image)

**Figure 59.**

2. Select the check boxes and complete the fields and as explained in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services to Scan</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>Select the <strong>HTTP</strong> check box to enable Hypertext Transfer Protocol (HTTP) scanning. This service is enabled by default and uses default port 80. You can change the standard service port or add another port in the corresponding Ports to Scan field.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Select the <strong>HTTPS</strong> check box to enable Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). This service is disabled by default. The HTTPS default port is 443. You can change the standard service port or add another port in the corresponding Ports to Scan field.</td>
</tr>
<tr>
<td>FTP</td>
<td>Select the <strong>FTP</strong> check box to enable File Transfer Protocol (FTP). This service is enabled by default and uses default port 21. You can change the standard service port or add another port in the corresponding Ports to Scan field.</td>
</tr>
</tbody>
</table>

**Note:** If a protocol uses a port other than the standard service port (for example, port 80 for HTTP), enter this nonstandard port in the Ports to Scan field. For example, if the HTTP service on your network uses both port 80 and port 8080, enter both port numbers in the Ports to Scan field, and separate them by a comma.

3. Click **Apply** to save your settings.
Configuring Web Malware Scans

If you have used the Setup Wizard, you might have already configured the Web malware action and exception scan settings; the Malware Scan screen allows you to modify these settings.

Whether or not the STM detects Web-based malware threats, you can configure it to take a variety of actions (some of the default actions are listed in Table 24 on page 85), skip files that are too large, and send notifications, emails, or both to the end users.

To configure the Web-based malware settings:

1. Select Application Security > HTTP/HTTPS from the menu. The HTTP/HTTPS submenu tabs display, with the Malware Scan screen in view:

![Malware Scan Screen](image)

Figure 60.
2. Complete the fields, select the check boxes, and make your selections from the drop-down lists as explained in the following table:

Table 33. Malware Scan Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>From the HTTP or HTTPS drop-down list, specify one of the following actions to be taken when an infected Web file or object is detected:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Quarantine file.</strong> The file is placed in quarantine, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Delete file.</strong> This is the default setting. The Web file or object is deleted, and depending on the nature of the malware threat, a virus log entry or a spyware log entry is created.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Log only.</strong> Depending on the nature of the malware threat, only a virus log entry or a spyware log entry is created. The Web file or object is not placed in quarantine nor deleted.</td>
</tr>
<tr>
<td>Streaming</td>
<td>Select the <strong>Streaming</strong> check box to enable streaming of partially downloaded and scanned HTTP or HTTPS file parts to the end user. This method allows the user to experience more transparent Web downloading. Streaming is enabled by default.</td>
</tr>
</tbody>
</table>

**Scan Exceptions**

From the drop-down list, specify one of the following actions to be taken when a file or message exceeds the size that you specify in the file size field:

- **Skip.** The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting.
- **Block.** The file is blocked and does not reach the end user.

The default and maximum file sizes are as follows:

- For the STM600 and STM300, the default setting is to block any attachment larger than 10240 KB. The maximum file size that you can specify is 51200 KB.
- For the STM150, the default setting is to block any attachment larger than 8192 KB. The maximum file size that you can specify is 25600 KB.

**Note:** Setting the maximum file size to a high value might affect the STM’s performance. NETGEAR recommends the default value, which is sufficient to detect the vast majority of threats.

**HTML Scan**

Select this check box to enable scanning of HyperText Markup Language (HTML) files, which is enabled by default.

**Notification Settings**

Select the **Replace Page with the Following Warning Text** check box to enable the STM to replace the content of a Web page that is blocked because of a detected malware threat with the following text:

NETGEAR ProSecure Web/Email Security Threat Management Appliance has detected and stopped malicious code embedded in this web site for protecting your computer and network from infection. %VIRUSINFO%
Click **Apply** to save your settings.

### Configuring Web Content Filtering

If you want to restrict internal LAN users from access to certain types of information and objects on the Internet, use the STM’s content filtering and Web objects filtering. With the exception of the Web content categories that are mentioned in *Default Email and Web Scan Settings* on page 85, all requested traffic from any website is allowed. You can specify a message such as “Blocked by NETGEAR” that is displayed onscreen if a user attempts to access a blocked site (see the Notification Settings section that is described at the bottom of Table 34 on page 112). Several types of Web content blocking are available:

- **File extension blocking.** You can block files based on their extension. Such files can include executable files, audio and video files, and compressed files.

- **Web object blocking.** You can block the following Web objects: embedded objects (ActiveX, Java, Flash), proxies, and cookies; and you can disable Java scripts. However, websites that are on the whitelist (see *Configuring Web URL Filtering* on page 116) are never subject to Web object blocking.

- **Web category blocking.** You can block entire Web categories because their content is unwanted, offensive, or not relevant, or simply to reduce traffic.

---

**Note:** You can bypass any type of Web blocking for trusted domains by adding the exact matching domain names to the trusted host list (see *Specifying Trusted Hosts* on page 124). Access to the domains on the trusted host list is allowed for PCs in the groups for which file extension, object, or category blocking, or a combination of these types of Web blocking has been enabled.

---

**Note:** You can bypass any type of Web blocking for trusted URLs by adding the URLs to the whitelist (see *Configuring Web URL Filtering* on page 116). Access to the URLs on the whitelist is allowed for PCs in the groups for which file extension, object, or category blocking, or a combination of these types of Web blocking has been enabled.

---

### Table 33. Malware Scan Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Note:** You can customize this text. Make sure that you keep the %VIRUSINFO% metaword in the text to enable the STM to insert the correct malware threat information. In addition to the %VIRUSINFO% metaword, you can insert the following metawords in your customized message: %TIME%, %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%.

*Note:* The text is displayed on the Malware Scan screen with HTML tags. Click **Preview** to open a screen that displays the notification text in HTML format.
Note: For information about creating custom categories that allow you to set access exceptions for combinations of Web categories, see Creating Custom Categories for Web Access Exceptions on page 142.

If you have used the Setup Wizard, you might have already configured the Web category blocking settings; the Content Filtering screen allows you to modify these settings.

To configure Web content filtering:

1. Select Web Security > HTTP/HTTPS from the menu. The HTTP/HTTPS submenu tabs display, with the Malware Scan screen in view.

2. Click the Content Filtering submenu tab. The Content Filtering screen displays. Because of the large size of this screen, it is presented in this manual in three figures (the following figure, Figure 62 on page 111, and Figure 63 on page 112).

![Content Filtering Screen](image)

Figure 61. Content Filtering, screen 1 of 3
Figure 62. Content Filtering, screen 2 of 3
Figure 63. Content Filtering, screen 3 of 3

3. Complete the fields, select the check boxes, and make your selections from the drop-down lists as explained in the following table:

Table 34. Content Filtering Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Content Filtering  | Select this check box to log HTTP traffic. For information about how to view the logged traffic, see Querying Logs on page 194. By default, HTTP traffic is not logged.  
Note: Logging HTTP traffic might affect the STM’s performance (see Managing the STM’s Performance on page 82).                                                                                                           |
Table 34. Content Filtering Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Block Files with the Following Extensions | Select the check box to enable file extension blocking. By default, the File Extension field lists the most common file extensions that are detected. You can manually add or delete extensions. Use commas to separate different extensions. You can also use the drop-down list to add predefined file extensions from a specific category to the File Extension field:  
  • None. No file extensions are added to the File Extension field. This is the default setting.  
  • Executables. Executable file extensions (exe, com, dll, so, lib, scr, bat, and cmd) are added to the File Extension field.  
  • Audio/Video. Audio and video file extensions (wav, mp3, avi, rm, rmvb, wma, wmv, mpg, mp4, and aac) are added to the File Extension field.  
  • Compressed Files. Compressed file extensions (zip, rar, gz, tar, and bz2) added to the File Extension field. |
| Show This Message When a File was Blocked | The STM replaces the content of a Web page that is blocked because of violating file extensions with the following text, which you can customize:  
  Internet Policy has restricted access to this location with file extension:  
  %URL%  
  Note: Make sure that you keep the %URL% metaword in the text to enable the STM to show the URL of the blocked pager. |
| As an option, you can select the Insert Link to User Login Portal Page check box. When you select this check box, the screen that displays when a user attempts to access blocked content includes a hyperlink that allows the user to log in as another user:  
  You are logged in as %USER%  
  (Click here to login as another user)  
  Note: Make sure that you keep the %LOGIN-LINK% metaword in the text to enable the STM to insert the actual hyperlink. |
| The text is displayed on the Content Filtering screen with HTML tags. Click Preview to open a screen that displays the notification text in HTML format. |
| Block Web Objects                        | Select one or both of the following check boxes:  
  Remove Embedded Objects | All embedded objects such as ActiveX, Java, and Flash objects are removed from downloaded Web pages.  
  Note: Because embedded objects are commonly used on legitimate websites, blocking embedded objects globally might have a negative impact on a user’s Web browsing experience.  
  Disable Javascript | Javascript is disabled on downloaded Web pages. |
Select the **Web Categories You Wish to Block**

Select the **Enable Blocking** check box to enable blocking of Web categories, which is the default setting. Select the check boxes of any Web categories that you want to block. Use the action buttons at the top of the section in the following way:

- **Allow All.** All Web categories are allowed.
- **Block All.** All Web categories are blocked.
- **Set to Defaults.** Blocking and allowing of Web categories are returned to their default settings. See Table 24 on page 85 for information about the Web categories that are blocked by default. Categories that are preceded by a green rectangle are allowed by default; categories that are preceded by a pink rectangle are blocked by default.

### Web Categorization Schedule

**Do You Want this Schedule to be Active on All Days or Specific Days?**

Select one of the following radio buttons:

- **All Days.** The schedule is in effect all days of the week.
- **Specific Days.** The schedule is active only on specific days.

To the right of the radio buttons, select the check box for each day that you want the schedule to be in effect.

**Do You Want this Schedule to be Active All Day or at Specific Times during the Day?**

Select one of the following radio buttons:

- **All Day.** The schedule is in effect all hours of the selected day or days.
- **Specific Times.** The schedule is active only on specific hours of the selected day or days.

To the right of the radio buttons, fill in the Start Time and End Time fields (Hour, Minute, AM/PM) during which the schedule is in effect.

**Replace the Content of a Blocked Page with the Following Text**

The STM replaces the content of a Web page that is blocked because of violating content with the following text, which you can customize:

> Internet Policy has restricted access to this location belonging to the following categories:

> %FULL-CATEGORY-LIST%

**Note:** Make sure that you keep the %FULL-CATEGORY-LIST% metaword in the text to enable the STM to insert the categories that the blocked Web page falls under.
As an option, you can select one or both of the following check boxes:

- **Allow Users to Submit a "Report a URL Misclassification" Form.** When you select this check box, the screen that displays when a user attempts to access blocked content includes a hyperlink to report a URL misclassification. See [Click here to Report a URL Misclassification](#) in the Web Category Lookup section later in this table.

  **Note:** Make sure that you keep the %SUBMIT-URL-CATEGORIZATION% metaword in the text to enable the STM to insert the actual hyperlink.

- **Insert Link to User Login Portal Page.** When you select this check box, the screen that displays when a user attempts to access blocked content includes a hyperlink that allows the user to log in as another user:
  
  You are logged in as %USER%
  
  (Click here to login as another user)

  **Note:** Make sure that you keep the %LOGIN-LINK% metaword in the text to enable the STM to insert the actual hyperlink.

The text is displayed on the Content Filtering screen with HTML tags. Click [Preview](#) to open a screen that displays the notification text in HTML format.

### Web Category Lookup

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Enter a URL to find out if it has been categorized, and if so, in which category. Then click the <strong>Lookup</strong> button. If the URL has been categorized, the category appears next to Lookup Results.</td>
</tr>
<tr>
<td>Clear Web Category Cache</td>
<td>Click <strong>Clear Web Category Cache</strong> to enable the STM to synchronize with the NETGEAR server and download the most recent Web categorizations.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Synchronizing might temporarily slow down the STM’s performance because the STM needs to acquire the Web categorizations remotely instead of from its local cache.</td>
</tr>
</tbody>
</table>

4. **Click Apply** to save your settings.
Configuring Web URL Filtering

If you want to allow or block internal LAN users from access to certain sites on the Internet, use the STM’s Web URL filtering. You can create or import a whitelist that contains domain names and URLs that are accepted, and a blacklist with domain names and URLs that are blocked. The whitelist takes precedence over the blacklist.

**Note:** A URL that you enter on the whitelist or blacklist might contain other embedded URLs such as URLs for advertisements or sponsors, causing unexpected behavior. If you want to allow a URL by placing it on the whitelist, make sure that all embedded URLs are also placed on the whitelist. Similarly, if you want to block a URL by placing it on the blacklist, make sure that all embedded URLs are also placed on the blacklist.

**Note:** For information about creating custom categories that allow you to set access exceptions for combinations of URLs, see *Creating Custom Categories for Web Access Exceptions* on page 142.
To configure Web URL filtering:

1. Select **Web Security > HTTP/HTTPS** from the menu. The HTTP/HTTPS submenu tabs display, with the Malware Scan screen in view.

2. Click the **URL Filtering** submenu tab. The URL Filtering screen displays:

![URL Filtering screen](image)

**Figure 64.**
3. Select the check boxes and complete the fields and as explained in the following table:

Table 35. URL Filtering Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Whitelist (takes precedence over Blacklist)</strong></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>Select this check box to bypass scanning of the URLs that are listed in the URL field. Users are allowed to access the URLs that are listed in the URL field.</td>
</tr>
</tbody>
</table>
| URL             | This field contains the URLs for which scanning is bypassed. To add a URL to this field, use the Add URL field or the Import from File tool (see information later in this table). You can add a maximum of 2000 URLs.  

**Note:** If a URL is in both the whitelist and blacklist, then the whitelist takes precedence and URLs on the whitelist are not scanned.  

**Note:** Wildcards (*) are supported. For example, if you enter www.net*.com in the URL field, any URL that begins with www.net and ends with .com is allowed. |
| Delete          | To delete one or more URLs, highlight the URLs, and click the Delete table button. |
| Export          | To export the URLs, click the Export table button, and follow the instructions of your browser. |
| **Add URL**     | Type or copy a URL in the Add URL field. Then click the Add table button to add the URL to the URL field. |
| **Import from File** | To import a list with URLs into the URL field, click the Browse button and navigate to a file in .txt format that contains line-delimited URLs (that is, one URL per line). Then click the Upload table button to add the URLs to the URL field.  

**Note:** Any existing URLs in the URL field are overwritten when you import a list of URLs from a file. |
| **Blacklist**   |                                                                                   |
| Enable          | Select this check box to block the URLs that are listed in the URL field. Users attempting to access these URLs receive a notification (see information later in this table). |
| URL             | This field contains the URLs that are blocked. To add a URL to this field, use the Add URL field or the Import from File tool (see information later in this table). You can add a maximum of 2000 URLs.  

**Note:** If a URL is in both the whitelist and blacklist, then the whitelist takes precedence and URLs on the whitelist are not scanned.  

**Note:** Wildcards (*) are supported. For example, if you enter www.net*.com in the URL field, any URL that begins with www.net and ends with .com is blocked. |
| Delete          | To delete one or more URLs, highlight the URLs, and click the Delete table button. |
| Export          | To export the URLs, click the Export table button and follow the instructions of your browser. |
Table 35. URL Filtering Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add URL</td>
<td>Type or copy a URL in the Add URL field. Then click the Add table button to add the URL to the URL field.</td>
</tr>
<tr>
<td>Import from File</td>
<td>To import a list with URLs into the URL field, click the Browse button and navigate to a file in .txt format that contains line-delimited URLs (that is, one URL per line). Then click the Upload table button to add the URLs to the URL field. <strong>Note:</strong> Any existing URLs in the URL field are overwritten when you import a list of URLs from a file.</td>
</tr>
<tr>
<td>Replace the Content of a Blocked Page with the Following Text</td>
<td>When a user attempts to access a blocked URL, the STM replaces the content of the blocked URL with the following text, which you can customize: Internet Policy has restricted access to this location: %URL% <strong>Note:</strong> Make sure that you keep the %URL% metaword in the text to enable the STM to insert the category that the blocked Web page falls under.</td>
</tr>
<tr>
<td>Insert Link to User Login Portal Page</td>
<td>As an option, you can select the Insert Link to User Login Portal Page check box to include a hyperlink on screen that allows the user to log in as another user: You are logged in as %USER% (Click here to login as another user) <strong>Note:</strong> Make sure that you keep the %LOGIN-LINK% metaword in the text to enable the STM to insert the actual hyperlink.</td>
</tr>
</tbody>
</table>

4. Click **Apply** to save your settings.

**HTTPS Scan Settings**

HTTPS traffic is encrypted traffic that cannot be scanned or the data stream would not be secure. However, the STM can scan HTTPS traffic that is transmitted through an HTTP proxy. The STM can break up the SSL connection between the HTTPS server and the HTTP client, scan the HTTPS traffic, and then rebuild the SSL connection.
The following figure shows the HTTPS scanning traffic flow:

![HTTPS Scanning Traffic Flow Diagram]

**Figure 65.**

The HTTPS scanning process functions with the following principles:

- The STM breaks up an SSL connection between an HTTPS server and an HTTP client into two parts:
  - A connection between the HTTPS client and the STM
  - A connection between the STM and the HTTPS server
- The STM simulates the HTTPS server communication to the HTTPS client, including the SSL negotiation, certificate exchange, and certificate authentication. In effect, the STM functions as the HTTPS server for the HTTPS client.
- The STM simulates the HTTPS client communication to the HTTPS server, including the SSL negotiation, certificate exchange, and certificate authentication. In effect, the STM functions as the HTTPS client for the HTTPS server.

During SSL authentication, the HTTPS client authenticates three items:

- Is the certificate trusted?
- Has the certificate expired?
- Does the name on the certificate match that of the website?
If one of these is not satisfied, a security alert message displays in the browser window:

![Security Alert]

**Figure 66.**

However, even when a certificate is trusted or still valid, or when the name of a certificate does match the name of the website, a security alert message still displays when a user who is connected to the STM visits an HTTPS site. The appearance of this security alert message is expected behavior because the HTTPS client receives a certificate from the STM instead of directly from the HTTPS server. If you want to prevent this security alert message from displaying, install a root certificate on the client PC. The root certificate can be downloaded from the STM’s User Portal Login screen (see Figure 88 on page 156).

If client authentication is required, the STM might not be able to scan the HTTPS traffic because of the nature of SSL. SSL has two parts—client and server authentication. HTTPS server authentication occurs with every HTTPS request, but HTTPS client authentication is not mandatory, and rarely occurs. Therefore it is of less importance whether the HTTPS request comes from the STM or from the real HTTPS client.

However, certain HTTPS servers do require HTTPS client certificate authentication for every HTTPS request. Because of the design of SSL, the HTTPS client needs to present its own certificate in this situation rather than using the one from the STM, preventing the STM from scanning the HTTPS traffic. For information about certificates, see Managing Digital Certificates on page 76.

You can specify trusted hosts for which the STM bypasses HTTPS traffic scanning. For more information, see Specifying Trusted Hosts on page 124.
To configure the HTTPS scan settings:

1. Select **Web Security > HTTP/HTTPS** from the menu. The HTTP/HTTPS submenu tabs display, with the Malware Scan screen in view.

2. Click the **HTTPS Settings** submenu tab. The HTTPS Settings screen displays:

![HTTPS Settings Screen](image)

**Figure 67.**
3. Select the check boxes and complete the field as explained in the following table:

Table 36. HTTPS Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Tunneling</strong></td>
<td>Select this check box to allow scanning of HTTPS connections through an HTTP proxy, which is disabled by default. Traffic from trusted hosts is not scanned (see Specifying Trusted Hosts on page 124).</td>
</tr>
<tr>
<td><strong>HTTPS SSL Settings</strong></td>
<td>Select the Allow the STM to handle HTTPS connections using SSLv2 check box to allow HTTPS connections using SSLv2, SSLv3, or TLSv1. If this check box is cleared, the STM allows HTTPS connections using SSLv3 or TLSv1, but SSLv2 connections are dropped by the STM.</td>
</tr>
<tr>
<td><strong>HTTPS 3rd Party Website Certificate Handling</strong></td>
<td>Select this check box to allow a Secure Sockets Layer (SSL) connection with a valid certificate that is not signed by a trusted Certificate Authority (CA). The default setting is to allow such as a connection.</td>
</tr>
</tbody>
</table>
| **Show This Message When an SSL Connection Attempt Fails** | By default, a rejected SSL connection is replaced with the following text, which you can customize:  
  The SSL connection cannot be established.  
  URL: %URL%  
  REASON: %REASON%  
  Note: The text is displayed on the HTTPS Settings screen with HTML tags. Click Preview to open a screen that displays the notification text in HTML format.  
  Note: Make sure that you keep the %URL% and %REASON% metawords in the text to enable the STM to insert the correct URL information and the reason of the rejection. |

4. Click **Apply** to save your settings.

**Note:** For information about certificates that are used for SSL connections and HTTPS traffic, see Managing Digital Certificates on page 76.
Specifying Trusted Hosts

You can specify trusted hosts for which the STM bypasses HTTPS traffic scanning and security certificate authentication. The security certificate is sent directly to the client for authentication, which means that the user does not receive a security alert for trusted hosts. For more information about security alerts, see Managing Digital Certificates on page 76.

Note that certain sites contain elements from different HTTPS hosts. As an example, assume that the https://example.com site contains HTTPS elements from the following three hosts:

- trustedhostserver1.example.com
- trustedhostserver2.example.com
- imageserver.example.com

To completely bypass the scanning of the https://example.com site, you need to add all three hosts to the trusted hosts list because different files from these three hosts are also downloaded when a user attempts to access the https://example.com site.

To specify trusted hosts:

1. Select Web Security > HTTP/HTTPS from the menu. The HTTP/HTTPS submenu tabs display, with the Malware Scan screen in view.
2. Click the Trusted Hosts submenu tab. The Trusted Hosts screen displays. (The following figure contains an example.)

![Figure 68.](image)

To specify trusted hosts:
3. Complete the fields and select the check box as explained in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do Not Intercept HTTPS Connections for the following Hosts</td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>Select this check box to bypass scanning of trusted hosts that are listed in the Hosts field. Users do not receive a security alert for trusted hosts that are listed in the Hosts field.</td>
</tr>
<tr>
<td>Hosts</td>
<td>This field contains the trusted hosts for which scanning is bypassed. To add a host to this field, use the Add Host field or the Import from File tool (see later in this table). You can add a maximum of 200 hosts.</td>
</tr>
<tr>
<td>Delete</td>
<td>To delete one or more hosts, highlight the hosts, and click the Delete table button.</td>
</tr>
<tr>
<td>Export</td>
<td>To export the hosts, click the Export table button and follow the instructions of your browser.</td>
</tr>
<tr>
<td>Add Host</td>
<td>Type or copy a trusted host in the Add Host field. Then click the Add table button to add the host to the Hosts field.</td>
</tr>
<tr>
<td>Import from File</td>
<td>To import a list with trusted hosts into the Hosts field, click the Browse button and navigate to a file in .txt format that contains line-delimited hosts (that is, one host per line). Then click the Upload table button to add the hosts to the Host field.</td>
</tr>
</tbody>
</table>

**Note:** Any existing hosts in the Hosts field are overwritten when you import a list of hosts from a file.

4. Click **Apply** to save your settings.

**Configuring FTP Scans**

Some malware threats are specifically developed to spread through the FTP protocol. By default, the STM scans FTP traffic, but you can specify how the STM scans FTP traffic and which action is taken when a malware threat is detected.

**Note:** The STM does not scan password-protected FTP files.
To configure the FTP scan settings:

1. Select **Web Security > FTP** from the menu. The FTP screen displays:

   ![FTP Screen](image)

   **Figure 69.**

2. Complete the fields, select the check boxes, and make your selections from the drop-down lists as explained in the following table:

   **Table 38. FTP Scan Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td>From the FTP drop-down list, specify one of the following actions to be taken when an infected FTP file or object is detected:</td>
</tr>
<tr>
<td>FTP</td>
<td><strong>Quarantine file.</strong> The FTP file or object is placed in quarantine, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry.</td>
</tr>
<tr>
<td>FTP</td>
<td><strong>Delete file.</strong> This is the default setting. The FTP file or object is deleted, and depending on the nature of the malware threat, a virus log entry or a spyware log entry is created.</td>
</tr>
<tr>
<td>FTP</td>
<td><strong>Log only.</strong> Depending on the nature of the malware threat, only a virus log entry or a spyware log entry is created. The FTP file or object is not deleted.</td>
</tr>
</tbody>
</table>
ProSecure Web/Email Security Threat Management (STM) Appliance

Table 38. FTP Scan Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Exception</strong></td>
<td></td>
</tr>
<tr>
<td>From the drop-down list, specify one of the following actions to be taken when a file or object exceeds the size that you specify in the file size field:</td>
<td></td>
</tr>
<tr>
<td>• <strong>Skip</strong>. The file or object is not scanned but skipped, leaving the end user vulnerable. This is the default setting.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Block</strong>. The file or object is blocked and does not reach the end user.</td>
<td></td>
</tr>
<tr>
<td>The default and maximum file sizes are as follows:</td>
<td></td>
</tr>
<tr>
<td>• For the STM600 and STM300, the default setting is to block any file or object larger than 10240 KB. The maximum file size that you can specify is 51200 KB.</td>
<td></td>
</tr>
<tr>
<td>• For the STM150, the default setting is to block any file or object larger than 8192 KB. The maximum file size that you can specify is 25600 KB.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong>: Setting the maximum file size to a high value might affect the STM’s performance. NETGEAR recommends the default value, which is sufficient to detect the vast majority of threats.</td>
<td></td>
</tr>
<tr>
<td><strong>Block Files with the Following Extensions</strong></td>
<td></td>
</tr>
<tr>
<td>Select the check box to enable file extension blocking. By default, the File Extension field lists the most common file extensions that are detected. You can manually add or delete extensions. Use commas to separate different extensions.</td>
<td></td>
</tr>
<tr>
<td>You can also use the drop-down list to add predefined file extensions from a specific category to the File Extension field:</td>
<td></td>
</tr>
<tr>
<td>• <strong>None</strong>. No file extensions are added to the File Extension field. This is the default setting.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Executables</strong>. Executable file extensions (exe, com, dll, so, lib, scr, bat, and cmd) are added to the File Extension field.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Audio/Video</strong>. Audio and video file extensions (wav, mp3, avi, rm, rmvb, wma, wmv, mpg, mp4, and aac) are added to the File Extension field.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Compressed Files</strong>. Compressed file extensions (zip, rar, gz, tar, and bz2) are added to the File Extension field.</td>
<td></td>
</tr>
</tbody>
</table>

3. Click **Apply** to save your settings.

**Configuring Application Control**

The STM lets you control user access to Web applications such as instant messaging, media, peer-to-peer services, and online tools. Blocking an application prohibits all traffic to and from the application, which can be useful when you want to control the STM’s throughput. By default, none of the applications are blocked.

**Note**: For information about creating custom categories that allow you to set access exceptions for combinations of applications, see Creating Custom Categories for Web Access Exceptions on page 142.
To enable and configure application control:

1. Select **Application** from the menu. The Application Control screen displays.

   Because of the size of this screen, and because of the way the information is presented, the Application Control screen is divided and presented in this manual in three figures: the following figure shows only the very top part of the screen, **Figure 71** on page 129 shows the Instant Messaging and Media Application sections, and **Figure 72** on page 129 shows the Peer to Peer and Tools sections.

![Application Control, screen 1 of 3](image)

   **Figure 70. Application Control, screen 1 of 3**

2. In the Application Settings section of the screen, select the **Enable Application Control** check box.

3. Under the Application Settings section of the screen, click **Apply**. The configurations of the individual applications can now take effect.

4. For each of the four application sections on the screen—Instant Messaging, Media Applications, Peer to Peer, and Tools—select the **Block** check box to specify to block all applications for that section, or select the individual check boxes to specify to block individual applications.
5. After you have configured each section, first click **Apply** to save the settings before you continue with the next section. You need to save the configuration changes for each section individually.
For reference, you can specify access control for the following applications:

- **Instant Messaging:**
  - Google Talk
  - ICQ
  - mIRC
  - MSN Messenger
  - QQ
  - Yahoo Messenger

- **Media Applications:**
  - iTunes (Music Store, update)
  - Quicktime (Update)
  - Real Player (Guide)
  - Rhapsody (Guide, Music Store)
  - Winamp (Internet Radio/TV)

- **Peer to Peer:**
  - BitTorrent
  - eDonkey
  - Gnutella

- **Tools**
  - Alexa Toolbar
  - GoToMyPC
  - Weatherbug
  - Yahoo Toolbar

### Setting Scanning Exclusions and Web Access Exceptions

After you have specified which IP addresses and ports the STM scans for malware threats, you can set scanning exclusion rules for certain IP addresses and ports. Similarly, after you have specified which content the STM filters, you can set exception rules for users and members of a group.

### Setting Scanning Exclusions

To save resources, you can configure scanning exclusions for IP addresses and ports that you know are secure. For example, if your network includes a Web server that hosts Web pages that are accessible by anyone on the Internet, the files that are hosted by your Web server do not need to be scanned. To prevent the STM from scanning these files, you can configure up to 127 scanning exclusion rules for your Web server.
To configure scanning exclusion rules:

1. Select **Global Settings > Scanning Exclusions** from the menu. The Scanning Exclusions screen displays. This screen shows the Scanning Exclusions table, which is empty if you have not specified any exclusions. (The following figure shows one exclusion rule in the table as an example.)

   ![Scanning Exclusions Screen](image)

   Figure 73.

2. In the Scanning Exclusions section of the screen, specify an exclusion rule as explained in the following table:

   **Table 39. Add Scanning Exclusion Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client IP</td>
<td>The client IP address and optional subnet mask that are excluded from all scanning.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>The destination IP address and optional subnet mask that are excluded from all scanning.</td>
</tr>
<tr>
<td>Port</td>
<td>The number of the port that is excluded from all scanning.</td>
</tr>
<tr>
<td>Brief Description</td>
<td>A description of the exclusion rule for identification and management purposes.</td>
</tr>
</tbody>
</table>

3. In the Add column, click the **Add** table button to add the exclusion rule to the Scanning Exclusions table. The new exclusion rule is enabled by default.

   To disable a rule, select the check box in the Enable column for the rule.

   To delete an exclusion rule from the Scanning Exclusions table, click the **Delete** table button in the Action column to the right of the rule that you want to delete.
Setting Access Exception Rules for Web Access

You can set up to 200 exception rules for users and members of a group to allow access to applications, file extensions and protocols, Web categories, and URLs that you have blocked for all other users, or the other way around, to block access to applications, file extensions and protocols, Web categories, and URLs that you have allowed access to for all other users.

If you have not created a custom group, an exception rule can apply to either one of the following groups or individual users:

- All users
- All authenticated users
- All unauthenticated users
- A local group or local user
- A group or users that is defined by its IP address
- A Lightweight Directory Access Protocol (LDAP) group or LDAP user
- A RADIUS VLAN group

To further refine exception rules, you can create custom groups that allow you to include a combination of local groups and local users, groups and users that are defined by their IP address, LDAP groups and users, and RADIUS groups and users. For more information, see Creating Custom Groups for Web Access Exceptions on page 139.

Note: Users and groups to which access exception rules apply are not the same as LAN groups. For information about how to specify members of a LAN group and to customize LAN group names, see Managing Users, Groups, and Authentication on page 147.

If you have not created a custom category, an exception rule can apply to either one of the following components:

- One built-in application group or built-in individual application
- A combination of file extensions and protocols
- One URL or URL expression
- One built-in Web category group or built-in individual Web category

To further refine exception rules, you can create custom categories that allow you to include either a selection of applications, or a selection of URLs, or a selection of Web categories. For more information, see Creating Custom Categories for Web Access Exceptions on page 142.

Tip: If you want to use a custom group and custom category, first create the custom group and custom category, then create the exception rule.
To set Web access exception rules:

1. Select **Global Settings > Exceptions** from the menu. The Exceptions submenu tabs display, with the Exceptions screen in view. This screen shows the Exceptions table, which is empty if you have not specified any exception rules. (The following figure shows several exception rules in the table as an example.)

![Figure 74.](image)

**Note:** If text in a field of the table exceeds the width of the column, hold the cursor over the field to display the entire text.

2. Under the Exceptions table, click the **Add** table button to specify an exception rule. The Add Exception screen displays:

![Figure 75.](image)
3. Complete the fields and make your selections from the drop-down lists as explained in the following table:

**Table 40. Add Exception Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td>From the drop-down list, select the action that the STM applies:</td>
</tr>
<tr>
<td></td>
<td>• Allow. The exception allows access to an application, Web category, or URL that is otherwise blocked.</td>
</tr>
<tr>
<td></td>
<td>• Block. The exception blocks access to an application, Web category, or URL that is otherwise allowed.</td>
</tr>
<tr>
<td><strong>Domain User/Group</strong></td>
<td>Click the <strong>Edit</strong> button to open the Applies To screen, which lets you configure a domain, group, or individual user to which the exception needs to apply (see the screen later in this table). If applicable, on the Applies To screen, click a <strong>Lookup</strong> button to retrieve a group or user. When you have made your decision, click an <strong>Apply</strong> button to add the domain to the Domain field on the Add Exception screen and the group and user to the User/Group field on the Add Exception screen.</td>
</tr>
<tr>
<td><strong>Note:</strong> The Domain field can remain blank for some special users or groups.</td>
<td></td>
</tr>
<tr>
<td><strong>Following are the options on the Applies To screen.</strong></td>
<td></td>
</tr>
</tbody>
</table>

![Applies To Screen](image-url)
### Table 40. Add Exception Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain User/Group (continued)</td>
<td>Click the <strong>Apply</strong> button to apply the exception to all users, both authenticated and unauthenticated.</td>
</tr>
<tr>
<td>Authenticated</td>
<td>Click the <strong>Apply</strong> button to apply the exception to all authenticated users. These are users who have actively logged in to the STM and who have been authenticated.</td>
</tr>
<tr>
<td>Unauthenticated</td>
<td>Click the <strong>Apply</strong> button to apply the exception to all unauthenticated users. These are users who have not actively logged in to the STM. By default, these users are assigned the account name anonymous.</td>
</tr>
</tbody>
</table>
| Local Groups             | Do the following:  
1. From the Name drop-down list, select a local group.  
2. Click the **Apply** button to apply the exception to the selected local group.  
You can specify local groups on the Groups screen (see Creating and Deleting Groups by Name on page 149). |
| Group Membership by IP   | Do the following:  
1. From the Name drop-down list, select a group that is defined by its IP address.  
2. Click the **Apply** button to apply the exception to the selected group.  
You can specify groups that are defined by their IP address on the IP/Subnet Groups screen (see Creating and Deleting Groups by IP Address and Subnet on page 151). |
| Local User Search        | Do the following:  
1. In the Name field, enter a user name.  
2. Click the **Lookup** button. If the user is found, he or she is listed to the left of the **Apply** button.  
3. Click the **Apply** button to apply the exception to the selected user. |
### Table 40. Add Exception Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain User/Group Search</td>
<td>Do the following:</td>
</tr>
<tr>
<td></td>
<td>1. From the Domain drop-down list, select an LDAP domain.</td>
</tr>
<tr>
<td></td>
<td>2. From the Type drop-down list, select <strong>User</strong>, <strong>Group</strong>, or <strong>User&amp;Group</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. In the Name field, enter the name of the user, group, or user and group, or leave this field blank.</td>
</tr>
<tr>
<td></td>
<td>4. Click the <strong>Lookup</strong> button. If the user or group is found, it is listed to the left of the <strong>Apply</strong> button. If you left the Name field blank, all users, groups, or users and groups are listed; in this case, make a selection.</td>
</tr>
<tr>
<td></td>
<td>5. Click the <strong>Apply</strong> button to apply the exception to the selected user or group.</td>
</tr>
<tr>
<td></td>
<td>You can specify LDAP domains, groups, and users on the LDAP screen (see <em>Creating and Deleting LDAP and Active Directory Domains</em> on page 161).</td>
</tr>
<tr>
<td>RADIUS User</td>
<td>Do the following:</td>
</tr>
<tr>
<td></td>
<td>1. From the Domain drop-down list, select a RADIUS domain.</td>
</tr>
<tr>
<td></td>
<td>2. From the VLAN ID/Name drop-down list, select a VLAN ID or VLAN name.</td>
</tr>
<tr>
<td></td>
<td>3. Click the <strong>Apply</strong> button to apply the exception to the selected VLAN.</td>
</tr>
<tr>
<td></td>
<td>You can specify RADIUS domains and VLANs on the RADIUS screen (see <em>Creating and Deleting RADIUS Domains</em> on page 167).</td>
</tr>
<tr>
<td>Custom Groups</td>
<td>Do the following:</td>
</tr>
<tr>
<td></td>
<td>1. From the Name drop-down list, select a custom group.</td>
</tr>
<tr>
<td></td>
<td>2. Click the <strong>Apply</strong> button to apply the exception to the selected group.</td>
</tr>
<tr>
<td></td>
<td>You can specify custom groups on the Custom Groups screen (see <em>Creating Custom Groups for Web Access Exceptions</em> on page 139).</td>
</tr>
<tr>
<td>Start Time</td>
<td>The time in 24-hour format (hours and minutes) when the action starts. If you leave these fields empty, the action applies continuously.</td>
</tr>
<tr>
<td>End Time</td>
<td>The time in 24-hour format (hours and minutes) when the action ends. If you leave these fields empty, the action applies continuously.</td>
</tr>
</tbody>
</table>
Table 40. Add Exception Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category (and related information)</td>
<td>From the Category drop-down list, select the category to which the action applies. Your selection determines which drop-down lists, fields, radio buttons, and check boxes display onscreen.</td>
</tr>
<tr>
<td>Applications</td>
<td>The action applies to an application. Select an application from the Sub Category drop-down list. For information about custom application categories, see Creating Custom Categories for Web Access Exceptions on page 142.</td>
</tr>
<tr>
<td>File Extensions</td>
<td>The action applies to one or more file extensions and one or more protocols. The following field and check boxes display on screen:</td>
</tr>
<tr>
<td></td>
<td>• <strong>File Extensions</strong>. Manually enter up to 40 file extensions. Use commas to separate multiple file extensions. Wildcards (<em>) are supported. A single asterisk (</em>) matches any file extension. You can also use the drop-down list to the right of the File Extension field to automatically add file extensions from the following categories:</td>
</tr>
<tr>
<td></td>
<td>- <strong>None</strong>. No file extensions are added to the File Extension field. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Executables</strong>. Executable file extensions (exe, com, dll, so, lib, scr, bat, and cmd) are added to the File Extension field.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Audio/Video</strong>. Audio and video file extensions (wav, mp3, avi, rm, rmvb, wma, wmv, mpg, mp4, and aac) are added to the File Extension field.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Compressed Files</strong>. Compressed file extensions (zip, rar, gz, tar, and bz2) are added to the File Extension field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Protocols</strong>. Select one or multiple check boxes to specify which protocols the action applies to:</td>
</tr>
<tr>
<td></td>
<td>- SMTP</td>
</tr>
<tr>
<td></td>
<td>- POP3</td>
</tr>
<tr>
<td></td>
<td>- IMAP</td>
</tr>
<tr>
<td></td>
<td>- HTTP</td>
</tr>
<tr>
<td></td>
<td>- HTTPS</td>
</tr>
<tr>
<td></td>
<td>- FTP</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>The action applies to a URL. The following field and drop-down list display onscreen. Select a radio button to either enter a URL expression or select a custom URL list.</td>
</tr>
<tr>
<td></td>
<td>• <strong>URL Expression</strong>. Enter a URL or URL expression such as &quot;video&quot; or &quot;chat&quot;. Wildcards (*) are supported. The maximum supported size of the URL or URL expression is 1024 bytes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Custom URL List</strong>. Select a custom URL list from the Sub Category drop-down list. For information about custom URL lists, see Creating Custom Categories for Web Access Exceptions on page 142.</td>
</tr>
</tbody>
</table>
4. Click **Apply** to save your settings. The new exception rule is added to the Exceptions table. To return to the Exception screen without adding the rule, click **Return**.

5. Select the check box to the left of the rule that you want to enable, or click the **Select All** table button to select all rules.

6. Click the **Enable** table button to enable the selected rule or rules.

---

**Note:** Enabled exception rules are preceded by a green circle in the ! column; disabled exception rules are preceded by a gray circle in the ! column.

---

**To make changes to an existing exception rule:**

1. In the Action column to the right of the exception rule, click the **Edit** table button. The Edit Exception screen displays. This screen is identical to the Add Exception screen (see Figure 74 on page 133).

2. Modify the settings that you wish to change (see the previous table).

3. Click **Apply** to save your changes. The modified exception rule is displayed in the Exceptions table.

**To delete or disable one or more exception rules:**

1. Select the check box to the left of the rule that you want to delete or disable, or click the **Select All** table button to select all rules.

2. Click one of the following table buttons:
   - **Disable.** Disables the rule or rules. The ! status icon changes from a green circle to a gray circle, indicating that the rule is or rules are disabled. (By default, when a rule is added to the table, it is automatically enabled.)
   - **Delete.** Deletes the rule or rules.

The table rank of the exception rule in the Exceptions table determines the order in which the rule is applied (from the top down). To change the position of the rules in the table, select one or more a rules, and then click one of the following table buttons:

- **Up.** Moves the rule or rules up one position in the table rank.
- **Down.** Moves the rule or rules down one position in the table rank.

---

**Table 40. Add Exception Settings (Continued)**

<table>
<thead>
<tr>
<th>Setting (and related information)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category Web Categories (continued)</td>
<td>The action applies to a Web category. Select a Web category from the Sub Category drop-down list. For information about custom Web categories, see Creating Custom Categories for Web Access Exceptions on page 142.</td>
</tr>
<tr>
<td>Note</td>
<td>A description of the exception rule for identification and management purposes or any other relevant information that you wish to include.</td>
</tr>
</tbody>
</table>
Creating Custom Groups for Web Access Exceptions

After you have specified groups and users (see Managing Users, Groups, and Authentication in Chapter 5), you can create up to 200 custom groups, each of which can include a combination of local groups and local users, groups and users that are defined by their IP address, LDAP groups and users, and RADIUS groups and users. You use these custom groups to set Web access exceptions on the Exceptions screen (see Setting Access Exception Rules for Web Access on page 132).

To create and manage custom groups:

1. Select Global Settings > Exceptions from the menu. The Exceptions submenu tabs display, with the Exceptions screen in view.
2. Click the Custom Groups submenu tab. The Custom Groups screen displays. This screen shows the Custom Groups table, which is empty if you have not specified any custom groups. (The following figure shows one custom group in the table as an example.)

![Custom Groups Table](image)
3. Under the Custom Groups table, click the **Add** table button to specify a custom group. The Add Custom Group screen displays:

![Add Custom Group Screen](image)

Figure 77.

4. Complete the fields and make your selections from the drop-down lists as explained in the following table:

**Table 41. Add Custom Group Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name of the custom group for identification and management purposes.</td>
</tr>
<tr>
<td>Brief Description</td>
<td>A description of the custom group for identification and management purposes.</td>
</tr>
<tr>
<td>Members in this group</td>
<td>When you click the <strong>Add</strong> button in the Add Users/Groups to this group section of the screen, the selected member is added to this field. You can add multiple members. To remove a member, highlight the member in this field, and then click the <strong>Delete</strong> button.</td>
</tr>
</tbody>
</table>
### Table 41. Add Custom Group Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Add Users/Groups to this group** | **Local Groups** Do the following:  
1. From the Name drop-down list, select a local group.  
2. Click the **Add** button to add the selected local group to the custom group. Repeat this step to add more local groups to the custom group.  
You can specify local groups on the Groups screen (see *Creating and Deleting Groups by Name* on page 149). |
| **Group Membership by IP**        | **Do the following:**  
1. From the Name drop-down list, select a group that is defined by its IP address.  
2. Click the **Add** button to add the selected group to the custom group. Repeat this step to add more users or groups, or both, to the custom group.  
You can specify groups that are defined by their IP address on the IP/Subnet Groups screen (see *Creating and Deleting Groups by IP Address and Subnet* on page 151). |
| **Local User Search**             | **Do the following:**  
1. In the Name field, enter a user name.  
2. Click the **Lookup** button. If the user is found, he or she is listed to the left of the Apply button.  
3. Click the **Add** button to add the selected local user to the custom group. Repeat this step to add more local users to the custom group. |
| **LDAP User/Group Search**        | **Do the following:**  
1. From the Domain drop-down list, select an LDAP domain.  
2. From the Type drop-down list, select **User**, **Group**, or **User&Group**.  
3. In the Name field, enter the name of the user, group, or user and group, or leave this field blank.  
4. Click the **Lookup** button. If the user or group is found, it is listed to the left of the Add button. If you left the Name field blank, all users, groups, or users and groups are listed. In this case, make a selection.  
5. Click the **Add** button to add the selected user or group to the custom group. Repeat this step to add more users or groups, or both, to the custom group.  
You can specify LDAP domains, groups, and users on the LDAP screen (see *Creating and Deleting LDAP and Active Directory Domains* on page 161). |
Table 41. Add Custom Group Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Users/Groups to this group (continued)</td>
<td>RADIUS User</td>
</tr>
</tbody>
</table>

5. After you have specified all members of the custom group, click Apply to save your settings. The new custom group is added to the Custom Groups table. To return to the Custom Groups screen without adding the group, click Return.

To make changes to an existing custom group:

1. In the Action column to the right of to the custom group, click the Edit table button. The Edit Custom Group screen displays. This screen is identical to the Add Custom Group screen (see Figure 77 on page 140).
2. Modify the settings that you wish to change (see the previous table).
3. Click Apply to save your changes. The modified custom group is displayed in the Custom Groups table.

To delete one or more custom groups:

1. Select the check box to the left of the custom group that you want to delete, or click the Select All table button to select all custom groups.
2. Click the Delete table button.

Creating Custom Categories for Web Access Exceptions

Use custom categories to set Web access exceptions on the Exceptions screen (see Setting Access Exception Rules for Web Access on page 132). Custom categories can include a selection of applications, or a selection of URLs, or a selection of Web categories, but no combination of applications, URLs, and Web categories. You can create up to 200 custom categories.
To create and manage custom categories:

1. Select **Global Settings > Exceptions** from the menu. The Exceptions submenu tabs display, with the Exceptions screen in view.

2. Click the **Custom Categories** submenu tab. The Custom Categories screen displays. This screen shows the Custom Categories table, which is empty if you have not specified any custom categories. (The following figure shows three custom categories in the table as an example.)

![Custom Categories Table](image)

**Figure 78.**

3. Under the Custom Categories table, click the **Add** table button to specify a custom category. The Add Custom Category screen displays. The nature of the screen depends on your selection from the Category Type drop-down list, which is set by default to Applications (this selection is shown in the following figure). The URL Filtering and Web Categories settings are shown in **Figure 80** on page 144 and **Figure 81** on page 144 respectively.

![Add Custom Category](image)

**Figure 79.** Category Type: Applications
Figure 80. Category Type: URL Filtering

Figure 81. Category Type: Web Categories
4. Complete the fields and make your selections from the drop-down lists as explained in the following table:

**Table 42. Add Custom Category Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name of the custom category for identification and management purposes.</td>
</tr>
<tr>
<td>Brief Description</td>
<td>A description of the category group for identification and management purposes.</td>
</tr>
<tr>
<td>Category Type</td>
<td>From the Category Type drop-down list, select the type of category that you want to create. Your selection determines the nature of the screen.</td>
</tr>
</tbody>
</table>
| Applications     | Use the move buttons to move entire application categories (for example, Instant Messaging), individual applications (for example, Instant Messaging - Google Talk), or combinations of both from the Applications outside this Category field to the Applications in this Category field (or the other way around). These are the functions of the move buttons:  
• < or > moves one or more highlighted selections from one field to the other.  
• << or >> moves all entries from one field to the other. |
| URL Filtering    | URLs in this Category field:  
This field contains the URLs that are added to the custom category. To add a URL to this field, use the Add URL field or the Import from File tool (see explanations later in this table). You can add a maximum of 2000 URLs.  

*Note:* Wildcards (*) are supported. For example, if you enter www.net*.com in the Add URL field and then click the Add table button, any URL that begins with www.net and ends with .com is included in the custom category.  
These are the functions of the table buttons to the right of the field:  
• **Delete**. To delete one or more URLs, highlight the URLs, and click the Delete table button.  
• **Export**. To export the URLs, click the Export table button, and follow the instructions of your browser.  
Add URL field:  
Type or copy a URL in the Add URL field. Then click the Add table button to add the URL to the URLs in this Category field.  
Import from File field:  
To import a list with URLs into the URLs in this Category field, click the Browse button and navigate to a file in .txt format that contains line-delimited URLs (that is, one URL per line). Then click the Upload table button to add the URLs to the URLs in this Category field.  

*Note:* Any existing URLs in the URLs in this Category field are overwritten when you import a list of URLs from a file.
5. Click **Apply** to save your settings. The new category is added to the Custom Categories table. To return to the Custom Categories screen without adding the category, click **Return**.

**To make changes to an existing custom category:**

1. In the Action column to the right of the custom category, click the **Edit** table button. The Edit Custom Category screen displays. This screen is identical to the Add Custom Category screen (see **Figure 77** on page 140).
2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified custom group is displayed in the Custom Categories table.

**To delete one or more custom categories:**

1. Select the check box to the left of the custom category that you want to delete, or click the **Select All** table button to select all custom categories.
2. Click the **Delete** table button.
This chapter describes how to manage users, groups, and authentication on the STM. This chapter contains the following sections:

- **About Users, Groups, and Domains** on this page
- **Configuring Groups** on page 148
- **Configuring User Accounts** on page 152
- **Configuring Authentication** on page 154
- **Global User Settings** on page 170
- **Viewing and Logging Out Active Users** on page 172

**About Users, Groups, and Domains**

Users can be individual users or can be part of a group, and a group is generally part of a domain. Normally, you first create a domain, then you create a group that you assign to a domain, and then you create users that you assign to a group. The STM does not let you create domains; the local groups that you define are automatically assigned to the STM’s prosecuredomain default domain. However, you can use existing LDAP and RADIUS domains on the STM.

The main purpose for using groups and domains is to apply exceptions (that is, adding or removing restrictions) for Web browsing, URL access, and application access (see **Setting Access Exception Rules for Web Access** on page 132).

**Note:** For information about a different type of users—those with administrative and guest privileges—see **About Users with Administrative and Guest Privileges** on page 61.
The STM supports both unauthenticated and authenticated users:

- **Unauthenticated users.** Anonymous users who do not log in to the STM and to which the STM’s default email and Web access policies apply.
- **Authenticated users.** Users who have a computer behind the STM, who log in to the STM with a user name and password, and who are assigned an access policy that normally differs from the STM’s default email and Web access policies. Different users or user groups can have different access policies, so there can be multiple access policies on the STM.

In addition to being authenticated as individual users, users can be authenticated on the STM according to group membership or IP address:

- **Group membership.** A group is defined in the STM’s local database, an LDAP database, or a RADIUS database. If you use a RADIUS database for authentication, a group can also be defined in a VLAN.
- **IP address.** A group is defined by its IP address and subnet.

**Note:** For detailed information about authentication, see Configuring Authentication on page 154.

The login window that is presented to this type of users is the User Portal Login screen (see Figure 88 on page 156), which requires three items: a user name, a password, and a domain selection. The domain determines the authentication method that needs to be used—LDAP, Active Directory, RADIUS, or the STM’s local database.

### Configuring Groups

The use of groups simplifies the application of exception policies that allow different sets of users to have different Internet access restrictions. Rather than applying the same exception to each user, it is easier to apply a single exception to the entire group. For information about exception policies, see Setting Access Exception Rules for Web Access on page 132.

**Note:** For information about custom groups that allow you to set access exceptions for a combination of local groups and local users, groups and users that are defined by their IP address, LDAP groups and users, and RADIUS groups and users, see Creating Custom Groups for Web Access Exceptions on page 139.
You can define groups either by name or by IP address and subnet:

- **Groups defined by name.** These are local groups on the STM to which you can add users from the STM’s local user database. Local groups are automatically assigned to the STM’s prosecredomain default domain.

  **Note:** For information about groups that are defined by VLANs, see Creating and Deleting VLANs for Use with RADIUS Domains on page 170.

- **Groups defined by IP address and subnet.** These are groups that can be on your local network or on a remote device.

  **Note:** If you use groups on a remote device, you need to configure your network’s firewall to allow access to the IP address and subnet mask that have been assigned to the remote group.

### Creating and Deleting Groups by Name

**To create a local group by name:**

1. Select **User Management > Groups** from the menu. The Groups screen displays. (The following figure contains one example.)

   ![Figure 82](image)

   The List of Groups table displays the local groups with the following fields:
   - **Name.** The name of the group, which is the defining characteristic of the group.
   - **Brief Description.** An optional brief description of the group.
   - **Action.** The Edit table button, which provides access to the Edit Group screen, and the Delete table button, which allows you to delete the group.
2. In the Add New Group section of the screen, complete the fields as explained in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A descriptive (alphanumeric) name of the group for identification and management purposes.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the group for identification and management purposes. This description is optional.</td>
</tr>
</tbody>
</table>

Table 43. Group Settings

3. Click the Add table button. The new group is added to the List of Groups table.

To delete a group from the List of Groups table, click the Delete table button in the Action column for the group that you want to delete.

**Note:** When you delete a group, an exception rule that is associated with this group no longer has any effect. You can delete such an exception rule.

**Editing Groups by Name**

**To edit a local group that you created by name:**

1. Select User Management > Groups from the menu. The Groups screen displays (see the previous figure).

2. In the Action column of the List of Groups table, click the Edit table button for the group that you want to edit. The Edit Group screen displays. (The following figure contains some examples.)

Figure 83.
3. Change the field and move the users as explained in the following table:

Table 44. Edit Group Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Description</td>
<td>You can edit the brief description of the group for identification and management purposes.</td>
</tr>
</tbody>
</table>

Use the move buttons to move all users or only selected users from the Local users field to the Users in this group field (or the other way around).

These are the functions of the move buttons:
- < or > moves one or more highlighted selections from one field to the other.
- << or >> moves all entries from one field to the other.

4. Click **Apply** to save your changes.

Creating and Deleting Groups by IP Address and Subnet

To create a group by IP address and subnet:

1. Select **User Management > IP Subnet/Groups** from the menu. The IP Subnet/Groups screen displays. (The following figure contains one example.)

![IP Subnet/Groups Screen](image)

Figure 84.

The Groups Membership by IP Address table displays the groups with the following fields:
- **IP Address.** The IP address for the group.
- **Netmask.** The subnet mask for the group.
- **Name.** The name of the group.
- **Action.** The Delete table button, which allows you to delete the group.
2. In the Add New IP Subnets/Groups section of the screen, complete the fields as explained in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>An IP address on your local network or on a remote device to which the users are assigned.</td>
</tr>
<tr>
<td>Netmask</td>
<td>The subnet mask to which the users are assigned. For an individual IP address, specify 255.255.255.255.</td>
</tr>
<tr>
<td>Name</td>
<td>A descriptive (alphanumeric) name of the group for identification and management purposes.</td>
</tr>
</tbody>
</table>

3. Click the **Add** table button. The new group is added to the Groups Membership by IP Address table.

To delete a group from the List of Groups table, click the **Delete** table button in the Action column for the group that you want to delete.

**Note:** When you delete a group, an exception rule that might be associated with this group no longer has any effect. You can delete such an exception rule.

### Configuring User Accounts

When you create a user account, you can assign the user to a local group. Therefore, you should first create any local groups, then user accounts. User accounts are added to the STM’s local user database.
Creating and Deleting User Accounts

To create an individual user account:

1. Select **Users > Users** from the menu. The Users screen displays:

![Users Screen](image).

The List of Users table displays the users with the following fields:

- **Enable**: The check box allows you to enable or disable the user.
- **Name**: The name of the user.
- **Group**: The group to which the user is assigned. If no group is displayed, the user is not assigned to any group.
- **Action**: The Edit table button, which provides access to the Edit User screen, and the Delete table button, which allows you to delete the user.

2. In the Add New Users section of the screen, complete the fields, make your selection from the drop-down list, and select the radio buttons as explained in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A descriptive (alphanumeric) name of the user for identification and management purposes.</td>
</tr>
<tr>
<td>Groups</td>
<td>The drop-down list shows the local groups that are listed on the Groups screen. From the drop-down list, select the group to which the user is assigned. For information about how to configure groups, see <strong>Configuring Groups</strong> on page 148.</td>
</tr>
</tbody>
</table>
| Password | Select one of the following radio buttons:  
  - The radio button to the left of the Password field. Enter the password that the user needs to enter to gain access to the STM. The password can be up to 64 characters.  
  - **Use username as the password**. The password that is assigned to the user is identical to the user name. |
3. Click the Add table button. The new user is added to the List of Users table.
To delete a user from the List of Users table, click the Delete table button in the Action column for the user that you want to delete.

**Editing User Accounts**

The only field that you can change for a user account is the password.

To modify the password for a user:

1. Select Users > Users from the menu. The Users screen displays (see the previous figure).
2. Click the Edit table button in the Action column for the user whose password you want to modify. The Edit User screen displays. (The following figure contains an example.)

![Edit User Screen](image)

**Figure 86.**

3. Modify the password:
   a. In the Password field, enter the new password.
   b. In the Confirm Password field, repeat the new password.
4. Click Apply to save your settings.

**Configuring Authentication**

The authentication options of the STM are discussed in the following sections:

- *Understanding the STM’s Authentication Options* on page 155
- *Understanding Active Directories and LDAP Configurations* on page 157
- *Creating and Deleting LDAP and Active Directory Domains* on page 161
- *Editing LDAP and Active Directory Domains* on page 164
- *Understanding the ProSecure DC Agent* on page 164
- *Requirements for the ProSecure DC Agent Software and DC Agent Server* on page 165
Understanding the STM’s Authentication Options

The login screen and authentication on the STM depend on the user type. There are two basic user types on the STM that are explained in the following sections:

- Administrative users and users with guest privileges
- Users with special access privileges

**Administrative Users and Users with Guest Privileges**

Users with administrative and guest privileges on the STM need to log in through the NETGEAR Configuration Manager Login screen (see the following figure), where they are authenticated through the STM’s local user database. These users need to provide their user name and password.

For information about the predefined administrator and guest user accounts, see About Users with Administrative and Guest Privileges on page 61. For information about how to change the administrator default name and password or guest default name and password, see Changing Administrative Passwords and Timeouts on page 62.

![NETGEAR Configuration Manager Login](image)

**Figure 87.**

**Users with Special Access Privileges**

Users who have a computer behind the STM and who are assigned access policies that differ from the STM’s default email and Web access policies (see Setting Access Exception Rules for Web Access on page 132) need to log in through the User Portal Login screen (see the following figure). These users need to provide their user name and password, and select the domain to which they have been assigned.
The lower part of the NETGEAR Configuration Manager Login screen (see the previous figure) provides a User Portal Login Link that lets you open the User Portal Login screen:

![User Portal Login](image)

**Figure 88.**

After a user has logged in through the User Portal Login screen, the Authentication screen displays:

![Authentication](image)

**Figure 89.**

The Authentication screen shows the IP address with which the user has logged in and lets a user change his or her password.

If you do not use the DC agent in your configuration (see *Understanding the ProSecure DC Agent* on page 164), after completing a session, a user needs to log out by following these steps:

1. Return to the User Portal Login screen (see *Figure 88*).

   **Note:** The user needs to know how to return to the User Portal Login screen. The administrator needs to provide the User Portal Login URL:

   *https://<IP_address>/~common/cgi-bin/user_login.pl* or
   *https://<FullyQualifiedDomainName>/~common/cgi-bin/user_login.pl*

   Alternately, the administrator can provide the NETGEAR Configuration Manager Login screen, from which the user can access the User Portal Login screen: *https://<IP_address>* or *https://<FullyQualifiedDomainName>*
2. Log in again.
3. On the Authentication screen (see the previous figure), click the Logout link.

WARNING!
Ensure that users understand that they need to log out after completing a session in order to prevent subsequent users from inheriting access privileges that were not assigned to them.

In addition to authentication through the STM’s local user database, the STM supports the following external authentication methods for users logging in through the User Portal Login screen:

- **LDAP.** A network-validated domain-based authentication method that functions with a Lightweight Directory Access Protocol (LDAP) authentication server. LDAP is a standard for querying and updating a directory. Because LDAP supports a multilevel hierarchy (for example, groups or organizational units), this information can be queried to provide specific group policies or bookmarks based on LDAP attributes.

- **Active Directory.** A network-validated domain-based authentication method that functions with a Microsoft Active Directory authentication server. Microsoft Active Directory authentication servers support a group and user structure. Because the Active Directory supports a multilevel hierarchy (for example, groups or organizational units), this information can be queried to provide specific group policies or bookmarks based on Active Directory attributes. A Microsoft Active Directory database uses an LDAP organization schema.

- **RADIUS.** A network-validated PAP or CHAP password-based authentication method that functions with Remote Authentication Dial In User Service (RADIUS).

  RADIUS supports two types of protocols:

  - **PAP.** Password Authentication Protocol (PAP) is a simple protocol in which the client sends a password in clear text.

  - **CHAP.** Challenge Handshake Authentication Protocol (CHAP) executes a three-way handshake in which the client and server trade challenge messages, each responding with a hash of the other’s challenge message that is calculated using a shared secret value.

When logging in through the User Portal Login screen, users need to provide their name and password, and select the domain that corresponds to the authentication method that has been assigned to them.

**Understanding Active Directories and LDAP Configurations**

This manual assumes that you already have a knowledge of Active Directories and LDAP servers. The following sections are meant to provide some additional information before you go to *Creating and Deleting LDAP and Active Directory Domains* on page 161.
**How an Active Directory Works**

Understanding how a typical Active Directory (AD) works might be of help when you are specifying the settings for the LDAP and Active Directory domains on the STM.

The following applies to a typical AD:

- Organizational unit (OU), common name (CN), and domain controller (DC) can all be used to build a search base in the AD. The following applies to the OU and CN containers:
  - An AD administrator can create an OU but cannot create a CN that was built in the AD server.
  - An AD administrator can apply a global policy object (GPO) to an OU but not to a CN.
- An OU is created in the root node (for example, dc=companyname, dc=com) of the hierarchy. In a company AD, an OU often represents a regional office or department.
- A group is created under cn=users.
- A user is created under each OU so that the user can logically show in a tree of the AD server.
- A relationship between a group and users is built using their attributes (by default: member and memberOf). These show in a lookup result.

The following is an example of how to set the search base:

If in a company AD server “cn=users” and “ou=companyname” and both are specified under “dc=companyname,dc=com,” the search base needs to be set as “dc=companyname,dc=com” in order for the STM to search both users and groups.

If the size limit is exceeded so that “dc=companyname,dc=com” misses some entries during the lookup process, a user can still be correctly authenticated. However, to prevent the size limit from being exceeded, an AD administrator needs to set a larger value in the LDAP server configuration so that the entire list of users and groups is returned in the lookup result. Another workaround is to use a specific search name or a name with a wildcard in the lookup process, so that the subset of the entire list is returned in the lookup result.

**How to Bind a Distinguished Name in an LDAP Configuration**

Understanding how to bind a distinguished name (DN) in an LDAP configuration might be of help when you are specifying the settings for the LDAP and Active Directory domains on the STM.

To bind a user with the name Jamie Hanson with the LDAP server:

1. On a computer that has access to the Active Directory (AD), open the Active Directory for Users and Computers.
2. Select the user Jamie Hanson.
3. Click the **General** tab. The general properties for Jamie Hanson display:

![Figure 90. Jamie Hanson Properties](image)

4. To verify Jamie Hanson’s user login name, click the **Account** tab. The account properties for Jamie Hanson display:

![Figure 91. Jamie Hanson Properties](image)

5. Log in to the STM.

6. Select **User Management > Authentications** from the menu. The LDAP screen displays.
7. In the List of LDAP table, click the **Edit** button in the Action column of domain ABC.com. The Edit LDAP screen displays.

8. To bind the user Jamie Hanson to the LDAP server for authentication on the STM, use one of the following two formats in the Bind DN field of the Edit LDAP screen:
   - The display name in DN format:
     
     \[\text{cn=Jamie Hanson,cn=users,dc=testAD,dc=com}\] (see the example in the following figure).

   ![Figure 92.](image)

   - The Windows account name in email format such as jhanson@testAD.com. (The following figure shows only the Bind DN field.)

   ![Figure 93.](image)

9. Click **Test** to verify that the LDAP server can actually function with the bind DN that you have modified. The automated test procedure checks the connection to the LDAP server, the bind DN, and the bind password. If any settings require changes, you are notified at the end of the automated test procedure.

10. Click **Apply** to save your settings.
Creating and Deleting LDAP and Active Directory Domains

To configure LDAP and Active Directory authentication:

1. Select **User Management > Authentication** from the menu. The authentication submenu tabs display with the LDAP screen in view:

![Figure 94. The List of LDAP table displays the following fields:](image)

The List of LDAP table displays the following fields:

- **Domain Name.** The name of the STM’s domain to which the server has been assigned.
- **Server.** The IP address of the LDAP or Active Directory server.
- **Action.** The Edit table button, which provides access to the Edit LDAP screen, and the Delete table button, which allows you to delete the LDAP or Active Directory server.
2. Complete the fields and make your selections from the drop-down list as explained in the following table:

Table 47. LDAP Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>A descriptive (alphanumeric) name of the LDAP or Active Directory authentication server for identification and management purposes.</td>
</tr>
<tr>
<td>Server</td>
<td>The server IP address or server host name of the LDAP or Active Directory authentication server.</td>
</tr>
<tr>
<td>Encryption</td>
<td>From the drop-down list, select the encryption type for the connection between the STM and the LDAP or Active Directory server:</td>
</tr>
<tr>
<td></td>
<td>• None. The connection is not encrypted. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• TLS. The connection uses Transport Layer Security (TLS) encryption.</td>
</tr>
<tr>
<td></td>
<td>• SSL. The connection uses Secure Socket Layer (SSL) encryption.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number for the LDAP or Active Directory authentication server. The default port for the LDAP server is 389, which is generally the default port for TLS encryption or no encryption. When the encryption is SSL, the default port is generally 636.</td>
</tr>
<tr>
<td>Bind DN</td>
<td>The LDAP or Active Directory bind distinguished name (DN) that is required to access the LDAP or Active Directory authentication server. This bind DN needs to be a user in the LDAP or Active Directory directory that has read access to all the users that you would like to import into the STM. The Bind DN field accepts two formats:</td>
</tr>
<tr>
<td></td>
<td>• A display name in the DN format. For example:</td>
</tr>
<tr>
<td></td>
<td>cn=Jamie Hanson,cn=users,dc=test,dc=com.</td>
</tr>
<tr>
<td></td>
<td>• A Windows login account name in email format. For example:</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:jhanson@testAD.com">jhanson@testAD.com</a>. This last type of bind DN can be used only for a Windows Active Directory server.</td>
</tr>
<tr>
<td>Bind Password</td>
<td>The authentication secret or password that is required to access the LDAP or Active Directory authentication server.</td>
</tr>
<tr>
<td>Search Base</td>
<td>The distinguished name (DN) at which to start the search, specified as a sequence of relative distinguished names (rdn), connected with commas and without any blank spaces. For most users, the search base is a variation of the domain name. For example, if your domain is yourcompany.com, your search base DN might be as follows: dc=yourcompany,dc=com.</td>
</tr>
<tr>
<td>UID Attribute</td>
<td>The attribute in the LDAP directory that contains the user’s identifier (uid). For an Active Directory, enter sAMAccountName. For an OpenLDAP directory, enter uid.</td>
</tr>
<tr>
<td>Member Groups Attribute</td>
<td>This field is optional. The attribute that is used to identify the groups an entry belongs to. For an Active Directory, enter memberOf. For OpenLDAP, you can enter a customized attribute to identify the groups of an entry.</td>
</tr>
</tbody>
</table>
3. Click **Test** to verify that the LDAP server can actually function with the LDAP settings that you have specified. The automated test procedure checks the connection to the LDAP server; the bind DN, and the bind password. If any settings require changes, you are notified at the end of the automated test procedure.

**Note:** If the automated test procedure returns the message “LDAP server test passed but size limit exceeded,” only a limited number of entries (for example, 1000) was returned after the LDAP server was queried. To ensure that the lookup results include all users and groups, set larger values in the LDAP server. Another workaround is to use a specific search name or a name with a wildcard in the lookup process, so that the subset of the entire list is returned in the lookup result.

4. Click **Add** to save your settings. The LDAP or Active Directory domain and server are added to the List of LDAP table.

To delete a domain and server from the List of LDAP table, click the **Delete** table button in the Action column for the domain and server that you want to delete.

**WARNING!**

After their sessions have expired, users can no longer log in to the STM if the domain that has been assigned to them is the domain that you deleted.
Editing LDAP and Active Directory Domains

To edit an LDAP or Active Directory domain:

1. Select User Management > Authentication from the menu. The authentication submenu tabs display with the LDAP screen in view (see Figure 94 on page 161).
2. In the Action column of the List of LDAP table, click the Edit table button for the domain and server that you want to edit. The Edit LDAP screen displays. This screen contains the same fields as the LDAP screen (see Figure 94 on page 161).
3. Modify the fields and make your selections from the drop-down list as explained in Table 47 on page 162.
4. Click Test to verify that the LDAP server can actually function with the LDAP settings that you have modified. The automated test procedure checks the connection to the LDAP server, the bind DN, and the bind password. If any settings require changes, you are notified at the end of the automated test procedure.
5. Click Apply to save your settings.

Understanding the ProSecure DC Agent

If you set up an open network, you would want to allow unauthenticated users to surf anonymously. For a secure network, you would use a more restrictive access policy for unauthenticated users and a less restricted access policy for authenticated users.

Without the use of the DC agent, any LDAP domain user surfs anonymously until providing credentials to the STM in order to proceed past a blocked Web activity. With use of the DC agent, LDAP domain users are immediately known to the STM when they are authenticated on a DC server on which the DC agent is installed.

If the LDAP directory authenticates through a domain controller (DC) server that runs Windows Server 2003 with Service Pack 1 (SP1) or Windows Server 2008, you can use the ProSecure DC Agent software to authenticate LDAP domain users.

The DC agent monitors all Windows login events (that is, all LDAP domain user authentications) on the DC server, and provides a mapping of Windows user names and IP addresses to the STM, enabling the STM to transparently apply user policies. The DC agent transfers encrypted names, IP addresses, groups, and login times of the users logged in to the STM, where this information remains securely (that is, it is not transferred out of the STM).
Requirements for the ProSecure DC Agent Software and DC Agent Server

Note the following requirements for the ProSecure DC agent software and domain controller (DC) servers:

• If the DC server is located behind a firewall or there is a firewall on the DC server, ensure that the firewall does not block the server's listening port. The default port that is used by the DC agent is 5182.

• The DC agent needs to be able to automatically log an account login event when a domain user account is authenticated against the LDAP directory on a DC server. Verify that the DC server has the following configuration:
  - The Audit Logon Events policy is defined and the Success check box is selected.
  - The Audit Account Logon Events policy is defined and the Success check box is selected.
  - The Audit Account Management policy is defined and the Success check box is selected.

  In addition, if you change the log path of the security log, restart the DC server to bring the change into effect.

• If you use the ProSecure DC Agent software on a DC server that is running Windows Server 2003, ensure that Windows Security Log settings in the Event Viewer are set to the maximum size of 16 MB and to overwrite events as needed.

Downloading ProSecure DC Agent Software, and Creating and Deleting DC Agents

When new ProSecure DC Agent software is available, the STM automatically downloads the software from the update server and notifies administrative users in several ways:

• The STM sends an email to administrative users.
• The STM records a syslog entry.
• The STM generates a notification screen that is presented to administrative users upon login.
To download ProSecure DC Agent software and add a DC agent:

1. Select **User Management > Authentication** from the menu. The authentication submenu tabs display with the LDAP screen in view. Locate the List of DC Agents table at the bottom of the screen. (See this section of the screen in the following figure.)

![List of DC Agent screen](image)

2. Under the List of DC Agents table, click the **Download/Install** link to download the ProSecure DC Agent software. Follow the instructions of your browser to save the software file to your computer.

3. Install the ProSecure DC Agent software on each domain controller (DC) server through which the LDAP directory authenticates users.

4. Complete the fields and make your selections from the drop-down lists as explained in the following table:

   **Table 48. DC Agent Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>From the Domain drop-down list, select an LDAP domain to bind with the DC agent. For information about configuring LDAP domains, see <em>Creating and Deleting LDAP and Active Directory Domains</em> on page 161.</td>
</tr>
<tr>
<td>DC Agent Listening Port</td>
<td>Enter the listening port of the DC agent. The listening port is the port through which the DC agent transfers the list of authenticated users to the STM. The default port is 5182.</td>
</tr>
<tr>
<td>Synchronization Interval</td>
<td>Enter the time interval (in seconds) at which the DC agent updates the list of authenticated users. The default interval is 15 seconds.</td>
</tr>
<tr>
<td>Expiration length</td>
<td>Enter time interval in hours or minutes (determined by your selection from the Expiration length drop-down list) that is allowed to elapse before a user login expires. The default setting is zero (0), that is, a user login does not expire.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the DC agent: A green circle indicates that the DC agent is active; a gray circle indicates that the DC agent is inactive.</td>
</tr>
</tbody>
</table>

5. To add the newly configured DC agent to the List of DC Agents table, click the **Add** table button in the Action column.

   For each DC agent in the List of DC Agents table, the Action column provides two table buttons:

   - **Apply.** Activates the DC agent. The circle in the Status column turns green.
   - **Delete.** Deletes the DC agent from the table.
To edit a DC agent:

1. In the Domain column, locate the DC agent that you want to edit, and make changes in the columns to the right of the Domain column.
2. Click Apply to save your changes.

Creating and Deleting RADIUS Domains

To configure RADIUS authentication:

1. Select User Management > Authentication from the menu. The authentication submenu tabs display with the LDAP screen in view.
2. Click the RADIUS submenu tab. The RADIUS screen displays. (The following figure contains two examples.)

![RADIUS Screen](image)

The List of RADIUS table displays the following fields:

- **Domain.** The name of the STM’s domain to which the server has been assigned.
- **Server.** The IP address of the RADIUS server.
- **Action.** The Edit table button, which provides access to the Edit RADIUS screen, and the Delete table button, which allows you to delete the RADIUS server.
3. Complete the fields and make your selections from the drop-down list as explained in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>A descriptive (alphanumeric) name of the RADIUS authentication server for identification and management purposes.</td>
</tr>
<tr>
<td>Server</td>
<td>The server IP address or server host name of the RADIUS authentication server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number for the RADIUS authentication server. The default port for the RADIUS server is 1812.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>The shared secret (password) that is required to access the RADIUS authentication server.</td>
</tr>
<tr>
<td>Repeat</td>
<td>The maximum number of times that the STM attempts to connect to the RADIUS server. The default setting is 3 times.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The period after which an unsuccessful connection attempt times out. The default setting is 5 seconds.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>From the drop-down list, select the encryption type for the connection between the STM and the LDAP or Active Directory server:</td>
</tr>
<tr>
<td></td>
<td>• PAP. The connection uses the Password Authentication Protocol (PAP). This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• CHAP. The connection uses the Challenge Handshake Authentication Protocol (CHAP).</td>
</tr>
</tbody>
</table>

Use the following user account to test RADIUS settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The user name to test the RADIUS settings with.</td>
</tr>
<tr>
<td>Password</td>
<td>The password to test the RADIUS settings with.</td>
</tr>
</tbody>
</table>

4. Click Test to verify that the RADIUS server can actually function with the RADIUS settings that you have specified. The automated test procedure checks the connection to the RADIUS server, the user name, and the password. If any settings require changes, you are notified at the end of the automated test procedure.

5. Click Apply to save your settings. The RADIUS domain and server are added to the List of RADIUS table.

To delete a domain and server from the List of RADIUS table, click the Delete table button in the Action column for the domain and server that you want to delete.

**WARNING!**

After their sessions have expired, users can no longer log in to the STM if the domain that has been assigned to them is the domain that you deleted.
Editing RADIUS Domains and Configuring VLANs

To edit a RADIUS domain:

1. Select User Management > Authentication from the menu. The authentication submenu tabs display with the LDAP screen in view.
2. Click the RADIUS submenu tab. The RADIUS screen displays (see Figure 96 on page 167).
3. In the Action column of the List of RADIUS table, click the Edit table button for the domain and server that you want to edit. The Edit Radius screen displays. (The following figure contains some examples.)

![Edit RADIUS Screen](image)

Figure 97.

4. Modify the fields and make your selections from the drop-down list as explained in Table 49 on page 168.
5. Click Test to verify that the RADIUS server can actually function with the RADIUS settings that you have modified. The automated test procedure checks the connection to the RADIUS server, the user name, and the password. If any settings require changes, you are notified at the end of the automated test procedure.
6. Click Apply to save your settings.
Creating and Deleting VLANs for Use with RADIUS Domains

After you have created a RADIUS domain by specifying a RADIUS server, you can add a virtual LAN (VLAN), and then set access exceptions for the logged-in RADIUS users (see Setting Access Exception Rules for Web Access on page 132).

In order to use the VLAN to set access exceptions on the STM, the following is required:

- You need to have defined a VLAN policy on another platform.
- You need to have added users to the VLAN policy.
- The RADIUS server needs to contain VLAN attributes in its user information.

At the bottom of the Edit Radius screen (see the previous figure, which contains one VLAN example), the List of VLAN table displays the following fields:

- VLAN ID/Name. The identifier or name for the VLAN.
- Brief Description. An optional brief description of the VLAN.
- Action. The Delete table button, which allows you to delete the VLAN.

To add a VLAN:

1. On the Edit Radius screen, locate the Add New VLAN ID/Name section at the very bottom of the screen. Specify the VLAN:
   a. In the VLAN ID/Name field, enter the identifier or the name of the VLAN.
   b. In the Brief Description field, enter a description of the VLAN. This field is optional.

2. Click the Add table button. The new VLAN is added to the List of VLAN table.

To delete a user from the List of VLAN table, click the Delete table button in the Action column for the VLAN that you want to delete.

Global User Settings

You can globally set the user session settings for authenticated users. These settings include the session expiration period, the allowed session idle time, and the default domain that is presented to the users.
To specify the global user configuration settings:

1. Select **User Management > Configuration** from the menu. The Configuration screen displays:

![Configuration Screen](image)

**Figure 98.**

2. Locate the Sessions Parameters section on screen. Specify the session settings:
   
   - **Session Expiration Length.** The period after which a session expires and a user needs to log in again. This setting applies to all users. From the drop-down list, select either **Minutes** or **Hours**. Then, in the field to the left of the drop-down list, enter a number for the minutes or hours. The session expiration length cannot exceed the idle time period.

   - **Idle Time.** The period after which an idle connection is terminated and a user needs to log in again. This setting applies to all users. From the drop-down list, select either **Minutes** or **Hours**. Then, in the field to the left of the drop-down list, enter a number for the minutes or hours. The idle time period cannot exceed the session expiration length.

3. Click **Apply** to save the session settings.
4. Locate the Users Portal Login Settings section on screen. Specify the default domain settings:
   • From the Default Domain drop-down list, select a domain that is presented as the default domain on the User Portal Login screen. The default domain that is presented is prosecuredomain. Users can still select another domain (if there are other domains configured on the STM) from the drop-down list on the User Portal Login screen.
   • Select the **Authenticate User with User Selected Domain** check box to limit the authentication on the User Portal Login screen to the domain that you select from the Default Domain drop-down list. If you do not select this check box, the STM attempts to authenticate users through all the domains that are listed in the drop-down list on the User Portal Login screen; when authentication through one domain fails, the STM attempts authentication through another domain.

5. Click **Apply** to save the default domain settings.

### Viewing and Logging Out Active Users

A user with administrative privileges can view the active users and log out selected or all active users.

**To log out all active users:**

1. Select **User Management > Active Users** from the menu. The Active Users screen displays:

   ![Active Users Screen](image)

   **Figure 99.**

2. Click the **Logout All Users** button in the gray settings bar at the top of the Active Users screen.
To view all or selected users:

1. On the Active Users screen (see the previous figure), select one of the following radio buttons:
   - **View All.** This selection returns all active users after you click the Search button.
   - **Search Criteria.** This selection lets you enter the following search criteria so that only selected users are returned after you click the Search button. Use either the IP Address field or the Domain and User fields. The setting of the Login Type check boxes affects both the IP address search method and the domain and user search method.
     - **IP Address.** Enter an IP address or an IP address and subnet mask in Classless Inter-Domain Routing (CIDR) notation (for example, /024).
     - **Domain.** Enter a domain (for example, prosecuredomain).
     - **User.** Enter a user name (for example, JackP). If you do not enter a user name, all users of the specified domain are displayed in the search results.
     - **Login Type.** Select the **DC Agent** check box to display only users who logged in through the DC agent in the search results. Select the **User Portal** check box to display only users who logged in through the user portal search results. By default, both check boxes are selected.

2. In the Display field, enter a number to specify how many entries per page the search result screen returns.

3. Click **Search.** The search results screen displays. (The following figure contains some examples.)

```
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Domain</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.50</td>
<td>elightpostLDAP</td>
<td>Administrator Domain Users Exchange Services Exchange Domain Servers Group Policy C</td>
</tr>
<tr>
<td>192.168.1.61</td>
<td>elightpostLDAP</td>
<td>blue</td>
</tr>
<tr>
<td>208.142.120.1</td>
<td>prosecuredomain</td>
<td>JackP</td>
</tr>
</tbody>
</table>
```

**Figure 100.**

The List of Users table displays the following fields:

- **IP Address.** The IP address that is associated with the user.
- **Domain.** The domain to which the user belongs.
- **User.** The user name.
- **Groups.** The groups to which the user belongs, if any.
- **Last Seen.** The most recent time that scanned traffic associated with the user (that is, IP address) passed through the STM.
- **Login Type.** The method through which the user logged in (DC agent or user portal).
To log out selected active users:

1. On the search results screen select the check boxes to the left of the users that you want to log out.

2. Click **Logout**.
This chapter describes the system monitoring features of the STM. You can be alerted to important events such as attacks and login failures. You can also view the system status and real-time traffic and security information. In addition, the diagnostics utilities are described.

**Note:** All email notification functions that are part of the Logs, Reports, and Alerts menus, and some of the functions that are part of the Diagnostics configuration menu require that you configure the email notification server—see Configuring the Email Notification Server on page 176.

This chapter contains the following sections:

- Configuring Logging, Alerts, and Event Notifications on this page
- Viewing System Status on page 192
- Querying Logs on page 194
- Viewing, Scheduling, and Generating Reports on page 200
- Viewing and Managing the Quarantine Files on page 208
- Using Diagnostics Utilities on page 215

### Configuring Logging, Alerts, and Event Notifications

You can configure the STM to email logs and alerts to a specified email address. For example, the STM can email security-related events such as malware incidents, infected clients, and failed authentications. By default, the STM logs content filtering events such as attempts to access blocked sites and URLs, unwanted email content, spam attempts, and many other types of events.

For you to receive the logs in an email message, the STM’s notification server needs to be configured and email notification needs to be enabled. If the notification server is not configured or email notification is disabled, you can still query the logs and generate log reports to view on the Web Management Interface or to save in CSV format.
For more information about logs, see *Querying Logs* on page 194.

### Configuring the Email Notification Server

If you have used the Setup Wizard, you might have already configured the email notification server; the Email Notification Server screen allows you to modify these settings.

The STM can automatically send information such as notifications and reports to an administrator. You need to configure the necessary information for sending email, such as the administrator’s email address, the email server, user name, and password.

**To configure the email notification server:**

1. Select **Global Settings > Email Notification Server** from the menu. The Email Notification Server screen displays. (The following figure contains some examples.)

   ![Figure 101.](image)

2. Complete the fields, select the radio button and check boxes, and make your selections from the drop-down lists as explained in the following table:

   **Table 50. Email Notification Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show as Mail Sender</td>
<td>A descriptive name of the sender for email identification purposes. For example, enter <code>stm600notification@netgear.com</code>.</td>
</tr>
<tr>
<td>Send Notifications to</td>
<td>The email address to which the notifications should be sent. Typically, this is the email address of a user with administrative privileges.</td>
</tr>
<tr>
<td>SMTP Server</td>
<td>The IP address and port number or Internet name and port number of your ISP’s outgoing email SMTP server. The default port number is 25.</td>
</tr>
<tr>
<td>Note:</td>
<td>If you leave this field blank, the STM cannot send email notifications.</td>
</tr>
</tbody>
</table>
Configuring and Activating System, Email, and Syslog Logs

You can configure the STM to log system events such as a change of time by an NTP server, secure login attempts, restarts, and other events. You can also send logs to the administrator or schedule logs to be sent to the administrator or to a syslog server on the network. In addition, the Log Management screen provides the option to selectively clear logs. Because this large screen has three sections, each with its own Apply button, this screen is presented in this manual in three figures (the following figure, Figure 103 on page 180, and Figure 104 on page 182).

**Emailing Logs**

To enable and configure logs to be sent to an email address:

1. Select **Monitoring > Logs** from the menu. The Logs submenu tabs display, with the Log Management screen in view (see the following figure, Figure 103 on page 180, and Figure 104 on page 182).

2. Locate the Email Logs to Administrator section on the screen. Select the **Enable** check box to enable the STM to send logs to an email address.

---

### Table 50. Email Notification Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Server Requires Authentication</td>
<td>If the SMTP server requires authentication, select the <strong>Mail Server Requires Authentication</strong> check box and enter the following settings:</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name for SMTP server authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for SMTP server authentication.</td>
</tr>
</tbody>
</table>

3. Click **Apply** to save your settings.
Figure 102. Log Management, screen 1 of 3

3. Complete the fields, select the radio button and check boxes, and make your selections from the drop-down lists as explained in the following table:

Table 51. Email Logs Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send to</td>
<td>The email address of the recipient of the log file. This is normally a user with administrative privileges. You enter up to three email address, separated by commas. Click <strong>Send Now</strong> to immediately send the logs that you first need to have specified (see the information later in this table). <strong>Note:</strong> To limit the size of the email, the STM does not send the actual logs to the specified email address but an email that contains links to the actual logs. These links remain active for a period of 10 days, after which the logs are no longer available.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Select a radio button to specify how often the log file is sent:</td>
</tr>
<tr>
<td></td>
<td>• <strong>When the space is full.</strong> Logs are sent when the storage space that is assigned to the logs is full.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Daily.</strong> Logs are sent daily at the time that you specify from the drop-down lists (hours and minutes).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Weekly.</strong> Logs are sent weekly at the day and time that you specify from the drop-down lists (weekday, hours, and minutes).</td>
</tr>
</tbody>
</table>
4. Click **Apply** to save your settings.

**Sending Logs to a Syslog Servers**

To enable and configure logs to be sent to a syslog server:

1. Select **Monitoring > Logs** from the menu. The Logs submenu tabs display, with the Log Management screen in view (see Figure 102 on page 178).
2. Locate the Send Logs via Syslog section on the screen (see the following figure), and select the **Enable** check box to enable the STM to send logs to a syslog server.
3. Complete the fields, select the check boxes, and make your selections from the drop-down lists as explained in the following table:

Table 52. Syslog Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the syslog server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number that the syslog server uses to receive logs. The default port number is 514.</td>
</tr>
<tr>
<td>Logs</td>
<td>Select the check boxes to specify which logs are sent to the syslog server:</td>
</tr>
<tr>
<td>System logs</td>
<td>The system event logs that include all system errors, informational messages, configuration changes, and system software updates.</td>
</tr>
<tr>
<td>Email traffic logs</td>
<td>All scanned incoming and outgoing traffic.</td>
</tr>
<tr>
<td>Web traffic logs</td>
<td>All scanned incoming and outgoing traffic.</td>
</tr>
<tr>
<td>Malware logs</td>
<td>All intercepted viruses and spyware.</td>
</tr>
<tr>
<td>Spam logs</td>
<td>All intercepted spam, including spam that was detected through the blacklist, real-time blacklist, and distributed spam analysis.</td>
</tr>
<tr>
<td>Email filter logs</td>
<td>All emails that are intercepted because of keyword, file type, file name, password, or size limit violations.</td>
</tr>
<tr>
<td>Content filter logs</td>
<td>All websites, URLs, and FTP sites that are intercepted because of Web category, blacklist, file type, or size limit violations.</td>
</tr>
<tr>
<td>Application logs</td>
<td>All intercepted application access violations.</td>
</tr>
</tbody>
</table>
Table 52. Syslog Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
</table>
| Facility | The facility indicates from which internal part of the STM the log message originates. For each log that you have selected to be sent to the syslog server (see earlier in this table), select one of the following facilities from the drop-down list:  
  • auth. Security and authorization log messages.  
  • authpriv. Security and authorization log messages for sensitive information.  
  • cron. Clock daemon log messages.  
  • deamon. Other daemon log messages.  
  • ftp. FTP log messages.  
  • kern. Kernel log messages.  
  • local0 through local7. Locally defined log messages (1 through 7).  
  • lpr. Line printer subsystem log messages.  
  • mail. Mail subsystem log messages.  
  • news. Usenet news subsystem log messages.  
  • syslog. Log messages that are generated internally by the syslog server (syslogd).  
  • user. Generic user-level log messages.  
  • uucp. Unix-Unix copy (UUCP) subsystem log messages. |
| Priority | For each log that you have selected to be sent to the syslog server (see earlier in this table), select one of the following severities from the drop-down list:  
  • emerg. The STM is unusable.  
  • alert. An action needs to be taken immediately.  
  • crit. There are critical conditions.  
  • err. There are error conditions.  
  • warning. There are warning conditions.  
  • notice. There are normal but significant conditions.  
  • info. Informational messages.  
  • debug. Debug-level messages.  

**Note:** All the logs with a severity that is equal to and above the severity that you specify are logged on the specified syslog server. For example, if you select crit as the severity, then the logs with the severities crit, alert, and emerg are logged.

4. Click **Apply** to save your settings.
Clearing Logs

To clear logs:

1. Select Monitoring > Logs from the menu. The Logs submenu tabs display, with the Log Management screen in view (see Figure 102 on page 178). Locate the Clear the Following Log Information section at the bottom of the screen:

   ![Clear Log Information](image)

   Figure 104. Log Management, screen 3 of 3

2. Select one or more check boxes to specify which logs are cleared:
   - **System**. The system event logs are cleared.
   - **Email traffic**. The logs with scanned incoming and outgoing email traffic are cleared.
   - **Web traffic**. The logs with scanned incoming and outgoing Web traffic are cleared.
   - **Malware**. The logs with intercepted viruses and spyware are cleared.
   - **Spam**. The logs with intercepted spam are cleared.
   - **Email filter**. The logs with intercepted emails are cleared.
   - **Content filter**. The logs with intercepted websites, URLs, and FTP sites are cleared.
   - **Application**. The logs with intercepted applications are cleared.

3. Click Clear Log Information.

Configuring Alerts

You can configure the STM to send an email alert when a failure, license expiration, or malware attack or outbreak occurs. Four types of alerts are supported:

- **Update Failure Alert**. Sent when an attempt to update any component such as a pattern file or scan engine firmware fails.
- **License Expiration Alerts**. Sent when a license is about to expire and then again when a license has expired.
- **Malware Alert**. Sent when the STM detects malware threats.
- **Malware Outbreak Alert**. Sent when the malware outbreak criteria that you have configured are reached or exceeded. Outbreak criteria are based on the number of malware threats detected within a specified period of time.
To configure and activate the email alerts:

1. Select **Monitoring > Alerts** from the menu. The Alerts screen displays:

2. Select the check boxes and complete the fields as explained in the following table:

**Table 53. Alerts Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Update Failure Alerts</td>
<td>Select this check box to enable update failure alerts.</td>
</tr>
<tr>
<td>Enable License Expiration Alerts</td>
<td>Select this check box to enable update license expiration alerts.</td>
</tr>
<tr>
<td>Enable Malware Alerts</td>
<td>Select this check box to enable malware alerts, and configure the Subject and Message fields.</td>
</tr>
<tr>
<td>Subject</td>
<td>Enter the subject line for the email alert. The default text is [Malware alert].</td>
</tr>
<tr>
<td>Message</td>
<td>Enter the content for the email alert. The default text is %VIRUSINFO%, which is the metaword that enables the STM to insert the correct malware threat information. Note: In addition to the %VIRUSINFO% metaword, you can insert the following metawords in your customized message: %TIME%, %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%.</td>
</tr>
</tbody>
</table>

---

**Figure 105.**

You can monitor the real-time traffic, security events, and statistics from the Dashboard screen. The Web Usage screen displays which hosts on your network are consuming the most resources.

Understanding the Information on the Dashboard Screen

When you start up the STM, the default screen that displays is the Dashboard screen, which lets you monitor the following items:

- CPU, memory, and hard disk status
- The number of active connections per protocol
- The total malware threats and the malware threats over the last seven days
- Total scanned services traffic over the last seven days
- Statistics for the most recent five and top five malware threats detected, applications blocked, Web categories blocked, and spam emails blocked
- The real-time security scanning status with detected network traffic, detected network threats, and service statistics for the six supported protocols (HTTP, HTTPS, FTP, SMTP, POP3, and IMAP)
- Interface statistics

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Malware Outbreak Alerts</td>
<td>Select this check box to enable malware outbreak alerts, and configure the Outbreak Criteria, Protocol, and Subject fields.</td>
</tr>
<tr>
<td>Outbreak Criteria</td>
<td>To define a malware outbreak, specify the following fields:</td>
</tr>
<tr>
<td></td>
<td>• malware found within. The number of malware incidents that are detected.</td>
</tr>
<tr>
<td></td>
<td>• minutes (maximum 90 minutes). The period in which the specified number of malware incidents are detected.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When the specified number of detected malware incidents is reached within the time threshold, the STM sends a malware outbreak alert.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the check box or check boxes to specify the protocols (SMTP, POP3, IMAP, HTTP, HTTPS, and FTP) for which malware incidents are detected.</td>
</tr>
<tr>
<td>Subject</td>
<td>Enter the subject line for the email alert.</td>
</tr>
</tbody>
</table>

3. Click **Apply** to save your settings.
To display the Dashboard screen, select **Monitoring > Dashboard** from the menu. The Dashboard submenu tabs display with the Dashboard screen in view. Because of the size of this screen, it is divided and presented in this manual in three figures (the following figure, *Figure 107* on page 187, and *Figure 108* on page 189), each with its own table that explains the fields.

![Dashboard Screen](image)

*Figure 106. Dashboard, screen 1 of 3*

Except for setting the poll interval and clearing the statistics, you cannot configure the fields on the Dashboard screen. Any changes need to be made on other screens.
To set the poll interval:

1. Click the Stop button.
2. From the Poll Interval drop-down list, select a new interval (the minimum is 5 seconds, the maximum is 5 minutes).
3. Click the Set Interval button.

To clear the statistics, click Clear Statistics.

The following table explains the fields of the Status, Total Threats, and Threats (Last 7 Days) sections of the Dashboard screen:

<table>
<thead>
<tr>
<th>Table 54. Dashboard: Status, Total Threats, and Threats (Last 7 Days) Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
</tr>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td>System</td>
</tr>
<tr>
<td>Services</td>
</tr>
<tr>
<td>Active Connections</td>
</tr>
<tr>
<td>Application Control</td>
</tr>
<tr>
<td><strong>Total Threats (Since Last Clear)</strong></td>
</tr>
<tr>
<td>Email</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Web</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Table 54. Dashboard: Status, Total Threats, and Threats (Last 7 Days) Information (Continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Displays the total number of:</td>
</tr>
<tr>
<td></td>
<td>• IM blocked.</td>
</tr>
<tr>
<td></td>
<td>• Tools blocked.</td>
</tr>
<tr>
<td></td>
<td>• Media blocked.</td>
</tr>
<tr>
<td></td>
<td>• P2P blocked.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>For information about how to configure these applications, see Configuring Application Control on page 127.</td>
</tr>
</tbody>
</table>

**Threats (Last 7 Days)**

This is a graphic that shows the relative number of threats and access violations over the last week, using different colors for the various applications:

**Note:** IMBlock stands for instant messaging applications blocked; P2PBlock stands for peer-to-peer applications blocked.
The following table explains the fields of the Total Scanned Services Traffic, Most Recent 5, and Top 5 sections of the Dashboard screen:

### Table 55. Dashboard: Total Scanned Services Traffic and Most Recent 5 and Top 5 Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total Scanned Services Traffic (Last 7 Days)</strong></td>
<td>This is a graphic that shows the relative number of traffic in bytes over the last week.</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td><strong>Most Recent 5 Description</strong></td>
</tr>
<tr>
<td>Malware</td>
<td>• <strong>Malware Name.</strong> The name of the malware threat.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Protocol.</strong> The protocol in which the malware threat was detected.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Date and Time.</strong> The date and time that the malware threat was detected.</td>
</tr>
<tr>
<td>Application</td>
<td>• <strong>Application.</strong> The name of the application that was blocked.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Client IP.</strong> The client IP address from which the application request came.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Date and Time.</strong> The date and time that the application request was blocked.</td>
</tr>
<tr>
<td>Web</td>
<td>• <strong>Category.</strong> The Web category that was blocked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For more information about Web categories, see Configuring Web Content Filtering on page 109.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Client IP.</strong> The client IP address from which the Web request came.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Date and Time.</strong> The date and time that the Web request was blocked.</td>
</tr>
<tr>
<td>Spam</td>
<td>• <strong>Recipient.</strong> The intended recipient of the spam message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Subject.</strong> The email subject line in the spam message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Date and Time.</strong> The date and time that the spam message was detected.</td>
</tr>
</tbody>
</table>
Chapter 6. Monitoring System Access and Performance

ProSecure Web/Email Security Threat Management (STM) Appliance

Figure 108. Dashboard, screen 3 of 3

Note: The previous figure shows the Interface Statistics section of the STM600. The STM300 and STM150 have different interfaces (see the following table).

The following table explains the fields of the Service Statistics and Interface Statistics sections of the Dashboard screen:

Table 56. Dashboard: Service Statistics and Interface Statistics Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Statistics</td>
<td></td>
</tr>
<tr>
<td>For each of the six supported protocols (HTTP, HTTPS, FTP, SMTP, POP3, and IMAP), this section provides the following statistics:</td>
<td></td>
</tr>
<tr>
<td>Total Scanned Traffic (MB)</td>
<td>The total quantity of scanned traffic in MB.</td>
</tr>
<tr>
<td>Total Emails/Files Scanned</td>
<td>The total number of scanned emails and files.</td>
</tr>
</tbody>
</table>
Monitoring Web Usage

The Web Usage screen shows you how the STM’s Web resources are being used. You can see, for example, which host on the STM uses most resources.

Table 56. Dashboard: Service Statistics and Interface Statistics Information (Continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Malwares Found</td>
<td>The total number of detected malware threats.</td>
</tr>
<tr>
<td>Virus</td>
<td>The total number of detected viruses.</td>
</tr>
<tr>
<td>Spyware</td>
<td>The total number of detected spyware threats.</td>
</tr>
<tr>
<td>Total Emails/Files Blocked</td>
<td>The total number of blocked emails and files.</td>
</tr>
<tr>
<td>Total Malware Quarantined</td>
<td>The total number of detected malware threats that were placed in quarantine.</td>
</tr>
<tr>
<td>Total Spam Quarantined</td>
<td>The total number of spam messages that were placed in quarantine.</td>
</tr>
<tr>
<td>Total Emails</td>
<td>The total number of spam emails that were detected.</td>
</tr>
<tr>
<td>Note:</td>
<td>These statistics apply only to SMTP.</td>
</tr>
<tr>
<td>Total URLs</td>
<td>The total number of URL requests that were blocked.</td>
</tr>
<tr>
<td>Note:</td>
<td>These statistics apply only to HTTP and HTTPS.</td>
</tr>
<tr>
<td>Total Spam Emails</td>
<td>The total number of spam emails that were detected.</td>
</tr>
<tr>
<td>Note:</td>
<td>These statistics apply only to SMTP and POP3.</td>
</tr>
<tr>
<td>Blacklist &amp; RBL</td>
<td>The total number of emails that were detected through the spam blacklist and the real-time blacklist (see Setting Up the Whitelist and Blacklist on page 98 and Configuring the Real-Time Blacklist on page 100).</td>
</tr>
<tr>
<td>Distributed Spam Analysis</td>
<td>The total number of spam messages that were detected through distributed spam analysis (see Configuring Distributed Spam Analysis on page 102).</td>
</tr>
</tbody>
</table>

Interface Statistics

STM600: MGMT (Management), PAIR1 UPLINK, PAIR1 DOWNLINK, PAIR2 UPLINK, PAIR2 DOWNLINK.
STM300: MGMT, UPLINK, DOWNLINK.
STM150: LAN1, LAN2, LAN3, LAN4, WAN.

For each interface the following statistics are displayed:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX</td>
<td>The number of transmitted packets in KB, MB, or GB (as stated on the screen).</td>
</tr>
<tr>
<td>RX</td>
<td>The number of received packets in KB, MB, or GB (as stated on the screen).</td>
</tr>
</tbody>
</table>
To view the STM’s Web usage:

1. Select Monitoring > Dashboard from the menu. The Dashboard submenu tabs display with the Dashboard screen in view.

2. Click the Web Usage submenu tab. The Web Usage screen displays:

![Web Usage Screen]

3. Use the From drop-down list to select the start date of the Web usage report (year, month, date) and the To drop-down list to select the end date of the report (year, month, date).

4. Click View. The STM generates a Web usage report.

The Web usage reports shows the following columns:

- **TOP**. The Web usage ranking.
- **Category**. The Web content filtering category.
- **Requests**. The number of requests for the category.
- **% of Requests**. The percentage of requests for the category in relation to the total number of Web requests.
- **IPs**. The number of IP addresses that request the category.
- **% of IPs**. The percentage of IP addresses that request the category in relation to the total number of IP addresses.
- **Blocked**. Whether or not the category is blocked by the STM.
Viewing System Status

The System Status screen provides real-time information about the following components of the STM:

- Firmware versions and update information of the STM, software versions and update information of the components, license expiration dates for each type of license, and hardware serial number
- Management interface information
- MAC addresses for the STM’s interfaces

To view the System Status screen select Monitoring > System Status. The following figure displays the System Status screen of the STM600. The Interfaces section of the System Status screen differs for the STM300 and STM150 (see the explanation in the following table).

![System Status Screen](image)

Figure 110.
The following table explains the fields of the System Information, Management Interface Information, and Interfaces sections of the System Status screen:

### Table 57. System Status Information

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Information</strong></td>
<td></td>
</tr>
<tr>
<td>Firmware Information</td>
<td>The current version and most recent update (that is, the most recently downloaded version) for the software, scan engine, pattern file, and operating system (OS). Click + More to display the versions and most recent downloads for the antispam engine, applications engine, applications pattern file, stream engine, stream pattern file, mini engine, mini pattern file, policyd, scand, urld, update client, and rescue software.</td>
</tr>
<tr>
<td>Hardware Serial Number</td>
<td>The hardware serial number of the STM.</td>
</tr>
<tr>
<td>License Expiration Date</td>
<td>The license keys and the expiration dates for the email protection, Web protection, and maintenance and support licenses.</td>
</tr>
</tbody>
</table>

Note: When a license has expired, the license expiration date is displayed in red font.

When a license expires, a LED on the front panel of the STM blinks continuously to remind you to renew the license. To stop the blinking, click Stop LED Blinking. On the STM150: The Test LED blinks when a license expires. On the STM300 and STM600: The Status LED blinks when a license expires.

<table>
<thead>
<tr>
<th>Management Interface Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>These fields are self-explanatory. You can configure these fields on the Network Settings screen (see Configuring Network Settings on page 52).</td>
</tr>
<tr>
<td>Gateway IP Address</td>
<td></td>
</tr>
<tr>
<td>Primary DNS</td>
<td></td>
</tr>
<tr>
<td>Secondary DNS</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interfaces</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The MAC addresses of the STM’s interfaces. (The previous figure displays the System Status screen for the STM600.)</td>
<td></td>
</tr>
<tr>
<td>STM600: MGMT (Management), PAIR1 DOWNLINK, PAIR1 UPLINK, PAIR2 DOWNLINK, PAIR2 UPLINK.</td>
<td></td>
</tr>
<tr>
<td>STM300: MGMT, DOWNLINK, UPLINK.</td>
<td></td>
</tr>
<tr>
<td>STM150: LAN, WAN. (The four LAN interfaces share a single MAC address.)</td>
<td></td>
</tr>
</tbody>
</table>
Querying Logs

The extensive log querying functions of the STM can help you to monitor the protection of the network and fine-tune the performance of the STM.

For information about emailing logs and sending logs to a syslog server, see Configuring and Activating System, Email, and Syslog Logs on page 177.

The STM generates logs that provide detailed information about malware threats and traffic activities on the network. You can search and view these logs through the Web Management Interface or save the log records in CSV or HTML format and download them to a computer (the downloading option is not available for all logs). You can also specify how many entries are displayed per page (the default setting is 15 entries).

The STM provides nine types of logs:

- **Email traffic.** All scanned incoming and outgoing email traffic.
- **Web traffic.** All scanned incoming and outgoing Web traffic.
- **Virus.** All intercepted viruses.
- **Spyware.** All intercepted spyware.
- **Spam.** All intercepted spam, including spam that was detected through the blacklist, real-time blacklist, and distributed spam analysis.
- **Email filters.** All emails that are intercepted because of keyword, file type, file name, password, or size limit violations.
- **Content filters.** All websites, URLs, and FTP sites that are intercepted because of Web category, blacklist, file type, or size limit violations.
- **System.** The system event logs that include all system errors, informational messages, configuration changes, and system software updates.
- **Application.** All intercepted application access violations.

You can query and generate each type of log separately and filter the information based on a number of criteria. For example, you can filter the virus logs using the following criteria (other log types have similar filtering criteria):

- Start date and time
- End date and time
- Protocols (HTTP, HTTPS, FTP, SMTP, POP3, and IMAP)
- Virus name
- Action (delete, quarantine, quarantine email, block email, and log)
- Domain name
- User name
- Client IP address
- Server IP address
To query and download logs:

1. Select **Monitoring > Logs** from the menu. The Logs submenu tabs display, with the Log Management screen in view.

2. Click the **Logs Query** submenu tab. The Logs Query screen displays (see the following figure).

Depending on the selection that you make from the Log Type drop-down list, the screen adjusts to display the settings for the selected type of log. The following figure displays the Virus log information settings as an example.

![Image of the Logs Query screen](image_url)

Figure 111.
3. Select the check boxes and radio buttons, make your selections from the drop-down lists, and complete the fields as explained in the following table:

Table 58. Log Query Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Type</strong></td>
<td>Select one of the following log types from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• Email traffic. All scanned incoming and outgoing email traffic.</td>
</tr>
<tr>
<td></td>
<td>• Web traffic. All scanned incoming and outgoing email traffic.</td>
</tr>
<tr>
<td></td>
<td>• Virus. All intercepted viruses.</td>
</tr>
<tr>
<td></td>
<td>• Spyware. All intercepted spyware.</td>
</tr>
<tr>
<td></td>
<td>• Spam. All intercepted spam, including spam that was detected through the blacklist, real-time blacklist, and distributed spam analysis.</td>
</tr>
<tr>
<td></td>
<td>• Email filters. All emails that are intercepted because of keyword, file type, file name, password, or size limit violations.</td>
</tr>
<tr>
<td></td>
<td>• Content filters. All websites, URLs, and FTP sites that are intercepted because of Web category, blacklist, file type, or size limit violations.</td>
</tr>
<tr>
<td></td>
<td>• System. The system event logs that include all system errors, informational messages, configuration changes, and system software updates.</td>
</tr>
<tr>
<td></td>
<td>• Application. All intercepted application access violations.</td>
</tr>
<tr>
<td>View All</td>
<td>Select one of the following radio buttons:</td>
</tr>
<tr>
<td>Search Criteria</td>
<td>• View All. Display or download the entire selected log.</td>
</tr>
<tr>
<td></td>
<td>• Search Criteria. Query the selected log by configuring the search criteria that are available for the selected log.</td>
</tr>
<tr>
<td><strong>Start Date/Time</strong></td>
<td>From the drop-down lists, select the year, month, day, hours, and minutes for the start date and time.</td>
</tr>
<tr>
<td></td>
<td>This field is available for the following logs: Email traffic, Web traffic, Virus, Spyware, Spam, Email filters, Content filters, System, and Application.</td>
</tr>
<tr>
<td><strong>End Date/Time</strong></td>
<td>From the drop-down lists, select the year, month, day, hours, and minutes for the end date and time.</td>
</tr>
<tr>
<td></td>
<td>This field is available for the following logs: Email traffic, Web traffic, Virus, Spyware, Spam, Email filters, Content filters, System, and Application.</td>
</tr>
<tr>
<td>Protocols</td>
<td>Select one or more check boxes to specify the protocols that are queried.</td>
</tr>
<tr>
<td></td>
<td>The following protocols can be selected:</td>
</tr>
<tr>
<td></td>
<td>• For the Email traffic log: SMTP, POP3, and IMAP.</td>
</tr>
<tr>
<td></td>
<td>• For the Web traffic log: HTTP, HTTPS, and FTP.</td>
</tr>
<tr>
<td></td>
<td>• For Virus, and Spyware logs: SMTP, POP3, IMAP, HTTP, HTTPS, and FTP.</td>
</tr>
<tr>
<td></td>
<td>• For the Spam log: SMTP and POP3.</td>
</tr>
<tr>
<td></td>
<td>• For the Email filters log: SMTP, POP3, and IMAP.</td>
</tr>
<tr>
<td></td>
<td>• For the Content filters log: HTTP, HTTPS, and FTP.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description (or Subfield and Description)</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Search Criteria (continued)</td>
<td>Domain&lt;br&gt;The domain name that is queried.&lt;br&gt;This field is available for the following logs: Email traffic, Web traffic, Virus, Spyware, Spam, Email filters, Content filters, and Application.</td>
</tr>
<tr>
<td>User</td>
<td>The user name that is queried.&lt;br&gt;This field is available for the following logs: Email traffic, Web traffic, Virus, Spyware, Spam, Email filters, Content filters, and Application.</td>
</tr>
<tr>
<td>Client IP</td>
<td>The client IP address that is queried.&lt;br&gt;This field is available for the following logs: Email traffic, Web traffic, Virus, Spyware, Content filters, and Application.</td>
</tr>
<tr>
<td>Server IP</td>
<td>The server IP address that is queried.&lt;br&gt;This field is available for the following logs: Email traffic, Web traffic, Virus, Spyware, Content filters, and Application.</td>
</tr>
<tr>
<td>Reason</td>
<td>Select one or more check boxes to specify the reasons that are queried:&lt;br&gt;The following reasons can be selected:&lt;br&gt;• For the Email filters log: keyword, file type, file name, password, and size limit.&lt;br&gt;• For the Content filters log: Web category, file type, blacklist, and size limit.</td>
</tr>
<tr>
<td>Virus Name</td>
<td>The name of the virus that is queried.&lt;br&gt;This field is available only for the Virus log.</td>
</tr>
<tr>
<td>Spyware Name</td>
<td>The name of the spyware that is queried.&lt;br&gt;This field is available only for the Spyware log.</td>
</tr>
<tr>
<td>Action</td>
<td>Select one or more check boxes to specify the malware treatment actions that are queried.&lt;br&gt;The following actions can be selected:&lt;br&gt;• For the Virus and Spyware logs: Delete, Quarantine, Quarantine email, Block email, or Log.&lt;br&gt;• For the Spam log: Block, Tag, or Quarantine.</td>
</tr>
<tr>
<td>Detected By</td>
<td>Select one or all check boxes to specify the method by which spam is detected: Blacklist, RBL, or Distributed Spam Analysis.&lt;br&gt;This field is available only for the Spam log.</td>
</tr>
<tr>
<td>Subject</td>
<td>The email subject that is queried:&lt;br&gt;This field is available for the following logs: Email traffic, Spam, and Email filters.</td>
</tr>
<tr>
<td>Sender Email</td>
<td>The email address of the sender that is queried.&lt;br&gt;This field is available only for the Email traffic log.</td>
</tr>
</tbody>
</table>
4. Click one of the following action buttons:
   - **Search.** Query the log according to the search criteria that you specified and view the log through the Web Management Interface, that is, onscreen.
   - **Download.** Query the log according to the search criteria that you specified, and download the log to a computer.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Criteria (continued)</td>
<td>Recipient Email  The email address of the recipient that is queried. This field is available for the following logs: Email traffic, Virus, Spyware, Spam, and Email filters.</td>
</tr>
<tr>
<td></td>
<td>URL/Subject  The URL and subject that are queried. This field is available for the following logs: Traffic, Virus, and Spyware.</td>
</tr>
<tr>
<td></td>
<td>URL  The URL that is queried. This field is available for the following logs: Web traffic and Content filters.</td>
</tr>
<tr>
<td></td>
<td>Category  The Web or application category that is queried. This field is available for the following logs: Content filters and Application.</td>
</tr>
<tr>
<td></td>
<td>Size  The file's minimum and maximum size (in bytes) that are queried. This field is available only for the Web traffic log.</td>
</tr>
<tr>
<td></td>
<td>Type  Select one or more check boxes to specify the system event types that are queried: Error (all system errors), Info (all informational messages), Conf (all configuration changes), and Update (all system software updates). This field is available only for the System log.</td>
</tr>
<tr>
<td></td>
<td>Event  The description of the event incident that is queried. This field is available only for the System log.</td>
</tr>
<tr>
<td></td>
<td>Section  The application group (Instant Messaging, Media Applications, Peer to Peer, or Tools) that is queried. This field is available only for the Application log.</td>
</tr>
<tr>
<td>Display</td>
<td>The maximum number of pages that are displayed. The default setting is 15 entries.</td>
</tr>
</tbody>
</table>
| Download Log (zipped) File Format | Select a radio button to specify the format in which to download the zipped log file:  
- **CSV.** Download the log file as a comma-separated values (CSV) file.  
- **HTML.** Download the log file as an HTML file. |
Example: Using Logs to Identify Infected Clients

You can use the STM logs to help identify potentially infected clients on the network. For example, clients that are generating abnormally high volumes of HTTP traffic might be infected with spyware or a virus.

To identify infected clients that are sending spyware or a virus in outbound traffic, query the STM spyware and virus logs and see if any of your internal IP addresses are the source of spyware or a virus:

1. On the Log Query screen (see Figure 111 on page 195), select Web traffic as the log type.
2. Select the start date and time from the drop-down lists.
3. Select the end date and time from the drop-down lists.
4. Next to Protocols, select the HTTP check box.
5. Click Search. After a while, the log displays onscreen.
6. Check if there are clients that are sending out suspicious volumes of data, especially to the same destination IP address, on a regular basis.

If you find a client exhibiting this behavior, you can run a query on that client’s HTTP traffic activities to get more information. Do so by running the same HTTP traffic query and entering the client IP address in the Client IP field.

Log Management

Generated logs take up space and resources on the STM internal disk. To ensure that there is always sufficient space to save newer logs, the STM automatically deletes older logs whenever the total log size reaches 50 percent of the allocated file size for each log type.

Automated log purging means that you do not need to constantly manage the size of the STM logs and ensures that the latest malware incidents and traffic activities are always recorded.

Note: The STM saves its logs every 5 minutes. If a power failure affects the STM, logs that were created within the 5-minute period before the power failure occurred are lost. Therefore, NETGEAR recommends that you connect the STM to a syslog server to save the logs externally.

For information about how to manually purge selected logs, see Clearing Logs on page 182.
Viewing, Scheduling, and Generating Reports

The extensive reporting functions of the STM let you perform the following tasks that help you to monitor the protection of the network and the performance of the STM:

- Generating, viewing, and downloading Web, email, application, and system reports
- Scheduling automatic Web, email, application, and system reports, and emailing these reports to specified recipients

You can view the reports onscreen, download them to your computer, and configure the STM to send them to one or more email addresses.

The STM provides preconfigured report templates. As an option, you can apply advanced filtering options to specify the number of top entries to be included, the chart type, and the output format, and you can filter the report on the following components:

- Client IP addresses
- Users
- Destinations

Because of the size and nature of the Reports screen, it is divided and presented in this manual in several figures that are explained in the following sections:

- Report Templates on this page
- Generating Reports for Downloading on page 202
- Scheduling Automatic Generation and Emailing of Reports on page 203
- Advanced Report Filtering Options on page 204

Report Templates

The STM provides preconfigured report templates in four categories:

- Web Activity
- Email Activity
- Application Activity
- System Information
To display the report templates and view reports onscreen:

1. Select **Monitoring > Reports** from the menu. The Reports screen displays. The following figure shows only the Report Templates section of the screen with the preconfigured report templates.

   ![Report Templates](image)

   **Figure 112.**

   2. Click the red **More** button for a report category to display the advanced report templates for that category. The System Information category contains only a single report template.

   3. Click **View** for a report to display the selected report onscreen. To set a time range and advanced filtering options for a report, see the following sections.

For detailed information about report templates, including what type of information is presented in each report and what type of advanced filtering you can apply to each report, see *Appendix A, Report Templates.*
Generating Reports for Downloading

To generate a report:

1. Select Monitoring > Reports from the menu. The Reports screen displays. By default, the Generate Report radio button is selected. The following figure shows the Reports screen without the Template Reports section, and shows some samples in the Generated Report List.

![Reports Screen](image)

**Figure 113.**

2. In the Filtering Options section of the screen, make your selections from the Time Range drop-down lists. Specify a start date and time and an end date and time. For advanced filtering options, see Advanced Report Filtering Options on page 204.

3. In the Report Templates section of the screen, select the check boxes for the reports that you want to generate. For information, see Report Templates on page 200 and Appendix A, Report Templates.

4. In the Generate Report section of the screen, click Generate. After a short while, the report is added to the Generated Report List. This list can contain a maximum of 12 saved reports. (To delete a previously saved report, click its Delete table button in the Action column.)

5. Download the new report (or a previously saved report) by clicking its Download table button in the Action column.

   The report is downloaded as a zipped file. By default, the zipped file contains MHTML files. However, you can change the output format from the Output Format drop-down list.
in the advanced filtering options section of the screen (see Advanced Report Filtering Options on page 204).

**Scheduling Automatic Generation and Emailing of Reports**

**To schedule a report and enable the STM to email the report:**

1. Select Monitoring > Reports from the menu. The Reports screen displays.
2. In the Report Selection section of the screen, select the Schedule Report radio button. The screen adjusts to display the scheduling and emailing options. The following figure shows the Reports screen without the Template Reports section, and with some samples in the Scheduled Report List.

3. In the Filtering Options section of the screen, make your selections from the Frequency drop-down lists to specify the frequency with which the reports are generated.
   - **Daily.** If you do not use the drop-down lists to change the time, the report is generated daily at 3:00 a.m.
• **Weekly.** By default, the report is generated weekly on Sunday at 3:00 a.m. You can use the drop-down lists to change the day of the week and the time.

• **Monthly.** If you do not use the drop-down lists to change the time, the report is generated on the first of the month at 3:00 a.m. You cannot change the day of the month.

For advanced filtering options, see *Advanced Report Filtering Options* on page 204.

4. In the Report Templates section of the screen, select the check boxes for the reports that you want to generate. For information, see *Report Templates* on page 200 and *Appendix A, Report Templates*.

5. Configure the Schedule Report section of the screen as explained in the following table:

**Table 59. Schedule Report Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Name</td>
<td>Enter a unique name for the report.</td>
</tr>
<tr>
<td>Reports to keep</td>
<td>Enter the maximum number of reports that you want to be saved in the Scheduled Report List. The maximum number of report that can be saved is 12. The default number is 5.</td>
</tr>
<tr>
<td>Send Report by Email</td>
<td>Select the <strong>Send Report by Email</strong> check box to enable the STM to send the report to the recipients that you specify in the Email Report to field.</td>
</tr>
<tr>
<td>Email Report to</td>
<td>The email addresses of the report recipients.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Use commas to separate email addresses.</td>
</tr>
</tbody>
</table>

6. Still in the Schedule Report section of the screen, click the **Add** table button to add the report to the Scheduled Report List. The report is automatically enabled, which is indicated by a green circle in the leftmost column, enabling the STM to automatically generate the report at the specified date and time.

The buttons in the Action column of the Scheduled Report List allow you perform the following actions:

• **Edit.** Opens the Edit Scheduled Report screen to let you make changes to the report.

• **Disable.** Disables the automatic generation of the report. The circle in the leftmost column turns gray.

• **Enable.** Enables the automatic generation of the report. The circle in the leftmost column turns green.

• **Delete.** Deletes the report.

**Advanced Report Filtering Options**

You can configure advanced filtering options for both generated and scheduled reports. Although the Time Range drop-down lists apply only to the generated reports and the Frequency drop-down lists apply only to the scheduled reports, the advanced filtering options
are identical for both types of reports but need to be specified separately for each generated report and each scheduled report.

**To configure advanced filtering options:**

1. Select **Monitoring > Reports** from the menu. The Reports screen displays.
2. In the Report Selection section, select one of the following radio buttons:
   - **Generate Report.**
   - **Schedule Report.**
3. Depending on the whether you selected to generate or schedule a report, perform one of the following actions:
   - If you selected Generate Report, make your selections from the Time Range drop-down lists.
   - If you selected Schedule Report, make your selections from the Frequency drop-down lists.
4. In the Filtering Options section of the screen, click **Show Advanced Options**. The following figure shows only the advanced options of the Filtering Options section of the screen.

![Figure 115](image_url)

**Figure 115.**
5. Configure the advanced filtering options as explained in the following table:

**Table 60. Advanced Filtering Options Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Count</td>
<td>Enter a number between 1 and 100 to specify how many entries are included in reports that provide a top count, such as the Top Users by Requests report or the Top Spam Senders by Requests report. The default number is 10, which means that 10 users are included in the Top Users by Requests report and 10 senders are included in the Top Spam Senders by Requests report.</td>
</tr>
<tr>
<td>Chart Type</td>
<td>Specify the type of chart that is generated in the report by making one of the following selections from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Vertical Bars</strong>. This is the default selection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Line</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pie</strong>.</td>
</tr>
<tr>
<td>Output Format</td>
<td>Specify the output format of the report by making one of the following selections from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• <strong>HTML</strong>. The report is generated as a zipped file that contains MIME HTML (MHTML or MTH) files. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• <strong>PDF</strong>. The report is generated as a zipped file that contains PDF files.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CSV</strong>. The report is generated as a zipped file that contains comma-separated values (CSV) files.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>To filter the report results on a client IP address, enter the IP address and optional subnet mask in the IP Address fields below the Client IP Address table, and then click the <strong>Add</strong> table button to add the IP address to the Client IP Address table. You can add multiple IP addresses to the table. To delete an entry from the Client IP Address table, select the entry, and then click the <strong>Delete</strong> table button.</td>
</tr>
<tr>
<td>User</td>
<td>To filter the report results on a user identity, make a selection from the User Type drop-down list below the User table. The screen adjusts depending on your selection; the different options are explained in the following rows in this table. After you have specified the user identity, click the <strong>Add</strong> table button to add the user to the User table. You can add multiple users to the table. Wildcards (*) are supported. To delete an entry from the User table, select the entry, and then click the <strong>Delete</strong> table button.</td>
</tr>
<tr>
<td>Authenticated</td>
<td>Enter the name of an authenticated user, or use wildcards to specify a group of users. To specify all authenticated users, enter *. Then click the <strong>Add</strong> table button. You can add multiple users to the User table.</td>
</tr>
<tr>
<td>Unauthenticated</td>
<td>You cannot further specify unauthenticated users; just click the <strong>Add</strong> table button.</td>
</tr>
</tbody>
</table>
### Table 60. Advanced Filtering Options Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Users**     | **Local User** Enter the name of a local user, or use wildcards to specify a group of users. To specify all local users, enter *.
|               | Then click the **Add** table button.                                                                                                         |
|               | Alternately, click the **Lookup** table button to open a table that displays all local users, each user with an individual Add table button that lets you add the user to the User table. You can add multiple users to the User table. |
|               | **Note:** Groups to which local users might belong are not displayed.                                                                        |
|               | **LDAP User** Select an LDAP domain from the drop-down list to the right of the User Type drop-down list. Enter the name of an LDAP user, or use wildcards to specify a group of users. |
|               | To specify all LDAP users who belong to the selected LDAP domain, enter *. Then click the **Add** table button.                                   |
|               | Alternately, click the **Lookup** table button to open a table that displays all users who belong to the selected LDAP domain, each user with an individual Add table button that lets you add the user to the User table. You can add multiple users to the User table. |
|               | **RADIUS User** Select a RADIUS domain from the drop-down list to the right of the User Type drop-down list. Enter the name of a RADIUS user, or use wildcards to specify a group of users. |
|               | To specify all RADIUS users who belong to the selected RADIUS domain, enter *. Then click the **Add** table button.                                  |
|               | Alternately, click the **Lookup** table button to open a table that displays all users who belong to the selected RADIUS domain, each user with an individual Add table button that lets you add the user to the User table. You can add multiple users to the User table. |
| **Destination** | To filter the report results on a Web destination such as a domain, Web category, or application, make a selection from the Limit drop-down list below the Destination table. The screen adjusts depending on your selection; the different options are explained in the following rows in this table. After you have specified the destination, click the **Add** table button to add the destination to the Destination table. You can add multiple destinations to the table. |
|               | To delete an entry from the Destination table, select the entry, and then click the **Delete** table button.                                    |
|               | **Domain** Enter the name of a domain or use wildcards to specify a group of domains. Then click the **Add** table button. You can add multiple domains to the Destination table. |
6. In the Report Templates section of the screen, select the check boxes for the reports that you want to generate. For information, see Report Templates on page 200 and Appendix A, Report Templates.

7. Depending on the whether you selected to generate or schedule a report, perform one of the following actions:
   - If you selected Generate Report, click Generate in the Generate Report section of the screen. For more information, see Generating Reports for Downloading on page 202.
   - If you selected Schedule Report, configure the settings in the Schedule Report section of the screen, and click the Add table button. For more information, see Scheduling Automatic Generation and Emailing of Reports on page 203.

### Viewing and Managing the Quarantine Files

Depending on the selections that you made on the screens of the Email Security and Web Security main menus (see Chapter 4, Content Filtering and Optimizing Scans), the STM intercepts and saves emails that are infected by spam and both emails and files that are infected by malware threats (viruses and spyware) to its quarantine files. You can search these files, view the search results through the Web Management Interface, and then take a variety of actions that are described in Viewing and Managing the Quarantined Spam Table on page 212 and Viewing and Managing the Quarantined Infected Files Table on page 213. You can also specify how many entries are displayed per page (the default setting is 15 entries).

---

**Note:** For information about how to specify the quarantine settings, see Managing the Quarantine Settings on page 81.
You can query and view the spam quarantine file and the malware quarantine file separately and filter the information based on a number of criteria. You can filter the spam quarantine file using the following criteria:

- Start date and time
- End date and time
- Domain name
- User name
- Source IP address
- Sender email address
- Recipient email address
- Subject
- Size of the email

You can filter the malware quarantine file using the following criteria:

- Start date and time
- End date and time
- Protocols (HTTP, HTTPS, FTP, SMTP, POP3, and IMAP)
- Domain name
- User name
- Malware name
- Client IP address
- Recipient email address
- URL or subject
- Size of the file
To query the quarantine files:

1. Select Monitoring > Quarantine from the menu. The Quarantine screen displays (see the following figure).

2. Depending on the selection that you make from the Quarantine File Type drop-down list, the screen adjusts to display the settings for the selected type of quarantine file. The following figure displays the spam quarantine file settings as an example.

3. Select the check boxes and radio buttons, make your selections from the drop-down lists, and complete the fields as explained in the following table:

**Table 61. Quarantine File Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Type</td>
<td>Select one of the following file types from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Spam.</strong> Quarantined spam that was detected through distributed spam analysis.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Malware.</strong> All quarantined spyware and viruses.</td>
</tr>
<tr>
<td>View All</td>
<td>Select one of the following radio buttons:</td>
</tr>
<tr>
<td></td>
<td>• <strong>View All.</strong> Display or download the entire selected quarantine file.</td>
</tr>
<tr>
<td>Search Criteria</td>
<td>• <strong>Search Criteria.</strong> Query the selected quarantine file by configuring the search criteria that are available for the selected file.</td>
</tr>
</tbody>
</table>
4. Click **Search**. Depending on the selected quarantine file (spam or malware), the Quarantine screen displays the Quarantined Spam table or the Quarantined Infected Files table, which are explained in the following sections.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description (or Subfield and Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Criteria</td>
<td></td>
</tr>
<tr>
<td>(continued)</td>
<td></td>
</tr>
<tr>
<td>Start Date/Time</td>
<td>From the drop-down lists, select the year, month, day, hours, and minutes for the start date and time.</td>
</tr>
<tr>
<td>End Date/Time</td>
<td>From the drop-down lists, select the year, month, day, hours, and minutes for the end date and time.</td>
</tr>
<tr>
<td>Protocols</td>
<td>Select one or more check boxes to specify the protocols that are queried (malware quarantine file only).</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain name that is queried.</td>
</tr>
<tr>
<td>User</td>
<td>The user name that is queried.</td>
</tr>
<tr>
<td>Malware Name</td>
<td>The name of the spyware or virus that is queried (malware quarantine file only).</td>
</tr>
<tr>
<td>Client IP</td>
<td>The client IP address that is queried (malware quarantine file only).</td>
</tr>
<tr>
<td>Source IP</td>
<td>The source IP address that is queried (spam quarantine file only).</td>
</tr>
<tr>
<td>Sender Email</td>
<td>The email address of the sender that is queried (spam quarantine file only).</td>
</tr>
<tr>
<td>Recipient Email</td>
<td>The email address of the recipient that is queried.</td>
</tr>
<tr>
<td>URL/Subject</td>
<td>The URL or subject that is queried (malware quarantine file only).</td>
</tr>
<tr>
<td>Subject</td>
<td>The subject that is queried (spam quarantine file only).</td>
</tr>
<tr>
<td>Size</td>
<td>The file’s minimum and maximum size (in bytes) that are queried.</td>
</tr>
<tr>
<td>Display</td>
<td>The maximum number of entries that are displayed on a page. The default setting is 15 entries.</td>
</tr>
</tbody>
</table>
Viewing and Managing the Quarantined Spam Table

When you query the spam quarantine file, the Quarantine screen with the Quarantined Spam table displays:

The Quarantined Spam table shows the following columns:

- **Check box.** Lets you select the table entry.
- **Date.** The date that the email was received.
- **Protocol.** The protocol (SMTP) in which the spam was found.
- **Domain.** The domain in which the spam was found.
- **User.** The user name that was used to log in to the STM.
- **Client IP.** The client IP address from which the spam originated.
- **From.** The email address of the sender.
- **To.** The email address of the recipient.
- **Subject.** The email subject line.
- **Size (Bytes).** The size of the email in bytes.

The following figure show the Quarantined Spam table with data. (Normally, this data does not fit on screen, and you need to scroll to see all data.)

After you have selected one or more table entries, take one of the following actions (or click the **Return** link to return to the previous screen):

- **Send as Spam.** The selected spam email files are tagged as spam for distributed spam analysis, and are sent to the intended recipients.
- **Send as Ham.** The selected spam email files are not tagged as spam for distributed spam analysis, are removed from quarantine, and are sent to the intended recipients.
• **Delete.** The selected spam email files are removed from quarantine and deleted.

**Viewing and Managing the Quarantined Infected Files Table**

When you query the malware quarantine file, the Quarantine screen with the Quarantined Infected Files table displays:

![Image](image-url)

Figure 119.

The Quarantined Infected Files table shows the following columns:

- **Check box.** Lets you select the table entry.
- **Date.** The date that the file was received.
- **Protocol.** The protocol (SMTP, POP3, IMAP, HTTP, FTP, HTTPS) in which the spyware or virus was found.
- **Domain.** The domain name that was used to log in to the STM.
- **User.** The user name that was used to log in to the STM.
- **Malware name.** The name of the spyware or virus.
- **File name.** The name of the file in which the spyware or virus was found.
- **Client IP.** The client IP address from which the spyware or virus originated.
- **Server IP.** The server IP address from which the spyware or virus originated.
- **From.** The email address of the sender.
- **To.** The email address of the recipient.
- **URL/Subject.** The URL or subject that is associated with the spyware or virus.
- **Size (Bytes).** The size of the virus or spyware file in bytes.

The following figure shows the Quarantined Infected Files table with data. (Normally, this data does not fit onscreen, and you need to scroll to see all data.)
After you have selected one or more table entries, take one of the following actions (or click the Return link to return to the previous screen):

- **Resend to Admin.** The selected malware files are removed from quarantine, zipped together as an email attachment, and then sent to the recipient that you have specified on the Email Notification Server screen (see Configuring the Email Notification Server on page 176).

- **Delete.** The selected malware files are removed from quarantine and deleted.

**User-Generated Spam Reports**

Users logging in through the User Portal Login screen can select to receive a report with intercepted spam emails that were intended for their email address.

**To send a spam report to an email address, a user should do the following:**

1. On the User Portal Login screen (see Figure 88 on page 156), click the here link in the Check your quarantined mail here section. The Send Spam Report screen displays. (The following figure shows the STM300).

2. Select the start date and time from the Begin Date/Time drop-down lists.

3. Specify the recipient’s email address in the Send to field.
4. Click **Send Report**.

The report provides summary information such as time, sender, recipient, subject, and size, and a retrieve link. The user can retrieve an individual email by clicking the internal or external retrieve link for the email. The presence of an external retrieve links (see the red box in the following figure) depends on the setting of the Set Public Host/IP Address and Port check box on the Distributed Spam Analysis screen (see *Configuring Distributed Spam Analysis* on page 102).

![Figure 122. Using Diagnostics Utilities](image)

### Using Diagnostics Utilities

The STM provides diagnostic tools that help you analyze traffic conditions and the status of the network. Two sets of tools are available:

- **Network diagnostic tools.** These tools include a ping utility, traceroute utility, and DNS lookup utility.

- **Traffic diagnostic tools.** These tools allow you to perform real-time, per-protocol traffic analysis between specific source and destination addresses and let you generate reports on network usage in your network.

**Note:** For normal operation, diagnostic tools are not required.

To display the Diagnostics screen, select **Monitoring > Diagnostics** from the menu. To facilitate the explanation of the tools, the Diagnostics screen is divided and presented in this manual in three figures (the following figure, *Figure 125* on page 217, and *Figure 126* on page 218).
Using the Network Diagnostic Tools

This section discusses the Ping or Trace an IP Address section, the Perform a DNS Lookup section, and the Test URL section of the Diagnostics screen:

![Diagnostics Screen](image)

**Figure 123. Diagnostics, screen 1 of 3**

**Sending a Ping Packet**

Use the ping utility to send a ping packet request to check the connection between the STM and a specific IP address. If the request times out (no reply is received), it usually means that the destination is unreachable. However, some network devices can be configured not to respond to a ping. The ping results are displayed on a new screen; click Back on the Windows menu bar to return to the Diagnostics screen.

**To send a ping:**

1. Locate the Ping or Trace an IP Address section on the Diagnostics screen. In the Host field, enter the IP address or host name that you want to ping.
2. Click the Ping button. The results of the ping are displayed below the Host field.

**Tracing a Route**

A traceroute lists all routers between the source (the STM) and the destination IP address.

**To send a traceroute:**

1. Locate the Ping or Trace an IP Address section on the Diagnostics screen. In the Host field, enter the IP address or host name for which you want trace the route.
2. Click the Traceroute button. The results of the traceroute are displayed below the Host field.
Looking Up a DNS Address

A Domain Name Server (DNS) converts the Internet name (for example, www.netgear.com) to an IP address. If you need the IP address of a Web, FTP, mail, or other server on the Internet, request a DNS lookup to find the IP address.

To look up a DNS address:

1. Locate the Perform a DNS Lookup section on the Diagnostics screen. In the Domain Name field, enter a domain name.
2. Click the Lookup button. The results of the lookup action are displayed below the Domain Name field.

Testing a URL

Testing a URL allows you to verify that the STM can connect to the Internet. The test performs a DNS lookup and captures the HTTP page.

To test a URL:

1. Locate the Test URL section on the Diagnostics screen. In the URL field, enter a URL.
2. Click the wget button. The results of the URL test are displayed below the URL field:

   ![Figure 124. Using the Realtime Traffic Diagnostics Tool](image)

   Using the Realtime Traffic Diagnostics Tool

   This section discusses the Realtime Traffic Diagnostics section of the Diagnostics screen:

   ![Figure 125. Diagnostics, screen 2 of 3](image)

   You can use the realtime traffic diagnostics tool to analyze traffic patterns with a network traffic analyzer tool. Depending on the network traffic analyzer tool that you use, you can find
out which applications are using most bandwidth, which users use most bandwidth, how long users are connected, and other information.

To use the realtime traffic diagnostics tool:

1. Locate the Realtime Traffic Diagnostics section on the Diagnostics screen. Select one or more check boxes to specify the protocols for which you want to capture the traffic flow. The check boxes that you can select are HTTP, SMTP, POP3, IMAP, and FTP.
2. In the Source IP Address field, enter the IP address of source of the traffic stream that you want to analyze.
3. In the Destination IP Address field, enter the IP address of the destination of the traffic stream that you want to analyze.
4. Click Start. You are prompted to save the downloaded traffic information file to your computer; however, do not save the file until you have stopped capturing the traffic flow.
5. When you want to stop capturing the traffic flow, click Stop.
6. Select a location to save the captured traffic flow. (The default file name is diagnostics.result.dat.) The file is downloaded to the location that you specify.
7. When the download is complete, browse to the download location you specified and verify that the file has been downloaded successfully.
8. Send the file to NETGEAR Technical Support for analysis.

Gathering Important Log Information and Generating a Network Statistics Report

When you request support, NETGEAR Technical Support might ask you to collect the debug logs and other information from your STM.

This section discusses the Gather Important Log Information section, Network Statistics Report section, and Reboot the System section of the Diagnostics screen:

Figure 126. Diagnostics, screen 3 of 3
Gathering Important Log Information

To gather log information about your STM:

1. Locate the Gather Important Log Information section on the Diagnostics screen. Click Download Now. You are prompted to save the downloaded log information file to your computer. The default file name is importantlog.gpg.
2. When the download is complete, browse to the download location you specified and verify that the file has been downloaded successfully.

Generating Network Statistics

The network statistic report provides a detailed overview of the network utilization in the STM managed network environment. The report allows you to see what consumes the most resources on the network.

To generate the network statistic report:

Locate the Network Statistics Report section on the Diagnostics screen. Click Generate Network Statistics. The network statistic report is sent in an email to the recipient that you have configured on the email Notification Server screen (see Configuring the Email Notification Server on page 176).

Restarting and Shutting Down the STM

You can perform a remote restart, for example, when the STM seems to have become unstable or is not operating normally.

Note: Restarting breaks any existing connections either to the STM (such as your management session) or through the STM (for example, LAN users accessing the Internet). However, connections to the Internet are automatically reestablished when possible.

To restart the STM:

Locate the Restart & Shutdown section on the Diagnostics screen (this section is not shown on any of the Diagnostics screen figures in this manual). Click the Restart button. The STM restarts. (If you can see the unit: The reboot process is complete when the Test LED on the front panel goes off.)

Note: See also Updating the Software on page 71.
**Note:** For the STM150 only, there is an alternate way to restart: Press the **Power** button on the rear panel of the STM150 (see *Rear Panel STM150* on page 20). The front panel Test LED flashes, and the STM150 reboots.

---

**To shut down the STM:**

Locate the Restart & Shutdown section on the Diagnostics screen (this section is not shown on any of the Diagnostics screen figures in this manual). Click the **Shutdown** button. The STM shuts down.

---

**WARNING!**

You can shut down the STM using the Web Management Interface, but you cannot start up the STM using the Web Management Interface.
This chapter provides troubleshooting tips and information for the STM. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

• Is the STM on?
  Go to Basic Functioning on page 223.

• Have I connected the STM correctly?
  Go to Basic Functioning on page 223.

• I cannot access the STM’s Web Management Interface.
  Go to Troubleshooting the Web Management Interface on page 224.

• A time-out occurs.
  Go to When You Enter a URL or IP Address a Time-Out Error Occurs on page 225.

• I have problems with the LAN connection.
  Go to Troubleshooting a TCP/IP Network Using a Ping Utility on page 225.

• I want to clear the configuration and start over again.
  Go to Restoring the Default Configuration and Password on page 227.

• The date or time is not correct.
  Go to Problems with Date and Time on page 228.

• I need help from NETGEAR.
  Go to Using Online Support on page 228.

Note: The STM’s diagnostic tools are explained in Using Diagnostics Utilities on page 215.
Basic Functioning

After you turn on power to the STM, check that the following sequence of events occurs:

1. When power is first applied, verify that the Power LED is on.
2. After approximately 2 minutes, verify that:
   a. The Test LED (STM150) or Status LED (STM300 and STM600) is no longer lit.
   b. The left LAN port LEDs are lit for any local ports that are connected.
   c. The left WAN port LEDs are lit for any WAN ports that are connected.

If a port’s left LED is lit, a link has been established to the connected device. If a port is connected, verify the following right LED behavior in relation to the established port speed:

• Connected to a 1000-Mbps device:
  - STM150: The right LED is green.
  - STM300: The right LED is amber.
  - STM600: The right LED is amber.

• Connected to a 100-Mbps device:
  - STM150: The right LED is amber.
  - STM300: The right LED is green.
  - STM600: The right LED is green.

• Connected to a 10-Mbps device: For all STM models, the right LED is off.

If any of these conditions does not occur, see the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your STM is turned on, make sure that the power cord is correctly connected to your STM and that the power supply adapter is correctly connected to a functioning power outlet. If the error persists, you have a hardware problem and should contact NETGEAR Technical Support.

Test LED or Status LED Never Turns Off

When the STM is powered on, the Test LED (STM150) or Status LED (STM300 and STM600) turns on for approximately 2 minutes and then turns off when the STM has completed its initialization. If the Test LED (STM150) or Status LED (STM300 and STM600) remains on, there is a fault within the STM.
If all LEDs are still on more than several minutes minute after power-up, do the following:

- Turn the power off, and then turn it on again to see if the STM recovers.
- Clear the STM’s configuration to factory defaults. Doing so sets the STM’s IP address to 192.168.1.201. This procedure is explained in *Restoring the Default Configuration and Password* on page 227.

If the error persists, you might have a hardware problem and should contact NETGEAR Technical Support.

**LAN or WAN Port LEDs Not On**

If either the LAN LEDs or WAN LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the STM and at the hub, router, or workstation.
- Make sure that power is turned on to the connected hub, router, or workstation.
- Be sure you that are using the correct cables:

  When connecting the STM’s uplink (WAN) ports to one or two devices that provide the Internet connections, use the cables that are supplied with the devices. These cables could be a standard straight-through Ethernet cables or an Ethernet crossover cables.

**Troubleshooting the Web Management Interface**

If you are unable to access the STM’s Web Management Interface from a PC on your local network, check the following:

- Check the Ethernet connection between the PC and the STM as described in the previous section (*LAN or WAN Port LEDs Not On*).
- If your STM’s IP address has been changed and you do not know the current IP address, clear the STM’s configuration to factory defaults. This sets the STM’s IP address to 192.168.1.201. This procedure is explained in *Restoring the Default Configuration and Password* on page 227.

  **Tip:** If you do not want to revert to the factory default settings and lose your configuration settings, you can restart the STM and use a sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the STM’s LAN interface address.

- Make sure that you are using the SSL https://address login rather than the http://address login.
• Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using
Internet Explorer, click Refresh to be sure that the Java applet is loaded.
• Try quitting the browser and launching it again.
• Make sure that you are using the correct login information. The factory default login name
is admin and the password is password. Make sure that Caps Lock is off when entering
this information.

If the STM does not save changes you have made in the Web Management Interface, check
the following:
• When entering configuration settings, be sure to click the Apply button before moving to
another screen, or your changes are lost.
• Click the Refresh or Reload button in the Web browser. The changes might have
occurred, but the Web browser might be caching the old configuration.

When You Enter a URL or IP Address a Time-Out Error Occurs

A number of things could be causing this situation; try the following troubleshooting steps:
• Check whether other computers on the LAN work correctly. If they do, ensure that your
computer’s TCP/IP settings are correct.
• If the computer is configured correctly but still not working, ensure that the STM is
connected and turned on. Connect to the Web Management Interface and check the
STM’s settings. If you cannot connect to the STM, see the information in the previous
section (Troubleshooting the Web Management Interface on page 224).
• If the STM is configured correctly, check your Internet connection (for example, your
modem or router) to make sure that it is working correctly.

Troubleshooting a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and firewalls contain a ping utility that sends an echo request
packet to the designated device. The device then responds with an echo reply.
Troubleshooting a TCP/IP network is made very easy by using the ping utility in your PC or
workstation.
ProSecure Web/Email Security Threat Management (STM) Appliance

Testing the LAN Path to Your STM

You can ping the STM from your PC to verify that the LAN path to the STM is set up correctly.

**To ping the STM from a PC running Windows 95 or later:**

1. From the Windows toolbar, click **Start** and select **Run**.
2. In the field provided, type `ping` followed by the IP address of the STM; for example:
   ```
   ping 192.168.1.201
   ```
3. Click **OK**. A message, similar to the following, should display:
   ```
Pinging <IP address> with 32 bytes of data
If the path is working, you will see this message:
   Reply from <IP address>: bytes=32 time=NN ms TTL=xxx
If the path is not working, you will see this message:
   Request timed out
   ```
   If the path is not functioning correctly, you could have one of the following problems:

   - **Wrong physical connections**
     - Make sure that the LAN port LED is on. If the LED is off, follow the instructions in **LAN or WAN Port LEDs Not On** on page 224.
     - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and STM.
   - **Wrong network configuration**
     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
     - Verify that the IP address for your STM and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows Run dialog box, type:

```plaintext
ping -n 10 <IP address>
```

in which `<IP address>` is the IP address of a remote device such as your ISP’s DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your STM listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC’s Network Control Panel.
• Check to see that the network address of your PC (the portion of the IP address that is specified by the netmask) is different from the network address of the remote device.
• Check that the modem or router is connected and functioning.

Restoring the Default Configuration and Password

To reset the STM to its original factory default settings:

1. Select Administration > Backup and Restore Settings from the menu. The Backup and Restore Settings screen displays.

![Backup and Restore Settings](image)

Figure 127.

2. Next to Revert to factory default settings, click the Default button.

The STM restarts. During the reboot process, the Backup & Restore Settings screen remains visible. The reboot process is complete after several minutes when the Test LED (STM150) or Status LED (STM300 and STM600) on the front panel goes off.

**WARNING!**

When you restore the factory default settings, the STM settings are erased. All scan and antispam settings are lost. Back up your settings if you intend to use them.

**Note:** After rebooting with factory default settings, the STM administrator account password is password, the guest account password is guest, and the LAN IP address is 192.168.1.201.
Note: For the STM150 only, there is an alternate way to return the settings to factory default: Using a sharp object, press and hold the Reset button on the rear panel of the STM150 (see Rear Panel STM150 on page 20) for about 10 seconds until the front panel Test LED flashes and the STM150 returns to factory default settings.

Problems with Date and Time

The System Date and Time screen displays the current date and time of day (see Configuring Date and Time Service on page 74). The STM uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The STM has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the STM, wait at least 5 minutes and check the date and time again.

- Time is off by one hour. Cause: The STM does not automatically sense daylight savings time. Go to the System Date & Time screen (Administration > System Date & Time), and select or clear the check box marked Automatically Adjust for Daylight Savings Time.

Using Online Support

The STM includes online support tools that allow NETGEAR Technical Support to securely perform diagnostics of the STM, and that let you submit suspicious files for analysis by NETGEAR. You can also access the Knowledge Base and documentation online.

Enabling Remote Troubleshooting

One of the advanced features that the STM provides is online support through a support tunnel. With this feature, NETGEAR Technical Support staff is able to analyze from a remote location any difficulty you might be experiencing with the STM and to perform advanced diagnostics. Make sure that ports 443 and 2222 are open on your firewall, and that you have the support key that was given to you by NETGEAR.
To initiate the support tunnel:

1. Select **Support > Online Support** from the menu. The Online Support screen displays:

![Online Support Screen](image)

To initiate the support tunnel:

2. In the Support Key field, enter the support key that was given to you by NETGEAR.

3. Click **Connect**. When the tunnel is established, the tunnel status field displays ON.

To terminate the tunnel, click **Disconnect**. The Tunnel Status field displays OFF.

If NETGEAR Technical Support cannot access the STM remotely, they might ask you to save a log file to your computer and then email it to NETGEAR for analysis (see *Gathering Important Log Information and Generating a Network Statistics Report* on page 218).

**Installing Hot Fixes**

NETGEAR might release hot fixes or patches if certain problems are found in any software release. When a hot fix is available, install it immediately to ensure optimum performance of the STM. Hot fixes might be released through NETGEAR resellers or might be available on the NETGEAR ProSecure website at [http://prosecure.netgear.com](http://prosecure.netgear.com).

To display information about installed hot fixes, select **Support > Hot Fixes** from the menu. The Hot Fixes screen displays:

![Hot Fixes Screen](image)
The Hot Fixes table displays the installed hot fixes with the following fields:

- **Installed At.** The date and time when the hot fix was installed on the STM.
- **Component.** The component for which the hot fix provides a patch.
- **Base Version.** The base software version for the hot fix. The hot fix cannot be installed on an earlier or later software version, but only on the software version for which it is intended.
- **Hot Fix Name.** The name of the hot fix.

**To install a hot fix:**

1. Obtain the hot fix from NETGEAR or its authorized reseller.
2. Save the hot fix file on the computer that you will use to access the STM.
3. Log in to the STM.
4. Select **Support > Hot Fixes** from the menu. The Hot Fixes screen displays (see the previous figure).
5. Next to the Import from File field, click **Browse**.
6. Navigate to the location on your computer where you have saved the hot fix file, and then select it.
7. Click **Open**. The hot fix file now appears in the Import from File field.
8. Click **Apply** to install the hot fix.
   
   The Test LED (STM150) or Status LED (STM300 and STM600) blinks during the hot fix installation.

**Sending Suspicious Files to NETGEAR for Analysis**

You can report any undetected malware file or malicious email to NETGEAR for online for analysis. The file is compressed and password protected before it is sent.
To submit a file to NETGEAR for analysis:

1. Select **Support > Malware Analysis** from the menu. The Malware Analysis screen displays:

![Malware Analysis Screen](image)

2. Complete the fields as explained in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Address</td>
<td>The email address of the submitter to enable NETGEAR to contact the submitter if needed.</td>
</tr>
<tr>
<td>Import from File</td>
<td>Click <strong>Browse</strong> to navigate to the file that you want to submit to NETGEAR.</td>
</tr>
<tr>
<td>Source / Product Model</td>
<td>Specify where the file originated (for example, an email address if received via email) and, if known, which product or scan feature (for example, the STM or a desktop antivirus application) detected the file.</td>
</tr>
<tr>
<td>Description</td>
<td>As an option, include a description or any information that is relevant.</td>
</tr>
</tbody>
</table>

3. Click **Submit**.

**Accessing the Knowledge Base and Documentation**

To access NETGEAR’s Knowledge Base for the STM, select **Support > Knowledge Base** from the menu.

To access NETGEAR’s documentation library for your STM model, select **Support > Documentation** from the menu.
The following table provides information about the preconfigured report templates. These report templates are accessible from the Reports screen (see Viewing, Scheduling, and Generating Reports on page 200).

In the Filtering Options columns of the following table, a ✓ indicates that the option is supported; an ✗ indicates that the option is not supported. Some reports require you to enable logging of HTTP traffic (for more information, see the Content Filtering screen and Configuring Web Content Filtering on page 109) so the report can provide HTTP traffic statistics. This requirement is indicated by a ✓ in the Enable logging of HTTP traffic column.

**Note:** “By hour” report templates show only the most recent 24 hours of statistics data if the selected time range is longer than one day; “By day” report templates show only the most recent 30 or 31 days of statistics data if the selected time range is longer than one month; “By month” report templates show only the most recent 12 months of statistics data if the selected time range is longer than one year.

### Table 63. Report Templates Information

<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Enable logging of HTTP traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Client IP Address</td>
<td>User</td>
</tr>
<tr>
<td>Web Activity</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Top Users by Requests</td>
<td>Top users by number of Web requests:</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>• Chart with the number of Web requests per user</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table with the following items:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- User identity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Number of Web requests</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Bandwidth usage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Top Users by Bandwidth</td>
<td>Top users by bandwidth usage:</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>• Chart with the bandwidth usage per user</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table with the following items:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- User identity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Bandwidth usage</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Number associated of Web requests</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 63. Report Templates Information (Continued)

<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Enable logging of HTTP traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Client IP Address</td>
<td>User</td>
</tr>
</tbody>
</table>
| Top Destination Domains by Requests | Top destination domains by number of requests:  
• Chart with the requests by destination domains listed  
• Table with the following items:  
  - Destination domain name  
  - Number of requests  
  - Associated bandwidth usage | ✓ ✓ ✓ ✓ | ✗ ✓ |
| Top Destination Domains by Bandwidth | Top destination domains by bandwidth usage:  
• Chart with the bandwidth usage by destination domains listed  
• Table with the following items:  
  - Destination domain name  
  - Bandwidth usage  
  - Number of associated requests | ✓ ✓ ✓ ✓ | ✗ ✓ |
| Top Web Categories by Requests | Top Web categories by number of requests:  
• Chart with the number of requests by Web category listed  
• Table with the following items:  
  - Web category  
  - Number of requests  
  - Associated bandwidth usage | ✓ ✓ ✓ ✓ | ✗ ✓ |
| Top Web Categories by Bandwidth | Top Web categories by bandwidth usage:  
• Chart with the bandwidth usage by Web category listed  
• Table with the following items:  
  - Web category  
  - Bandwidth usage  
  - Number of associated requests | ✓ ✓ ✓ ✓ | ✗ ✓ |
| Top Blocked Users by Requests | Top blocked users by number of Web requests:  
• Chart with the number of Web requests per user  
• Table with the following items:  
  - User identity  
  - Number of Web requests | ✓ ✓ ✓ ✓ | ✗ ✓ |
| Top Blocked Destination Domains by Requests | Top blocked destination domains by number of requests:  
• Chart with the number of requests by destination domain listed  
• Table with the following items:  
  - Destination domain name  
  - Number of requests | ✓ ✓ ✓ ✓ | ✗ ✓ |
<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Filter Log HTTP Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Blocked Web Categories by Requests</td>
<td>Top blocked Web categories by number of requests:</td>
<td>✅✅✅✅ ✗ ✗</td>
<td></td>
</tr>
<tr>
<td>Top Blocked Users by Web Categories</td>
<td>Top blocked users by number of Web category requests:</td>
<td>✅✅✅ ✗ ✗ ✗</td>
<td></td>
</tr>
<tr>
<td>Top Blocked Users by Blacklist</td>
<td>Top users by number of blacklisted website requests:</td>
<td>✅✅✅ ✗ ✗ ✗ ✗</td>
<td></td>
</tr>
<tr>
<td>Top Blocked Users by File Type</td>
<td>Top users by number of blocked file extension requests:</td>
<td>✅✅✅ ✗ ✗ ✗ ✗</td>
<td></td>
</tr>
<tr>
<td>Top Blocked Users by Malware</td>
<td>Top users by number of blocked malware downloads:</td>
<td>✅✅✅ ✗ ✗ ✗ ✗</td>
<td></td>
</tr>
<tr>
<td>Requests by Hour</td>
<td>For each Web server protocol separately, the number of requests per hour for the</td>
<td>✅✅✅ ✗ ✗ ✗</td>
<td></td>
</tr>
<tr>
<td></td>
<td>time range that you specify in the Filtering Options section of the Reports screen:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 63. Report Templates Information (Continued)
Table 63. Report Templates Information (Continued)

<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Enable logging of HTTP traffic</th>
</tr>
</thead>
</table>
| Requests by Day | For each Web server protocol separately, the number of requests per day for the time range that you specify in the Filtering Options section of the Reports screen:  
  • Chart with the number of Web requests per day  
  • Table with the following items:  
    - Day  
    - Number of Web requests per day  
    - Associated bandwidth usage per day | ✓ ✓ ✓ ✓× ✓ | ✓ |
| Requests by Month | For each Web server protocol separately, the number of requests per month for the time range that you specify in the Filtering Options section of the Reports screen:  
  • Chart with the number of Web requests per month  
  • Table with the following items:  
    - Month  
    - Number of Web requests per month  
    - Associated bandwidth usage per month | ✓ ✓ ✓ ✓× ✓ | ✓ |
| Bandwidth by Hour | For each Web server protocol separately, the bandwidth usage per hour for the time range that you specify in the Filtering Options section of the Reports screen:  
  • Chart with the bandwidth usage per hour  
  • Table with the following items:  
    - Hour  
    - Bandwidth usage per hour  
    - Associated number of requests per hour | ✓ ✓ ✓ ✓× ✓ | ✓ |
| Bandwidth by Day | For each Web server protocol separately, the bandwidth usage per day for the time range that you specify in the Filtering Options section of the Reports screen:  
  • Chart with the bandwidth usage per day  
  • Table with the following items:  
    - Day  
    - Bandwidth usage per day  
    - Associated number of requests per day | ✓ ✓ ✓ ✓× ✓ | ✓ |
| Bandwidth by Month | For each Web server protocol separately, the bandwidth usage per month for the time range that you specify in the Filtering Options section of the Reports screen:  
  • Chart with the bandwidth usage per month  
  • Table with the following items:  
    - Month  
    - Bandwidth usage per month  
    - Associated number of requests per month | ✓ ✓ ✓ ✓× ✓ | ✓ |
Table 63. Report Templates Information (Continued)

<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Enable logging of HTTP traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For HTTP and HTTPS separately, the number of blocked Web category requests per hour for the time range that you specify in the Filtering Options section of the Reports screen:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blocked Categories by Hour</td>
<td>• Chart with the number of blocked Web category requests per hour</td>
<td>✓ ✓ ✓ ✓ ✗ ✗</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table with the following items:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Hour</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Number of blocked Web category requests per hour</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blocked Categories by Day</td>
<td>For HTTP and HTTPS separately, the number of blocked Web category requests per day for the time range that you specify in the Filtering Options section of the Reports screen:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Chart with the number of blocked Web category requests per day</td>
<td>✓ ✓ ✓ ✓ ✗ ✗</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table with the following items:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Day</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Number of blocked Web category requests per day</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blocked Categories by Month</td>
<td>For HTTP and HTTPS separately, the number of blocked Web category requests per month for the time range that you specify in the Filtering Options section of the Reports screen:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Chart with the number of blocked Web category requests per month</td>
<td>✓ ✓ ✓ ✓ ✗ ✗</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table with the following items:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Month</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Number of blocked Web category requests per month</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blocked Files by Hour</td>
<td>For each Web server protocol separately, the number of blocked file extension requests per hour for the time range that you specify in the Filtering Options section of the Reports screen:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Chart with the number of blocked file extension requests per hour</td>
<td>✓ ✓ ✓ ✓ ✗ ✗</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table with the following items:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Hour</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Number of blocked file extension requests per hour</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blocked Files by Day</td>
<td>For each Web server protocol separately, the number of blocked file extension requests per day for the time range that you specify in the Filtering Options section of the Reports screen:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Chart with the number of blocked file extension requests per day</td>
<td>✓ ✓ ✓ ✓ ✗ ✗</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table with the following items:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Day</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Number of blocked file extension requests per day</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 63. Report Templates Information (Continued)

<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Enable logging of HTTP traffic</th>
</tr>
</thead>
</table>
| Blocked Files By Month        | For each Web server protocol separately, the number of blocked file extension requests per month for the time range that you specify in the Filtering Options section of the Reports screen:  
  • Chart with the number of blocked file extension requests per month  
  • Table with the following items:  
    - Month  
    - Number of blocked file extension requests per month                                                                                                                                                                                                                                         | ✓      | ✓      | ✓      | x      |
| Top Infected Malwares         | Top malware by number of detected infections or infection attempts received over Web requests:  
  • A chart with the number of detected infections or infection attempts per malware  
  • Table with the following items:  
    - Malware name  
    - Number of detected infections or infection attempts                                                                                                                                                                                                                                       | ✓      | ✓      | ✓      | x      | x      | x      |
| Top Infected Clients          | Top client IP addresses by number of detected malware infections or infection attempts received over Web requests:  
  • Chart with the number of detected malware infections or infection attempts per client IP address  
  • Table with the following items:  
    - Client IP address  
    - Number of detected malware infections or infection attempts                                                                                                                                                                                                                               | ✓      | ✓      | ✓      | x      | x      | x      |
| Infected Malwares by Hour     | For each Web server protocol separately, the number of detected malware infections or infection attempts per hour for the time range that you specify in the Filtering Options section of the Reports screen:  
  • Chart with the number of detected malware infections or infection attempts per hour  
  • Table with the following items:  
    - Hour  
    - Number of detected malware infections or infection attempts per hour                                                                                                                                                                                                                       | ✓      | ✓      | ✓      | x      | x      | x      |
| Infected Malwares by Day      | For each Web server protocol separately, the number of detected malware infections or infection attempts per day for the time range that you specify in the Filtering Options section of the Reports screen:  
  • Chart with the number of detected malware infections or infection attempts per day  
  • Table with the following items:  
    - Day  
    - Number of detected malware infections or infection attempts per day                                                                                                                                                                                                                       | ✓      | ✓      | ✓      | x      | x      | x      |
ProSecure Web/Email Security Threat Management (STM) Appliance

Table 63. Report Templates Information (Continued)

<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Enable logging of HTTP traffic</th>
</tr>
</thead>
</table>
| Infected Malwares by Month      | For each Web server protocol separately, the number of detected malware infections or infection attempts per month for the time range that you specify in the Filtering Options section of the Reports screen:  
  • Chart with the number of detected malware infections or infection attempts per month  
  • Table with the following items:  
    - Month  
    - Number of detected malware infections or infection attempts per month                                                                                             | ✓ ✓ ✓ ✗ ✗ ✗ ✗       |                                 |
| User Activity                   | Top users by number of blocked and allowed Web requests:  
  • Chart with the number of blocked and allowed Web requests per user  
  • Table with the following items:  
    - User identity  
    - Last time that the user was detected (“Last seen”)  
    - Total number of Web requests  
    - Number of allowed Web requests  
    - Number of blocked Web requests  
    - Associated bandwidth usage                                                                                                                                        | ✓ ✓ ✓ ✓ ✗           | ✓ |
| Email Activity                  | Top Spam Senders by Requests  
  For the blacklist and real-time blacklist combined and for the distributed spam analysis separately, the top spam senders by number of detected spam messages:  
  • Chart with the number of detected spam messages per sender  
  • Table with the following items:  
    - Sender’s email address  
    - Number of detected spam messages                                                                                                                                 | ✓ ✓ ✗ ✗ ✗ ✗          | ✗ |
|                                 | Top Spam Recipients by Requests  
  For the blacklist and real-time blacklist combined and for the distributed spam analysis separately, the top spam recipients by number of detected spam messages:  
  • Chart with the number of detected spam messages per recipient  
  • Table with the following items:  
    - Recipient's email address  
    - Number of detected spam messages                                                                                                                                 | ✓ ✓ ✗ ✗ ✗ ✗          | ✗ |
Table 63. Report Templates Information (Continued)

<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Enable logging of HTTP traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For SMTP and POP3 separately, the number of detected spam messages per hour for the time range that you specify in the Filtering Options section of the Reports screen:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Chart with the number of detected spam messages per hour</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table with the following items:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Hour</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Number of detected spam messages per hour</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td>For SMTP, the blacklist and real-time blacklist information is presented combined; for POP3, only blacklist information is presented; for both SMTP and POP3, the distributed spam analysis information is presented separately.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spam by Hour</td>
<td></td>
<td>✓✓ x x x x x</td>
<td></td>
</tr>
<tr>
<td>Spam by Day</td>
<td>For SMTP and POP3 separately, the number of detected spam messages per day</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Chart with the number of detected spam messages per day</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table with the following items:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Day</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Number of detected spam messages per day</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td>For SMTP, the blacklist and real-time blacklist information is presented combined; for POP3, only blacklist information is presented; for both SMTP and POP3, the distributed spam analysis information is presented separately.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spam by Day</td>
<td></td>
<td>✓✓ x x x x x</td>
<td></td>
</tr>
<tr>
<td>Spam by Month</td>
<td>For SMTP and POP3 separately, the number of detected spam messages per month for the time range that you specify in the Filtering Options section of the Reports screen:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Chart with the number of detected spam messages per month</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table with the following items:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Month</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Number of detected spam messages per month</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td>For SMTP, the blacklist and real-time blacklist information is presented combined; for POP3, only blacklist information is presented; for both SMTP and POP3, the distributed spam analysis information is presented separately.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spam by Month</td>
<td></td>
<td>✓✓ x x x x x</td>
<td></td>
</tr>
</tbody>
</table>
Table 63. Report Templates Information (Continued)

<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Enable logging of HTTP traffic</th>
</tr>
</thead>
</table>
| Email Messages by Hour | For each email server protocol separately, the number of email messages per hour for the time range that you specify in the Filtering Options section of the Reports screen:  
  • Chart with the number of email messages per hour  
  • Table with the following items:  
    - Hour  
    - Number of email messages per hour  
    - Associated bandwidth usage per hour | ✓ ✓ ✗ ✗ ✗ ✗ ✗ ✗ |        |
| Email Messages by Day | For each email server protocol separately, the number of email messages per day for the time range that you specify in the Filtering Options section of the Reports screen:  
  • Chart with the number of email messages per day  
  • Table with the following items:  
    - Day  
    - Number of email messages per day  
    - Associated bandwidth usage per day | ✓ ✓ ✗ ✗ ✗ ✗ ✗ ✗ |        |
| Email Messages by Month | For each email server protocol separately, the number of email messages per month for the time range that you specify in the Filtering Options section of the Reports screen:  
  • Chart with the number of email messages per month  
  • Table with the following items:  
    - Month  
    - Number of email messages per month  
    - Associated bandwidth usage per month | ✓ ✓ ✗ ✗ ✗ ✗ ✗ ✗ |        |
| Filtered Emails by Hour | For each email server protocol separately, the number of filtered email messages per hour for the time range that you specify in the Filtering Options section of the Reports screen:  
  • Chart with the number of filtered email messages per hour  
  • Table with the following items:  
    - Hour  
    - Number of filtered email messages per hour | ✓ ✓ ✗ ✗ ✗ ✗ ✗ ✗ |        |
| Filtered Emails by Day | For each email server protocol separately, the number of filtered email messages per day for the time range that you specify in the Filtering Options section of the Reports screen:  
  • Chart with the number of filtered email messages per day  
  • Table with the following items:  
    - Day  
    - Number of filtered email messages per day | ✓ ✓ ✗ ✗ ✗ ✗ ✗ ✗ |        |
### Table 63. Report Templates Information (Continued)

<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Enable logging of HTTP traffic</th>
</tr>
</thead>
</table>
| Filtered Emails by Month        | For each email server protocol separately, the number of filtered email messages per month for the time range that you specify in the Filtering Options section of the Reports screen:  
- Chart with the number of filtered email messages per month  
- Table with the following items:  
  - Month  
  - Number of filtered email messages per month | ✓ ✓ x x x x |                                |
| Top Infected Malwares           | Top virus or spyware by number of detected infections or infection attempts received over email messages:  
- A chart with the number of detected infections or infection attempts per malware  
- Table with the following items:  
  - Virus or spyware name  
  - Number of detected infections or infection attempts | ✓ ✓ x x x x |                                |
| Top Infected Clients            | Top client IP addresses by number of detected virus or spyware infections or infection attempts received over email messages:  
- Chart with the number of detected virus or spyware infections or infection attempts per client IP address  
- Table with the following items:  
  - Client IP address  
  - Number of detected virus or spyware infections or infection attempts | ✓ ✓ x x x x |                                |
| Infected Malwares by Hour       | For each email server protocol separately, the number of detected virus or spyware infections or infection attempts per hour for the time range that you specify in the Filtering Options section of the Reports screen:  
- Chart with the number of detected virus or spyware infections or infection attempts per hour  
- Table with the following items:  
  - Hour  
  - Number of detected virus or spyware infections or infection attempts per hour | ✓ ✓ x x x x |                                |
ProSecure Web/Email Security Threat Management (STM) Appliance

### Table 63. Report Templates Information (Continued)

<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Enable logging of HTTP traffic</th>
</tr>
</thead>
</table>
| Infected Malwares by Day                      | For each email server protocol separately, the number of detected virus or spyware infections or infection attempts per day for the time range that you specify in the Filtering Options section of the Reports screen:  
  - Chart with the number of detected virus or spyware infections or infection attempts per day  
  - Table with the following items:  
    - Day  
    - Number of detected virus or spyware infections or infection attempts per day | ✓ ✓ ✗ ✗ ✗ ✗ ✗ | ✗ ✗ ✗ ✗ ✗ ✗ ✗ |
| Infected Malwares by Month                    | For each email server protocol separately, the number of detected virus or spyware infections or infection attempts per month for the time range that you specify in the Filtering Options section of the Reports screen:  
  - Chart with the number of detected virus or spyware infections or infection attempts per month  
  - Table with the following items:  
    - Month  
    - Number of detected virus or spyware infections or infection attempts per month | ✓ ✓ ✗ ✗ ✗ ✗ ✗ | ✗ ✗ ✗ ✗ ✗ ✗ ✗ |

### Application Activity

<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Enable logging of HTTP traffic</th>
</tr>
</thead>
</table>
| Top Blocked Users by Requests                 | Top users by number of blocked application requests:  
  - Chart with the number of blocked application requests per user  
  - Table with the following items:  
    - User identity  
    - Number of blocked applications | ✓ ✓ ✗ ✗ ✗ ✗ ✗ | ✗ ✗ ✗ ✗ ✗ ✗ ✗ |
| Top Blocked Applications by Requests          | Top blocked applications by number of requests:  
  - Chart with the number of requests per blocked application  
  - Table with the following items:  
    - Application name  
    - Number of blocked requests | ✓ ✓ ✗ ✗ ✗ ✗ ✗ | ✗ ✗ ✗ ✗ ✗ ✗ ✗ |

### Application Activity, Advanced (Click +More onscreen)

<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Enable logging of HTTP traffic</th>
</tr>
</thead>
</table>
| Top Blocked Clients by Requests               | Top clients IP addresses by number of blocked applications:  
  - Chart with the number of blocked applications per client IP address  
  - Table with the following items:  
    - Client IP address  
    - Number of blocked applications | ✓ ✓ ✗ ✗ ✗ ✗ ✗ | ✗ ✗ ✗ ✗ ✗ ✗ ✗ |
Table 63. Report Templates Information (Continued)

<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Enable logging of HTTP traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Client IP Address</td>
<td>User</td>
</tr>
<tr>
<td>Blocked Applications by Hour</td>
<td>The number of blocked applications per hour for the time range that you specify in the Filtering Options section of the Reports screen: • Chart with the number of blocked applications per hour • Table with the following items: - Hour - Number of blocked applications per hour</td>
<td>✓ ✓ x x ✓ x</td>
<td></td>
</tr>
<tr>
<td>Blocked Applications by Day</td>
<td>The number of blocked applications per day for the time range that you specify in the Filtering Options section of the Reports screen: • Chart with the number of blocked applications per day • Table with the following items: - Day - Number of blocked applications per day</td>
<td>✓ ✓ x x ✓ x</td>
<td></td>
</tr>
<tr>
<td>Blocked Applications by Month</td>
<td>The number of blocked applications per month for the time range that you specify in the Filtering Options section of the Reports screen: • Chart with the number of blocked applications per month • Table with the following items: - Month - Number of blocked applications per month</td>
<td>✓ ✓ x x ✓ x</td>
<td></td>
</tr>
<tr>
<td>System Information</td>
<td><strong>Note:</strong> There is no table for this information.</td>
<td>✗ ✗ ✗ ✗ ✗ ✗ ✗</td>
<td></td>
</tr>
</tbody>
</table>

CPU & Memory Usage

<table>
<thead>
<tr>
<th>Activity</th>
<th>Information Reported</th>
<th>Filtering Options</th>
<th>Enable logging of HTTP traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU &amp; Memory Usage</td>
<td>CPU and memory usage, presented separately: • Chart with the CPU usage and the memory usage</td>
<td>✗ ✗ ✗ ✗ ✗ ✗ ✗</td>
<td></td>
</tr>
</tbody>
</table>
To return the STM to the default factory configuration settings that are shown in the following table, click the Default button on the Backup and Restore Settings screen (see Reverting to Factory Default Settings on page 70).

Table 64. STM Default Configuration Settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Login</strong></td>
<td></td>
</tr>
<tr>
<td>User Login URL</td>
<td><a href="https://192.168.1.201">https://192.168.1.201</a></td>
</tr>
<tr>
<td>Admin User Name (case-sensitive)</td>
<td>admin</td>
</tr>
<tr>
<td>Admin Login Password (case-sensitive)</td>
<td>password</td>
</tr>
<tr>
<td>Guest User Name (case-sensitive)</td>
<td>guest</td>
</tr>
<tr>
<td>Guest Login Password (case-sensitive)</td>
<td>guest</td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td></td>
</tr>
<tr>
<td>System Configuration</td>
<td>Web-based configuration and status monitoring</td>
</tr>
<tr>
<td>Required Minimum Browser versions</td>
<td>• Microsoft Internet Explorer 5.1 or later</td>
</tr>
<tr>
<td></td>
<td>• Mozilla Firefox 1.x or later</td>
</tr>
<tr>
<td></td>
<td>• Apple Safari 1.2 or later</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>To enable a computer to scan secure HTTPS traffic, you need to import the root CA certificate into your browser from the STM login screen.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>GMT (Greenwich Mean Time)</td>
</tr>
<tr>
<td>Time Adjusted for Daylight Savings Time</td>
<td>Enabled</td>
</tr>
<tr>
<td>SNMP</td>
<td>Disabled</td>
</tr>
<tr>
<td>Administration Console Port</td>
<td>RS232</td>
</tr>
</tbody>
</table>
Table 64. STM Default Configuration Settings (Continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN Connections</td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>Default address</td>
</tr>
<tr>
<td>MTU Size</td>
<td>1500</td>
</tr>
<tr>
<td>Ports</td>
<td>STM150: 5 AutoSense 10/100/1000BASE-T, RJ-45</td>
</tr>
<tr>
<td></td>
<td>STM300: 3 AutoSense 10/100/1000BASE-T, RJ-45</td>
</tr>
<tr>
<td></td>
<td>STM600: 5 AutoSense 10/100/1000BASE-T, RJ-45</td>
</tr>
<tr>
<td>LAN IP Address</td>
<td>In line transparent bridged</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

The following table shows the STM specifications.

Table 65. STM Specifications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supported Protocols</strong></td>
<td></td>
</tr>
<tr>
<td>Data Protocols</td>
<td>HTTP, HTTPS, FTP, IMAP, POP3, SMTP</td>
</tr>
<tr>
<td><strong>Power</strong></td>
<td></td>
</tr>
<tr>
<td>Worldwide</td>
<td>100–240V AC/50–60 Hz, universal input, 1.5A max.</td>
</tr>
<tr>
<td><strong>Physical Specifications</strong></td>
<td></td>
</tr>
<tr>
<td>Dimensions (H x L x W )</td>
<td>STM150: 43.5 x 258 x 440 mm (1.7 x 10.2 x 17.3 in.)</td>
</tr>
<tr>
<td></td>
<td>STM300: 44.4 x 500 x 426 mm (1.75 x 19.7 x 16.8 in.)</td>
</tr>
<tr>
<td></td>
<td>STM600: 44.4 x 500 x 426 mm (1.75 x 19.7 x 16.8 in.)</td>
</tr>
<tr>
<td>Weight</td>
<td>STM150: 3.68 kg (8.1 lb.)</td>
</tr>
<tr>
<td></td>
<td>STM300: 8.2 kg (18.1 lb.)</td>
</tr>
<tr>
<td></td>
<td>STM600: 8.2 kg (18.1 lb.)</td>
</tr>
<tr>
<td>From Factor</td>
<td>1U</td>
</tr>
<tr>
<td><strong>Environmental Specifications</strong></td>
<td></td>
</tr>
<tr>
<td>Operating temperature</td>
<td>0° to 40° C (32° to 104° F)</td>
</tr>
<tr>
<td>Storage temperature</td>
<td>–20° to 70° C (–4° to 70° F)</td>
</tr>
<tr>
<td>Operating humidity</td>
<td>5–95% maximum relative humidity, noncondensing</td>
</tr>
<tr>
<td>Meets requirements of</td>
<td>RoHS</td>
</tr>
</tbody>
</table>
### Table 65. STM Specifications (Continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Electromagnetic Emissions</strong></td>
<td></td>
</tr>
<tr>
<td>Meets requirements of</td>
<td>FCC Part 15 Class A</td>
</tr>
<tr>
<td></td>
<td>VCCI Class A</td>
</tr>
<tr>
<td></td>
<td>CE mark, commercial</td>
</tr>
<tr>
<td><strong>Safety</strong></td>
<td></td>
</tr>
<tr>
<td>Meets requirements of</td>
<td>UL listed</td>
</tr>
<tr>
<td></td>
<td>C-Tick</td>
</tr>
</tbody>
</table>
This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

<table>
<thead>
<tr>
<th>Document</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparing Your Network</td>
<td><a href="http://documentation.netgear.com/enu/wsdhcp/index.htm">http://documentation.netgear.com/enu/wsdhcp/index.htm</a></td>
</tr>
<tr>
<td>Glossary</td>
<td><a href="http://documentation.netgear.com/enu/glossary/index.htm">http://documentation.netgear.com/enu/glossary/index.htm</a></td>
</tr>
</tbody>
</table>
Notification of Compliance

NETGEAR Wired Products

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National
laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to
comply with the applicable requirements may result in unlawful operation and adverse action
against the end-user by the applicable National regulatory authority.

This product’s firmware limits operation to only the channels allowed in a particular Region or
Country. Therefore, all options described in this user’s guide may not be available in your version
of the product.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with
approved antennas only. Any product changes or modifications will invalidate all applicable
regulatory certifications and approvals

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two
conditions: (1) This device may not cause harmful interference, and (2) this device must
accept any interference received, including interference that may cause undesired operation.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled
environment. This equipment should be installed and operated with minimum distance of 20
cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or
transmitter.

FCC Declaration Of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole
responsibility that the ProSecure Web/Email Security Threat Management Appliance
STM150, STM300, or STM600 complies with Part 15 of FCC Rules.
Operation is subject to the following two conditions:

• This device may not cause harmful interference, and
• This device must accept any interference received, including interference that may cause undesired operation.

**FCC Radio Frequency Interference Warnings & Instructions**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

• Reorient or relocate the receiving antenna.
• Increase the separation between the equipment and the receiver.
• Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
• Consult the dealer or an experienced radio/TV technician for help.

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

**Canadian Department of Communications Radio Interference Regulations**

This digital apparatus, ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600, does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

**European Union**

The ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600 complies with essential requirements of EU EMC Directive 2004/108/EC and Low Voltage Directive 2006/95/EC as supported by applying the following test methods and standards:

• EN55022: 2006 / A1: 2007
• EN60950-1: 2005 2nd Edition
• EN 61000-3-2:2006
• EN 61000-3-3:1995 w/A1: 2001+A2: 2005

For the EU Declaration of Conformity, please visit: http://kb.netgear.com/app/answers/detail/a_id/11621/sno/0.
**Additional Copyrights**

<table>
<thead>
<tr>
<th>License</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Copyright (c) 2001, Dr. Brian Gladman, <a href="mailto:brg@gladman.uk.net">brg@gladman.uk.net</a>, Worcester, UK. All rights reserved. TERMS Redistribution and use in source and binary forms, with or without modification, are permitted subject to the following conditions: 1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The copyright holder's name must not be used to endorse or promote any products derived from this software without his specific prior written permission. This software is provided &quot;as is&quot; with no express or implied warranties of correctness or fitness for purpose.</td>
</tr>
<tr>
<td>OpenSSL</td>
<td>Copyright (c) 1998–2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: &quot;This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<a href="http://www.openssl.org/">http://www.openssl.org/</a>).&quot; 4. The names &quot;OpenSSL Toolkit&quot; and &quot;OpenSSL Project&quot; must not be used to endorse or promote products derived from this software without prior written permission. For written permission, contact <a href="mailto:openssl-core@openssl.org">openssl-core@openssl.org</a>. 5. Products derived from this software may not be called &quot;OpenSSL&quot; nor may &quot;OpenSSL&quot; appear in their names without prior written permission of the OpenSSL Project. 6. Redistributions of any form whatsoever must retain the following acknowledgment: &quot;This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<a href="http://www.openssl.org/">http://www.openssl.org/</a>).&quot; THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT &quot;AS IS,&quot; AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes cryptographic software written by Eric Young (<a href="mailto:eay@cryptsoft.com">eay@cryptsoft.com</a>). This product includes software written by Tim Hudson (<a href="mailto:tjh@cryptsoft.com">tjh@cryptsoft.com</a>).</td>
</tr>
</tbody>
</table>
| MD5 | Copyright (C) 1990, RSA Data Security, Inc. All rights reserved.  
License to copy and use this software is granted provided that it is identified as the “RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as “derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing the derived work.  
RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided “as is” without express or implied warranty of any kind.  
These notices must be retained in any copies of any part of this documentation and/or software. |
| PPP | Copyright (c) 1989 Carnegie Mellon University. All rights reserved.  
Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Carnegie Mellon University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.  
THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. |
This software is provided “as is,” without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:  
1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.  
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.  
3. This notice may not be removed or altered from any source distribution.  
Jean-loup Gailly: jloup@gzip.org; Mark Adler: madler@alumni.caltech.edu.  
The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files rfc1950.txt (zlib format), rfc1951.txt (deflate format), and rfc1952.txt (gzip format). For more information, see http://www.ietf.org/rfc/. |
Index

Numerics

10BaseT, 100BaseT, and 1000BaseT 55

A

AC input
  STM150 20
  STM300 21
  STM600 21
access
  preventing inherited privileges 156
  read/write and read-only 61
  remote management 64
  rules for Web access 132
action buttons (Web Management Interface) 31
activating service licenses 12, 50
Active Directory (AD)
  domains 161
  how it works 158
  overview 157
ActiveX objects 86
address binding, permanent 57, 59
administrator (admin)
  overview 61
  receiving
    alerts by email 182
    logs by email 178
    reports by email 204
  settings 63
airflow 23
alerts
  email address for sending alerts 176
  specifying alerts to send via email 182
Alexa Toolbar 86, 130
allowing
  emails 100
  URLs 118
  Web access exceptions 134
  Web categories 47, 114
antispm settings, backing up 68
antivirus
  action if infected emails 38
  user notification settings 93
application software, updating 71
applications
  activity reports 243
  control 127
  custom categories 143, 145
  logs 179, 180, 194, 196
  recent 5 and top 5 violations 188
  setting access exceptions 137
  status 187
attached devices, monitoring with SNMP 65
audio and video files
  email filtering 97
  FTP filtering 127
  Web filtering 113, 137
authenticated users 135
authentication
  methods 157
  using the DC agent 164
Auto Uplink 11
automatically updating software 72
autosensing, speed 54, 55

B

backing up settings 68
binding MAC addresses 59
BitTorrent 85, 130
blacklist
  emails 98
  URLs 118
blocking
  emails 100
  file extensions 94, 97, 109, 113, 127
  file names 94, 97
  keywords, emails 94, 96
  sites, reducing traffic 82
  URLs 118
  Web access exceptions 134
  Web categories 47, 109, 114
  Web objects 109, 113
bottom panel and label
  STM150 22
  STM300 22
  STM600 23
browsers, for Web Management Interface 28
bundle key, for registering 50
buttons (hardware)
   Power
      STM150 20
      STM300 21
      STM600 21
   Reset (STM150 only) 20, 71
buttons (software) 31, 32

C
   CA (Certification Authority) 76
   cache, clearing Web categories 115
   capabilities and features 9
   card, service registration 12
   categories, Web content 47, 114
   certificates
      authentication 120
      commercial CAs 77
      exchange 120
      managing 76
      NETGEAR default 78
      self-signed 77
      third party website 123
      trusted 79
      untrusted 80
   warning messages 29, 65, 121
   Certification Authority (CA) 76
   Challenge Handshake Authentication Protocol (CHAP) 157
   clearing statistics 186
   clients, identifying infected 199
   community strings, SNMP 66
   community, ProSecure™ 2
   comparison, STM models 12
   compatibility, protocols 246
   compliance
      notification of 249
      regulatory and safety 247
   compressed files
      email filtering 97
      FTP filtering 127
      Web filtering 113, 137
   concurrent number of users and scanned HTTP connections 12
   configuration
      changes, system logs 179
      settings, defaults 245
      using the Setup Wizard 32
   Configuration Manager login 155
   configuration menu (Web Management Interface) 31
   connections, concurrently scanned, HTTP 12
   console port
      STM150 20
      STM300 16
      STM600 18
   content filtering
      See also emails.
      See also Web content filtering.
      audio, compressed, executable, and video files 137
      blocked Web page, user notification settings 113, 114
      emails 94, 95
      logs 179, 180, 194, 196
      overview 84, 109
      scheduling 114
      settings, using the Setup Wizard 46
      Web 47, 112, 114
   control, applications 127
   cookies 86
   CPU usage 186
   critical updates 74
   crossover cable 11, 224

D
   dates
      setting 36, 75, 76
      troubleshooting 228
   daylight savings time 36, 76
   DC (domain controller) agent 164
   debug logs 218
   dedicated management VLAN port 12
   defaults
      configuration
         list of settings 245
         restoring 70, 227
      content filtering settings 85
      domains, for authentication 172
      IP address 34, 54
      login time-out 30
      NETGEAR certificate 78
      subnet mask 34, 54
      user name and password 29
   deployment
      rack mounting 24
      scenarios 25
      testing and verifying connectivity 49
   diagnostic tools 216
   distinguished name (DN) 158
   distributed spam analysis 102, 103
   DNS
      looking up an address 217
      server IP addresses 34, 54
Index    |    255

ProSecure Web/Email Security Threat Management (STM) Appliance documentation

online 231

reference 248
domain controller (DC) agent 164
domains

default 172

LDAP and Active Directory (AD) 161

overview 147

RADIUS 167

trusted 109

Web access exceptions, applying to 134
downlink (LAN) ports 14, 16
downloading

DC agent software 165

SSL certificate 29

STM software 73
dropped packets, session limit exceeded 57
duplex, settings 54
dust 23
dynamic MAC bindings 60

e

eDonkey 85, 130

EICAR 49
electrical noise 23

email notification server

configuring manually 176

settings, using the Setup Wizard 42

SMTP server 42, 176

emails

activity reports 239

antivirus settings 38

antivirus user notifications 93

attachments, sizes 39, 91

audio, compressed, executable, and video files, filtering 97

blocked, statistics 190

content filtering 94, 95
defaults, content filtering and scan settings 85
distributed spam analysis 102, 103

filter logs 179, 180, 194, 196

protection. See SMTP, POP3, or IMAP.

real-time blacklist 100

scanned, statistics 189

security settings, using the Setup Wizard 37

SMTP throughput (emails per hour) 12

spam protection, overview 97

traffic logs 179, 180, 194, 196

traffic statistics 186

whitelist and blacklist 98

environmental specifications 246

error, system logs 179

exceptions, Web access

custom categories 142

custom groups 139

setting rules 132

exclusions, scanning 130

executable files

e-mail filtering 97

FTP filtering 127

Web filtering 113, 137

F

facilities, syslog server 181

factory defaults

login 22

service licenses, automatic retrieval 51

settings, reverting to 70, 227

failure bypass 12

features and capabilities 9

file extensions

blocking

for emails 94, 97

for Web access 109, 113, 127

settings access exceptions 137

file names, blocking 94, 97

File Transfer Protocol. See FTP.

files, suspicious 230

filtering reports 204, 233

firmware

updating 71

versions 193

fixes, "hot" 229

Flash objects 86

forum, ProSecure™ 2

FQDN (fully qualified domain name) 65

front panel

STM150 14

STM300 16

STM600 18

FTP (File Transfer Protocol)

action, infected Web file or object 41

default port 40, 106

enabling scanning 40, 106

filtering files (audio, video, executable, and compressed) 127

sizes of files and objects 127

fully qualified domain name (FQDN) 65

G

gateway address 54

Gnutella 85, 130

Google Talk 85, 130
ProSecure Web/Email Security Threat Management (STM) Appliance

GoToMyPC 86, 130

groups
  by IP address and subnet, managing 151
  by IP membership, authentication 135, 141
  by name, managing 149
  local 135, 141
  membership 148
  overview 147
Web access exceptions
  applying to 134
  creating custom groups 139

guest users 61, 63

guidelines, performance and sizing 12

H

hard disk usage 186

Hard drive (HDD) LED
STM150, not applicable
STM300 17
STM600 19

hardware
  serial number 193
STM150
  bottom panel and label 22
  front panel 14
  LEDs 15, 223, 224
  rear panel 20
STM300
  bottom panel and label 22
  front panel 16
  LEDs 17, 223, 224
  rear panel 21
STM600
  bottom panel and label 23
  front panel 18
  LEDs 19, 223, 224
  rear panel 21

help button (Web Management Interface) 32

hosts
  public 105
  security alerts 77
  trusted
    importing 125
    SNMP 67
    specifying 124

hot fixes 229

HTML (Hypertext Markup Language), scanning 108

HTTP (Hypertext Transfer Protocol)
  action, infected Web file or object 40, 108
  default port 40, 106
  logging, traffic 112
  proxy settings
    configuring manually 61
    for HTTPS scanning 119, 123
    using the Setup Wizard 45
  scanning
    concurrent connections 12
    enabling 40, 106
    testing 49
  trusted hosts 124

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)
  action, infected Web file or object 41, 108
  default port 40, 106
  managing certificates 78
  scanning
    enabling 40, 106
    explanation of process 119
  trusted hosts 124

Hypertext Markup Language (HTML) 108

Hypertext Transfer Protocol over Secure Socket Layer. See HTTPS.

Hypertext Transfer Protocol. See HTTP.

I

ICMP (Internet Control Message Protocol) time-out 57

ICQ (instant messaging) 85, 130

IDS (intrusion detection system) 8

IETF (Internet Engineering Task Force) 65

IMAP (Internet Message Access Protocol)
  action, infected emails 38, 90
  blocking (password-protected attachments, file extensions, and file names) 96
  default port 38, 88
  enabling scanning 38, 88
  importing
    certificates 79
    trusted hosts 125
  informational messages, system logs 179
  initial configuration, Setup Wizard 32
  installation, steps 27
  instant messaging services
    configuring 130
    defaults 85
    statistics 187

interfaces
  binding to a MAC address 60
  speed and duplex settings 54
  status 193

Internet Control Message Protocol (ICMP) time-out 57

Internet Engineering Task Force (IETF) 65

Internet Message Access Protocol. See IMAP.
intrusion detection systems (IDS) and intrusion prevention systems (IPS) 8
IP addresses
- DNS servers 34, 54
- public 105
- STM 34, 54
- subnet mask, STM 34, 54
IPS (intrusion prevention system) 8
iTunes 85, 130

J
Java objects 86
Javascript 86, 113

K
KDE (MIB browser) 67
Kensington lock (STM150 only) 20
key (bundle), for registering 50
keywords, blocking in emails 94, 96
kit, rack-mounting 24
Knowledge Base 231

L
LAN default settings 246
LAN LEDs
- STM150 15
- STM300 16
- STM600 19
troubleshooting 223, 224
LAN ports
- STM150 14
- STM300 16
- STM600 19
troubleshooting 223, 224
LDAP (Lightweight Directory Access Protocol)
- binding a DN 158
- configuring a DN 162
- domains 161
- overview 157
- settings 162
- users and groups 136, 141
LEDs
Hard drive (HDD)
- STM150, not applicable
- STM300 17
- STM600 19
LAN
- STM150 15
- STM300 17
- STM600 19
locations
- STM150 14
- STM300 16
- STM600 18
Power
- STM150 15
- STM300 17
- STM600 19
Status
- STM150, not applicable
- STM300 17
- STM600 19
stop blinking (Test LED, Status LED) 193
Test (STM150 only) 15
troubleshooting 223, 224
WAN
- port speed indicators 223
- STM150 15
- STM300 17
- STM600 19
license expiration alert 182
licenses
- activating 50
- expiration dates 193
- key 12
- trial period 50
lifetime, quarantine 82
Lightweight Directory Access Protocol. See LDAP.
limits, sessions 57
listening port, DC agent 166
location, placement 23
lock, Kensington (STM150 only) 20
log information, diagnostics 219
logging
- administrator emailing options 178
- clearing 182
- email address for sending logs 176
- management 199
- querying logs 194
- search criteria 196
- selecting logs 196
- specifying logs to send via email 179
- syslog server 180
logging out users
- all active 172
- preventing inherited access privileges 156
login
- default settings 245
- time-out
- changing 62
- defaults 30
looking up DNS address 217

Index | 257
MAC addresses, binding 59
main navigation menu (Web Management Interface) 31
malware
alerts and outbreak alerts 182, 183
blocked page, user notification settings 108
detected, statistics 190
infected files, viewing 213
logs 179, 180
quarantine area size 82
quarantined
querying and viewing 209
statistics 190
recent 5 and top 5 threats 188
management
default settings 245
digital certificates 76
performance 82
Management Information Base (MiB) 67
management ports
STM150, not applicable
STM300 16
STM600 18
manually updating software 73
maximum transmission unit (MTU) settings 34, 55
media applications
configuring 130
defaults 85
status 187
memory usage 186
menu descriptions 31
MG-Soft MIB browser 67
MiB (Management Information Base), and MIB browsers 67
mIRC (instant messaging) 85, 130
misclassification, of URLs 115
models, STM 12
moisture 23
MSN Messenger 85, 130
MTU (maximum transmission unit) settings 34, 55
name, system 34, 54
NETGEAR Configuration Manager login 155
NETGEAR registration server 13
Net-SNMP (Linux Text) (MIB browser) 67
network
diagnostic tools 215, 216
refreshing 57
statistics report, diagnostics 219
Network Time Protocol (NTP), troubleshooting 228
notification settings (users)
antivirus 93
malware, blocked page 108
URLs, blocked 119
Web content filtering, blocked page 113, 114
NTP servers, settings 35, 75
online analysis, by NETGEAR 230
online documentation 231
online support 228
operating system, updating 44, 71
outbreak, malware alerts 182, 184
package contents, STM 13
packets
dropped, exceeding session limit 57
transmitted and received, statistics 190
pair of ports 12
Password Authentication Protocol (PAP) 157
password-protected attachments 94, 96
passwords
changing 62
default 29
restoring 227
pattern file
signatures 44
updating 71
peer-to-peer (P2P) services
configuring 130
defaults 85
status 187
performance and sizing guidelines 12
performance, management 82
permanent MAC bindings 60
phishing 102
physical specifications 246
pinging
ping utility, diagnostics 216
troubleshooting TCP/IP 225
placement, location 23
polling interval 186
POP3 (Post Office Protocol 3)
action, infected emails 38, 90
blocking (keywords, password-protected attachments, file extensions, and file names) 96
default port 38, 88
distributed spam analysis 103
enabling scanning 38, 88

ports
console
STM150 20
STM300 16
STM600 18
LAN
speed 223
STM150 14
STM300 16
STM600 18
locations
STM150 14
STM300 16
STM600 18
management
STM150, not applicable
STM300 16
STM600 18
public 105
WAN
STM150 14
STM300 16
STM600 18
Power button
STM150 20
STM300 21
STM600 21
Power LED
STM150 15
STM300 17
STM600 19
troubleshooting 223
power receptacle
STM150 20
STM300 21
STM600 21
power specifications, adapter 246
priorities, syslog server 181
product updates 2
ProSecure™ forum and community 2
ProSecure™ Web/Email Security Threat Management Appliance STM150, STM300, or STM600 Installation Guide 27
protocols
compatibilities 246
settings access exceptions 137
Web 105

proxies
for HTTPS scanning 119
HTTP
configuring manually 61
using the Setup Wizard 45
scanning defaults 86

Q
QQ (instant messaging) 85, 130
quarantine
infected files (malware), viewing 213
search criteria 211
settings 81
spam emails, viewing 212
viewing 208
question mark icon (Web Management Interface) 32
Quicktime 85, 130

R
rack-mount kit 24
RADIUS
domains 167
overview 157
shared secrets 168
users 136, 142
VLANs 170
RADIUS-CHAP and RADIUS-PAP 157, 168
read/write access, read-only access 61
Real Player 85, 130
real-time blacklist (RBL)
emails 100
terms of service 101
real-time clock (RTC) 35, 75
real-time protection, capabilities 10
real-time traffic, diagnostics 217
troubleshooting 228
rebooting 219
reducing traffic 82
reference documents 248
refreshing the network 57
registering with NETGEAR 50
registration information, retrieving 13
regulatory compliance 247
Remote Authentication Dial In User Service. See RADIUS.
remote management, access and configuration 64
remote troubleshooting, enabling 228
removing, embedded objects 113
reports
  email address for sending reports 176
  filtering options 204, 233
  generating 202
  scheduling 203
  templates 200, 233
  user-generated spam report 214
Web resource usage 191
Reset button, STM150 (only) 20, 71
restoring
  factory default settings 70, 227
  settings from backup file 69
Rhapsody 85, 130
routes, tracing 216
RTC (real-time clock) 35, 75
rules, Web access exceptions 132

S
safety compliance 247
scan engine
  capabilities 10
  updating 44, 71
scan settings, backing up 68
scanning
  email security settings 38
  exclusions 130
  HTML files 108
  overview 84
  size exceptions
    email attachments 39, 91
    FTP files and objects 127
    Web files and objects 41, 108
  Web security settings 40
scheduling
  content filtering 114
  reports 203
  updates 44, 71
  Web access exceptions 136
search criteria
  logs 196
  quarantine 211
Secure Socket Layer. See SSL.
security alerts, trusted or untrusted hosts 77
security subscription update settings
  configuring manually 71
  using the Setup Wizard 43
service licenses
  activating 50
  automatic retrieval 51
  expiration dates 193
  trial period 50
service registration card 12
sessions
  expiration length 171
  limits 57
  time-out 63
Setup Wizard, initial configuration 32
severities, syslog 180
shared secrets, RADIUS 168
shutting down 219
signatures, pattern file 44
Simple Mail Transfer Protocol. See SMTP.
Simple Network Management Protocol. See SNMP.
size, exceptions
  email attachments 39, 91
  FTP files and objects 127
  Web files and objects 41, 108
size, quarantine areas 82
sizing and performance, guidelines 12
SMTP (Simple Mail Transfer Protocol)
  action, infected emails 38, 89
  blocking (keywords, password-protected
    attachments, file extensions, and file names) 96
  default port 38, 88
  distributed spam analysis 103
  enabling scanning 38, 88
  server for email notification 42, 176
  throughput (emails per hours) 12
sniffer 224
SNMP (Simple Network Management Protocol)
  overview 65
  settings 66
  SNMPv1 and SNMPv2, supported 65
  traps 67
  trusted hosts 67
software updates, system logs 179
software, STM 44
spam
  blocked messages, recent 5 and top 5 188
  detected, statistics 190
  distributed spam analysis 102
  logs 179, 180, 194, 196
  protection, overview 97
  quarantine area size 82
  quarantined
    emails, viewing 212
    querying and viewing 209
    statistics 190
    real-time blacklist (RBL) 100
  reports, sending 104
  user-generated report 214
  whitelist and blacklist
  Spamhaus and Spamcop 101
  specifications, physical and technical 246
Index | 261

speed settings and autosensing 54
spyware
  
  logs 194, 196

  See also anti virus, See also emails.

SSL (Secure Socket Layer)
  
  connection and HTTPS scanning 120
  
  disabling SSLv2 connections 123
  
  encryption for LDAP 162
  
  SSLv2, SSLv3, and TLSv1 123

SSL certificates
  
  downloading 29
  
  warning message 65, 121

statistics (interfaces, service, and traffic) 189
status
  
  interfaces and Web Management Interface 193
  
  system 186, 192

Status LED
  
  STM150, not applicable
  
  STM300 17
  
  STM600 19
  
  stop blinking 193
  
  troubleshooting 223

STM150 hardware
  
  bottom panel and label 22
  
  front panel 14
  
  LEDs 15, 223, 224
  
  rear panel 20

STM300 hardware
  
  bottom panel and label 22
  
  front panel 16
  
  LEDs 17, 223, 224
  
  rear panel 21

STM600 hardware
  
  bottom panel and label 23
  
  front panel 18
  
  LEDs 19, 223, 224
  
  rear panel 21

Stream Scanning technology overview 10
streaming, scanned file parts 40, 108
submenu tabs (Web Management Interface) 31
subnet mask, STM 34, 54
support
  
  online 228
  
  technical 2

suspicous files 230
switch, power
  
  STM150 20
  
  STM300 21
  
  STM600 21

synchronization interval, DC agent 166
syslog server 180

system
  
  activity reports 244
  
  logs 179, 180, 194, 196
  
  name 34, 54
  
  status 186, 192

system date and time settings, using the Setup Wizard 35

T
table buttons (Web Management Interface) 32

tabs, submenu (Web Management Interface) 31
TCP (Transmission Control Protocol) time-out 57
TCP/IP network troubleshooting 225
technical specifications 246

technical support 2

templates, reports 200, 233
terms of service, real-time blacklist (RBL) 101

Test LED (STM150 only)
  
  description 15
  
  stop blinking 193
  
  troubleshooting 223

testing
  
  connectivity and HTTP scanning 49
  
  URLs 217

throughput
  
  SMTP (emails per hour) 12
  
  Web scan 12

time
  
  setting 36, 75, 76
  
  troubleshooting 228

time zone 36, 76

time, daylight savings
  
  applied automatically 36, 76
  
  troubleshooting 228

time-out
  
  errors 225
  
  sessions 63
  
  TCP, UDP, and ICMP 57

TLS (Transport Layer Security) 162
tools (online)
  
  configuring 130
  
  defaults 86
  
  status 187

tracing a route (traceroute) 216

trademarks 2
traffic
  
  diagnostic tools 215
  
  email and Web logs 179, 180, 194, 196
  
  real-time diagnostics 217
  
  reducing 82
  
  total scanned, in MB 189
  
  total, in bytes 188
Transmission Control Protocol (TCP) time-out 57
Transport Layer Security (TLS) 162
traps, SNMP 67
trial period, service licenses 50
troubleshooting
  basic functioning 223
  browsers 225
  configuration settings, using sniffer 224
  defaults 225
  LEDs 223, 224
  NTP 228
  remotely 228
  testing your setup 226
  time-out error 225
  Web Management Interface 224
trusted certificates 79
trusted domains 109
trusted hosts 124
trusted URLs 109

U
User Datagram Protocol (UDP) time-out 57
unauthenticated users 135
untrusted certificates 80
update failure alert 182, 183
update servers 44, 73
update settings
  backing up 68
  security subscriptions
    configuring manually 71
    using the Setup Wizard 43
updates
  critical 74
  product 2
  scheduling 44, 71
updating software 71
uplink (WAN) ports 14, 16
URLs
  blacklist 118
  blocked
    statistics 190
    user notification settings 119
  categorization 115
  custom categories 144, 145
  misclassification 115
  settings access exceptions 137
  testing 217
  trusted 109
  using wildcards 118
  whitelist 118
USB port, nonfunctioning
  STM150 14

STM300 16
STM600 18
User Datagram Protocol (UDP) time-out 57
user name, default 29
User Portal Login link 156
users
  accounts, configuring 152
  administrative (admin) 61, 63, 155
  authenticated 135, 148
  global settings 170
  guests 61, 63
  logging out 156
  number of concurrent 12
  overview 147
  searching 135, 141, 173
  special privileges 155
  unauthenticated 135, 148
  Web access exceptions, applying to 134

V
virus
  logs 194, 196
  See also malware.
VLAN port, dedicated management 12
VLANs (virtual LANs), using for authentication 170

W
WAN LEDs
  port speed indicators 223
  STM150 15
  STM300 17
  STM600 19
  troubleshooting 224
WAN ports
  STM150 14
  STM300 16
  STM600 18
warning message, SSL certificate 29, 65, 121
Weatherbug 86, 130
Web access exceptions
  custom categories 142
  custom groups 139
  setting rules 132
Web activity
  reports 233
  statistics 186
  traffic logs 179, 180, 194, 196
Web categories
  blocked, recent 5 and top 5 188
  blocking 109, 114
  blocking, using the Setup Wizard 47
  custom, for exceptions 142, 144
default settings 86
filtering, using the Setup Wizard 46
setting access exceptions 138
Web content filtering
   audio, compressed, executable, and video files 113, 137
   blocked malware, user notifications 108
   blocked page, user notifications 113, 114
   blocked URL, user notifications 119
defaults 85
files and objects, sizes 41, 108
logs 179, 180, 194, 196
overview 109
security settings, using the Setup Wizard 39
Web Management Interface 31
   browsers, qualified 28
   layout 30
   settings 34
   status 193
   troubleshooting 224
Web objects
   blocking 109, 113
default settings 86
   sizes 41, 108
Web protection. See HTTP, See HTTPS, See FTP.
Web resource usage
   monitoring 190
   reports 191
Web scanning
   defaults 85
   throughput 12
whitelist
   emails 98
   URLs 118
wildcards, using for URLs 118
Winamp 85, 130

Y
Yahoo Messenger 85, 130
Yahoo Toolbar 86, 130

Z
zone, time 36, 76