smoothwall®

The Web You Want

Smoothwall Unified Threat Management

Unified Threat Management User Portal Guide

For future reference

Unified Threat Management serial number:

Date installed:

Smoothwall contact:

Smoothwall® Unified Threat Management, User Portal Guide, October 2014

Smoothwall publishes this guide in its present form without any guarantees. This guide replaces any other guides delivered with earlier versions of Unified Threat Management.

For more information, contact: docs@smoothwall.net

Trademark notice

Acknowledgements

Smoothwall acknowledges the work, effort and talent of the Smoothwall GPL development team: Lawrence Manning and Gordon Allan, William Anderson, Jan Erik Askildt, Daniel Barron, Emma Bickley, Imran Chaudhry, Alex Collins, Dan Cuthbert, Bob Dunlop, Moira Dunne, Nigel Fenton, Mathew Frank, Dan Goscomb, Pete Guyan, Nick Haddock, Alan Hourihane, Martin Houston, Steve Hughes, Eric S. Johansson, Stephen L. Jones, Toni Kuokkanen, Luc Larochelle, Osmar Lioi, Richard Morrell, Piere-Yves Paulus, John Payne, Martin Pot, Stanford T. Prescott, Ralf Quint, Guy Reynolds, Kieran Reynolds, Paul Richards, Chris Ross, Scott Sanders, Emil Schweickerdt, Paul Tansom, Darren Taylor, Hilton Travis, Jez Tucker, Bill Ward, Rebecca Ward, Lucien Wells, Adam Wilkinson, Simon Wood, Nick Woodruffe, Marc Wormgoor.

Unified Threat Management contains graphics taken from the Open Icon Library project http://openiconlibrary.sourceforge.net/

Address	Smoothwall Limited 1 John Charles Way Leeds. LS12 6QA United Kingdom	
Email	info@smoothwall.net	
Web	www.smoothwall.net	
Telephone	USA and Canada: United Kingdom: All other countries:	1 800 959 3760 0870 1 999 500 +44 870 1 999 500
Fax	USA and Canada: United Kingdom: All other countries:	1 888 899 9164 0870 1 991 399 +44 870 1 991 399

Contents

About This Guide

This manual provides guidance for using the Unified Threat Management user portal.

Audience and Scope

This guide is aimed at general users receiving a delivery of the Unified Threat Management User Portal.

This guide assumes the following prerequisite knowledge:

- An overall understanding of the functionality of Unified Threat Management application
- Familiarity with using web browsers

Organization and Use

This guide is made up of the following chapters and appendices:

Conventions

The following typographical conventions are used in this guide:

Item	Convention	Example
Key product terms	Initial Capitals	Smoothwall Unified Threat Management
Cross-references and references to other guides	*Italics*	Refer to the *Unified Threat Management Administration Guide*
Filenames and paths	`Courier`	The `portal.xml` file
Variables that users replace	`Courier Italics`	`http://<my_ip>/portal`

To save paper, this guide is designed for double-sided printing.

Related Documentation

The following guides provide additional information relating to the Unified Threat Management application:

- *S4 and S8 Appliances Getting Started Guide*, which describes how to install Unified Threat Management on an S4, or an S8 appliance
- *S12 Appliance Getting Started Guide*, which describes how to install Unified Threat Management on an S12 appliance
- *Unified Threat Management Administration Guide*, which describes how to configure Unified Threat Management
- *Unified Threat Management Operations Guide*, which describes how to maintain Unified Threat Management
- http://www.smoothwall.net/support contains the Smoothwall support portal, knowledge base and the latest product manuals.

1 Introduction to the Unified Threat Management User Portal

This chapter provides an overview of the Unified Threat Management user portal, including:

About the Unified Threat Management User Portal

The Unified Threat Management user portal is aimed at users requiring quick access to the Unified Threat Management to carry out the following tasks:

- Generate reports
- Manage web access
- Manage Bandwidth classes — Note that this is a licensable feature
- Manage filter lists
- Use the policy tester
- Download software

Note: Some features may not be available to you. For more information, contact your Unified Threat Management system administrator.

Supported Browsers

The Unified Threat Management user portal supports the following browsers:

- Google Chrome
  - Note that Google Chrome OS is not supported
- Internet Explorer version 9 onwards
  - Note that version 11 on the Windows 8 RT platform is not supported
- Safari

Note: For information about using a browser not listed above, refer to your Smoothwall representative.

Accessing the User Portal

You access the user portal using the web browser of your choice, using login credentials provided by your Unified Threat Management system administrator.

To access the user portal do the following:

1. Start your web browser and enter the address to the user portal, using the following format:

   `http://<Unified Threat Management_IPAddress>/portal`

   where *`Unified Threat Management_IPAddress`* is the IP address for the Unified Threat Management.

   For example: `http://192.168.72.141/portal`

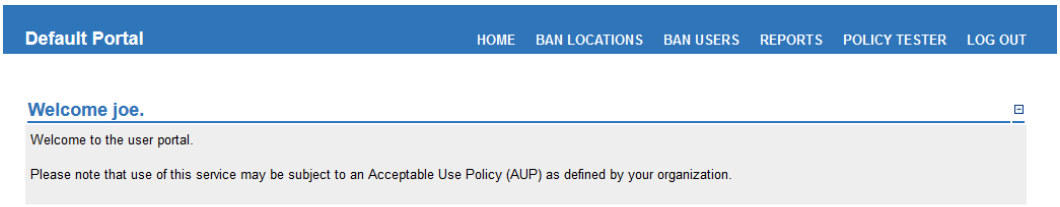
2. Click **OK** or **Proceed** to accept any certificates and other security information.

   The user portal's login page opens.

3. Enter your username and password and click **Login**.

   Your Unified Threat Management system administrator can provide the username and password for access.

   The user portal's home page opens, for example:



4. To leave the user portal, click **LOG OUT**. Unified Threat Management closes the home page and displays the login page again.

About the User Portal Home Page

The available menu options are determined by your login credentials. The following describes the menu options that may be on your Unified Threat Management user portal:

Menu Option	Description
HOME	Returns to the home page.
BAN LOCATIONS	Ban web access for specific locations. For more information, see *Banning Locations* on page 7.
BAN USERS	Temporarily bans web access for users. For more information, see *Banning Users* on page 8.
BANDWIDTH MANAGEMENT	Allows Bandwidth classes to be enabled or disabled quickly. For more information, see *Managing Bandwidth Classes* on page 9.
FILTER LIST	Accesses the Manage Filter List page. For more information, see *Customizing Filter Lists* on page 9.
POLICY TESTER	Tests if content for a specified URL will be available to a user at a specified location and time. For more information, see *Using the Policy Tester* on page 10
REPORTS	Accesses the reports page. For more information, see *Chapter 3, Working with Reports* on page 13.
LOG OUT	Logs the user out from the user portal. After you log out, you will have to log in again to use the user portal.
downloads	Displays a list of software your Unified Threat Management system administrator has made available for download from the user portal. For more information, see *Downloading Company Software* on page 11.

2 Using the Unified Threat Management Portal

This chapter describes how to use the various tasks available in the Unified Threat Management user portal, including:

Banning Locations

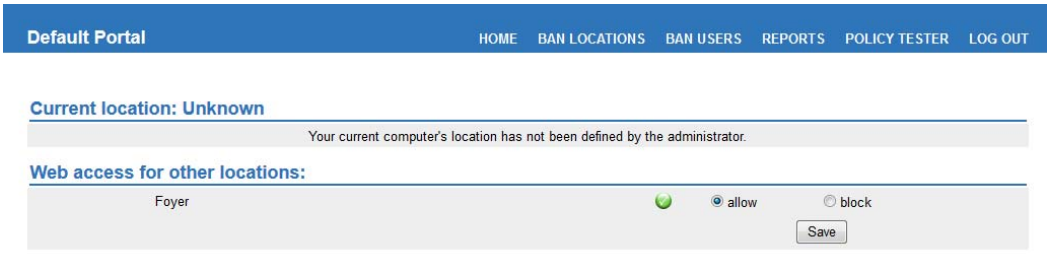
A location can either be a physical location, such as a building within a campus, or a network area, such as a subnet.

You can ban a location, and the web-enabled content at that location, from accessing the web. The ban will be in place until it is manually lifted.

To ban a location and its contents, do the following:

1. Log in to the user portal.
2. Select the **BAN LOCATIONS** menu option.

A page containing the locations you can ban is displayed, for example:



3. Locate the location you want to ban and highlight the **block** radio-button.
4. Click **Save**.

   The location, and the web-enabled content at that location, will be banned from accessing the web.
5. To lift the ban and allow web access again, locate the banned location, highlight **allow** and click **Save**.

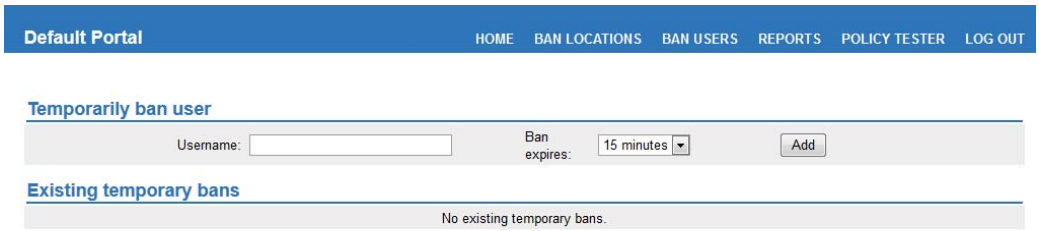
Banning Users

You can ban an individual user from accessing the web. Unlike location banning, the user ban is only for a set period of time. You cannot configure a time period for the ban.

To ban a user, do the following:

1. Log in to the user portal.
2. Select the **BAN USERS** menu option.

   The **Temporarily ban user** page opens, for example:



3. Enter the following information:
   - **Username** — Enter the username of the user you want to ban.
   - **Ban expires** — From the drop-down list, select the length of time for the ban. Valid values are: 15 minutes; 30 minutes; 45 minutes; 1 hour; 4 hours; 1 day; 1 week.
4. Click **Add**.

   The ban is enforced and current status is displayed.

Note: To lift a ban, contact your Unified Threat Management administrator.

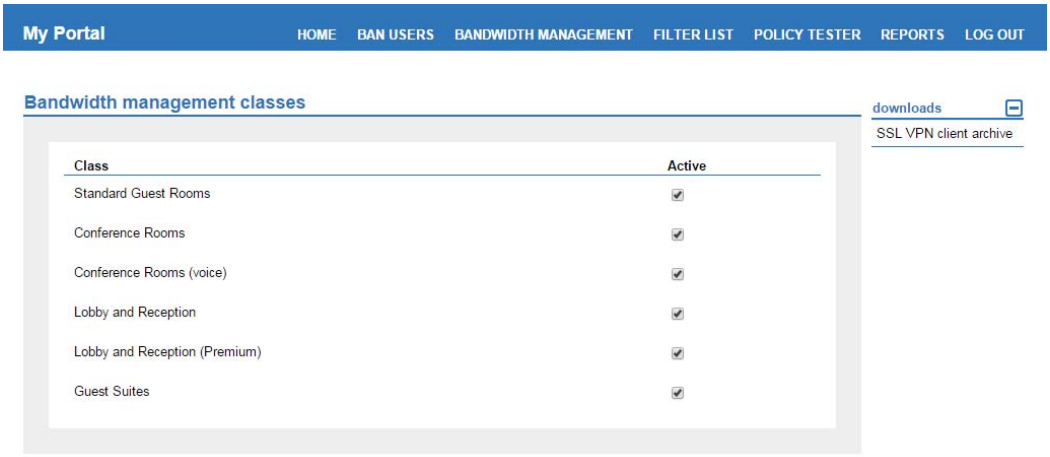
Managing Bandwidth Classes

Bandwidth is a licensed feature of your Smoothwall System. It provides you with the ability to create multi-tiered, application-aware, bandwidth shaping policies. For more information, contact your Smoothwall representative.

You can enable or disable a Bandwidth class from the user portal.

To enable or disable a Bandwidth class, do the following:

1. Log in to the user portal.
2. Select the **BANDWIDTH MANAGEMENT** menu option.



   A tick in the **Active** column indicates this class is enabled.
3. Highlight the relevant class, and either clear the selection to disable the class, or select the class to enable it.

For more information about using the Bandwidth feature, refer to the *Bandwidth Installation and Administration Guide*.

Customizing Filter Lists

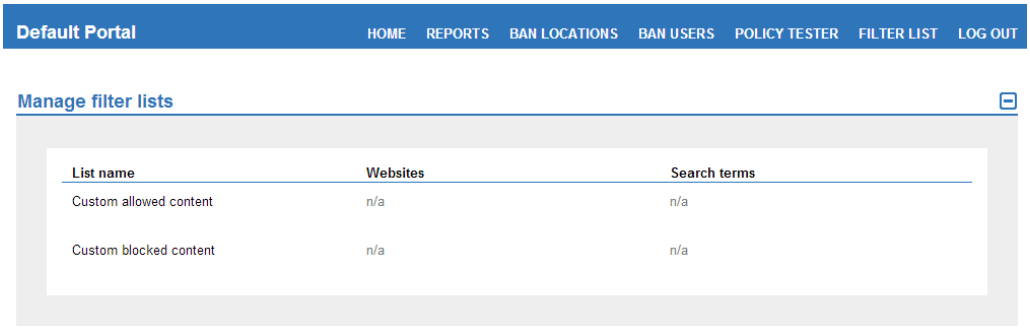
Filter lists, otherwise known as categories, are a collection of URLs, domains, and phrases. Unified Threat Management uses category groups to determine whether a user is allowed access to the content they have requested.

Within the user portal, you can add or remove URLs, domains, and phrases from filter lists.

To adjust the filter lists, do the following:

1. Log in to the user portal.

2. Select the **FILTER LIST** menu option.



3. Highlight the relevant list, and click an entry under either **Websites** or **Search terms**.
4. Either add, or remove, domains and search terms for this list.
5. Click **Save**.

Using the Policy Tester

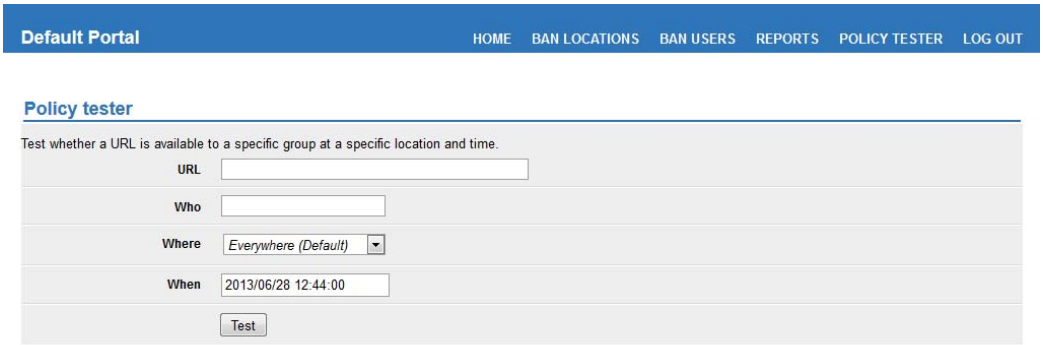
A policy is the web content filter applied to the user, designed to control the content the user is authorised to access.

Unified Threat Management's Policy tester enables you to test if a URL is allowed or blocked when requested. You can also check if a URL will be allowed or blocked for a user, a location or a time.

Tip: Use the Policy tester to check that a URL will be allowed when you need it, and to request that a blocked URL you need be unblocked by your Unified Threat Management system administrator.

To use the Policy tester, do the following:

1. Log in to the user portal.
2. Select the **POLICY TESTER** menu option to access the policy testing tool.



3. Enter the following information:

Setting	Description
URL	Enter the URL to be accessed.
Who	Optionally, enter the name of the user who will request the URL.
Where	Optionally, select the location from which the URL will be requested.

Setting	Description
When	Optionally, select at what time the URL will be requested.

4. Click **Test**.

   Unified Threat Management displays whether the URL is allowed or blocked for the option(s) you have specified.

5. Depending on your login credentials, you may be able to click **Request block** or **Request unblock** to send a request to your Unified Threat Management system administrator to block or unblock the URL.

Note: The **Request block** and **Request unblock** buttons will only be available if your Unified Threat Management system administrator has configured the portal to make them available.

Working with Reports

For a detailed description of how to run reports in a user portal, see *Chapter 3, Working with Reports* on page 13.

For a detailed description of the available reports to run in the user portal, see *Appendix A:Available Reports* on page 17.

Downloading Company Software

Your Unified Threat Management system administrator may make other company software available to download from the user portal.

To download the software, do the following:

1. Log in to the user portal.
2. In the **downloads** area, click on the software you want to download. When prompted by your browser, save the file to a suitable location.
3. Follow your system administrator's instructions on how to install and use the software.

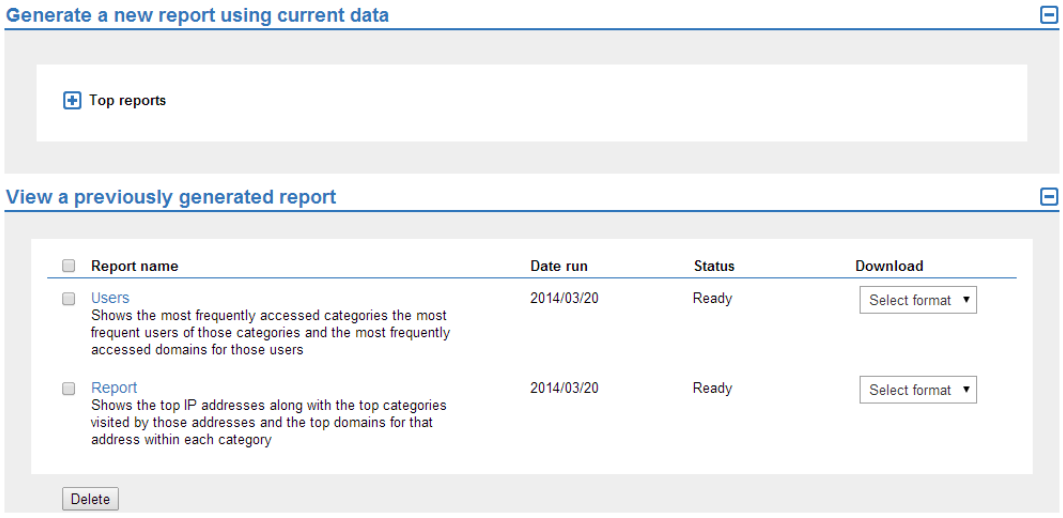
3 Working with Reports

This chapter describes how to use the reports feature of the user portal, including:

About Reports

You run reports from the **REPORTS** menu option of the user portal.

The REPORTS page is split into two panels - **Generate a new report using current data** and **View a previously generated report**:



The reports listed in the **Generate a new report using current data** panel are determined by the Unified Threat Management system administrator on setup.

View a previously generated report displays a list of reports previously run by that user login.

Note: Depending on the user portal setup, you may have the **REPORTS** panels as part of your HOME page.

Generating a New Report

To generate a new report, do the following:

1. Log in to the user portal.
2. Select the **REPORTS** menu option.
3. From the **Generate a new report using current data** panel, expand the report listings to locate the required report.
4. Click on a report name to generate it. You will be prompted to enter extra report parameters to customize the report for your operational needs, such as, a date range.

Unified Threat Management will generate the report, and provide a link to it in the **View a previously generated report** panel.

Viewing Previous Reports

Unified Threat Management saves all reports run by the user logged in, in the **View a previously generated report** panel.

The reports are listed from the most recent report run to the oldest. You can choose to display the report or to download a copy of it. The following file formats are supported:

- **csv** — Comma-separated format
- **pdf** — Portable document format, in color
- **tsv** — Tab-separated text format

To view a previously generated report, do the following:

1. Log in to the user portal.
2. Select the **REPORTS** menu option.
3. Highlight the relevant report in the **View a previously generated report** panel.
4. If a copy of the report is required, from the **Download** drop-down menu, select the required format.

   Unified Threat Management will re-generate the report, and create the requested output, either to screen or to an external file.

Deleting Reports

From time to time, you may need to reduce the number of previously generated reports saved by the user portal.

To delete a previously generated report, do the following:

1. Log in to the user portal.
2. Select the **REPORTS** menu option.
3. Within the **View a previously generated report**, locate the relevant report to delete.
4. Tick the check box next to the report.

   Note that you can select multiple reports to delete at the same time.
5. Click **Delete** to remove the reports from the list.

Appendix A: Available Reports

This appendix describes the reports available to run from Unified Threat Management.

The following table describes the report types, and shows the corresponding reports:

Report Folder	Description	Available Reports
Comparison reports	These reports provide time-based comparison of the common activity for each report type.	*Daily category comparison* on page 22
		Daily domain comparison on page 22
		Daily user comparison on page 22
Email	These reports provide an analysis of email traffic.	*Estimated cost of Spam and Malware* on page 23
		Incoming email summary incl last 24 hours on page 24
		Mailbox activity on page 24
		Malware Incl last 24 hours on page 25
		Outgoing email summary incl last 24 hours on page 25
Executive summary	These reports provide an analysis of the web traffic from specified reporting types.	*Executive summary of activity of a specific IP address* on page 23
		Executive summary of activity of a specific user on page 23
		Executive summary of all group activity on page 23

Report Folder	Description	Available Reports
Firewall and networking	These reports provide an analysis of the web traffic through your Smoothwall firewall.	*Application Bandwidth Statistics* on page 21
		Connection details and traffic statistics on page 22
		Firewall activity on page 24
		Interfaces and IP addresses on page 24
		VPN status and history on page 32
System	These reports provide an analysis of your Smoothwall System.	*Authentication Cache* on page 21
		Control page template on page 22
		Disk information on page 22
		Portal users logged in status on page 25
		Summary page template on page 25
		System information on page 26
		Updates on page 32
		Web filter statistics on page 32
Time of day activity	These reports provide an analysis of the web activity at specific times of the day.	*Times of day a group browses a specific URL* on page 27
		Times of day a user browses a specific URL on page 27
		Times of day a user browses and the categories browsed on page 27
		Times of day an IP address browses a specific URL on page 27
		Times of day an IP address browses and the categories browsed on page 28
		Times of day members of a group browses and the categories browsed on page 28
Time spent browsing	These reports provide an analysis of browsing activity.	*Amount of time a user spent browsing a URL* on page 20
		Amount of time a user spent browsing sites in a category on page 20
		Amount of time an IP address spent browsing a URL on page 20
		Amount of time an IP address spent browsing sites in a category on page 20

Report Folder	Description	Available Reports
Top reports	These reports provide an analysis of the web traffic of each report type.	*Top blocked domains by hits* on page 28
		Top blocked users by hits on page 28
		Top categories by hits and bandwidth on page 28
		Top categories by hits and bandwidth - with options on page 29
		Top client IPs by hits and bandwidth on page 29
		Top client IPs by hits and bandwidth - with options on page 29
		Top domains by hits and bandwidth on page 30
		Top domains by hits and bandwidth - with options on page 30
		Top search terms on page 30
		Top users by hits and bandwidth on page 31
		Top users by hits and bandwidth - with options on page 31
		Top users using banned search terms on page 31
User analysis	These reports provide an analysis of user activity.	*All blocked activity for a specific user* on page 20
		Bandwidth usage by a specific user on page 21
		Complete IP address audit trail on page 21
		Complete user audit trail on page 21
		Time spent browsing for a specific user on page 26
		Top search terms and the searches they were used in for a specific user on page 31

All other supplied reports have been deprecated from the Smoothwall System, but remain in the **Archive** folder for backwards compatibility.

Note: If you are using a user portal, the reports available to you are dependant on the configuration of your portal. For more information, see *Configuring a Portal* on page 35. Note that drill down reports are not available from the user portal.

The following sections describe each report in detail. The reports are listed in alphabetical order. Unless otherwise stated, all reports can be outputted to `.csv`, `.xls`, `.pdf` (either color, or black and white), and `.tsv`.

All blocked activity for a specific user

The **All blocked activity for a specific user** report lists the IP address used, the blocked URL, and the corresponding category. Blocked adverts are not included in the users' statistics.

Amount of time a user spent browsing a URL

The **Amount of time a user spent browsing a URL** report provides a graphical representation of the data.

Amount of time a user spent browsing sites in a category

The **Amount of time a user spent browsing sites in a category** report provides a graphical representation of the data.

Amount of time an IP address spent browsing a URL

The **Amount of time an IP address spent browsing a URL** report provides a graphical representation of the data.

Note: An IP address does not necessarily denote a particular user, as multiple users can use the same device depending on the setup.

Amount of time an IP address spent browsing sites in a category

The **Amount of time an IP address spent browsing sites in a category** report provides a graphical representation of the data.

Note: An IP address does not necessarily denote a particular user, as multiple users can use the same device depending on the setup.

Application Bandwidth Statistics

The **Application Bandwidth Statistics** report provides details of the bandwidth used by application groups, including:

- Measurements of the incoming and outgoing bandwidth.
- Measurements of the bandwidth used by individual IP addresses.
- Measurements of the bandwidth used by individual applications.
- Measurements of bandwidth across external interfaces, and, or, bridges.
- Application classification into groups, and bandwidth measurements of these groups. For a detailed description of each application grouping, see *Appendix B:Application Groups* on page 33.

Note: A Layer 7 licence (deep packet inspection) is required to run this report fully. Without this licence, limited information is displayed. For more information about obtaining a Layer 7 licence, refer to your Smoothwall representative.

Authentication Cache

The **Authentication Cache** report displays a list of users, and their state within the cache, during a specific date range.

Bandwidth usage by a specific user

The **Bandwidth usage by a specific user** report provides a graphical representation of the data.

Complete IP address audit trail

The **Complete IP address audit trail** report provides statistical information of all activity, including web browsing and IM activity, for a specific IP address.

To run the report for a specific IP address, click the **Advanced >>** button and enter the IP address in the **Client IP** box. Enter the required date range and click **Run report**.

Complete user audit trail

The **Complete user audit trail** report provides statistical information of all activity, including web browsing and IM activity, from a specific user.

Connection details and traffic statistics

The **Connection details and traffic statistics** report provides statistical information for inbound and outbound traffic on each interface. Information is split into the following tables:

- Interface and host bandwidth usage
- Per IP address statistics

Control page template

The **Control page template** is used on the control page. This displays control information about your Smoothwall System installation, including:

- Smoothwall System updates
- Tip of the day
- Support information, such as, serial number and license expiry dates.

Daily category comparison

The **Daily category comparison** report lists the top 50 categories accessed today, in descending order, plus their relative position for yesterday.

Daily domain comparison

The **Daily domain comparison** report lists the top 50 domains accessed today, in descending order, plus their relative position for yesterday.

Daily user comparison

The **Daily user comparison** report lists the top 50 users today, in descending order, plus their relative position for yesterday.

Disk information

The **Disk information** report displays the status of the hard drive in your Unified Threat Management, including:

- Disk information
- Processor information
- Memory information

- Disk space information (**Hard Disk Drive Info**), including how much space is taken by the system installation, and log files.

Estimated cost of Spam and Malware

The **Estimated cost of Spam and Malware** report provides the estimated return on investment of dealing with the quantity of spam and malware before it was rejected. The top originating recipients and domains are also listed.

To run the report, enter the required date range and click **Run report**.

Executive summary of activity of a specific IP address

The **Executive summary of activity of a specific IP address** report provides a graphical representation of the following activity from a specified IP address:

- The number of hits per day
- The number of hits per hour
- The total browsing time
- The top search terms, or phrases, used by the IP address
- The categories browsed

Note: An IP address does not necessarily denote a particular user, as multiple users can use the same device depending on the setup.

Executive summary of activity of a specific user

The **Executive summary for a user** report provides a graphical representation of the following activity from a specified username:

- The number of hits per day
- The number of hits per hour
- The total browsing time
- The top search terms, or phrases, used by the user
- The categories browsed

Executive summary of all group activity

The **Executive summary for all group activity** report scans all group activity, and provides a graphical representation of the number of hits from the top ten most active groups. The categories browsed by each group is also listed.

Firewall activity

The **Firewall activity** report displays important firewall activity, broken into:

- Statistics for the firewall (**main**)
- An outgoing audit (**auditoutput**)
- Port-forwarding activity (**portfw**)
- **srule**
- **srulestealth**

Incoming email summary incl last 24 hours

The **Incoming email summary incl last 24 hours** report provides a graphical representation of the number of emails received, the classification of those emails, and the bandwidth used per day. Email classifications are:

- Accepted
- Spam
- Virus

You can choose to run the report against a specific domain, or for all domains.

To run the report for a specific domain, click the **Advanced >>** button and choose the domain from the **Filter by domain** drop down list. Enter the required date range and click **Run report**.

Interfaces and IP addresses

The **Interfaces and IP addresses** report displays all external, internal, and VPN interfaces, including their connection details and DHCP leases. Information for each interface is grouped into the following tables:

- Network Address Resolution Protocol (ARP) information
- Network routing information

Mailbox activity

The **Mailbox activity** report provides a list of emails received by active mailboxes but redirected to the anti spam quarantine, and the size of the quarantine, in megabytes.The top ten quarantined users are also displayed, broken down into:

- By messages quarantined
- By messages released
- By message size

To run the report, enter the required date range and click **Run report**.

Malware Incl last 24 hours

The **Malware Incl last 24 hours** report provides a graphical representation of the number of times viruses and malware were attempted to be sent. Those received through the anti spam quarantine are also shown. The top viruses detected are also listed.

You can choose to run the report against a specific domain, or for all domains.

To run the report for a specific domain, click the **Advanced >>** button and choose the domain from the **Filter by domain** drop down list. Enter the required date range and click **Run report**.

Outgoing email summary incl last 24 hours

The **Outgoing email summary incl last 24 hours** report provides a graphical representation of the number of emails sent, the classification of those emails, and the bandwidth used per day. Email classifications are:

- Accepted
- Spam
- Virus

You can choose to run the report against a specific domain, or for all domains.

To run the report for a specific domain, click the **Advanced >>** button and choose the domain from the **Filter by domain** drop down list. Enter the required date range and click **Run report**.

Portal users logged in status

The **Portal users logged in status** report displays a list of those users who have access to the user portal, and the current state of their session.

Summary page template

The **Summary page template** provides the template for the Summary report found under **Logs and reports > Reports > Summary**. This displays summary information about your Smoothwall System installation, including:

- Alerts
- The running status of system services
- Network ARP table
- Updates for your Smoothwall System
- Tip of the day

- Summary of uptime
- Processor information
- Memory information
- Hard disk drive information
- Interface and host bandwidth usage
- Per IP address statistics
- Network routing table

System information

The **System information** report displays important information about your Unified Threat Management installation, including:

- Summary of uptime
- The ports that are in use
- System logs for:
  - Authentication service (**auth**)
  - Kernel (**kernel**)
  - System logs (**smoothwall**)
  - SSH (**ssh**)
- Loaded kernel modules
- Information about any installed Universal Power Supplies (UPS)
- Disk information
- Processor information
- Memory information
- Hard disk drive information
- The running status of system services
- Updates for your Smoothwall System

Time spent browsing for a specific user

The **Time spent browsing for a specific user** report provides a graphical representation of the data.

Time spent browsing sites in a specific category for a specific user

The **Time spent browsing sites in a specific category for a specific user** report provides a graphical representation of the data.

Times of day a group browses a specific URL

The **Times of day a group browses a specific URL** report provides a graphical representation of the data.

Note: Even though a date range can be entered, the graph only displays data for a 24-hour period. It is recommended you limit your report range to a 24-hour period.

Times of day a user browses a specific URL

The **Times of day a user browses a specific URL** report provides a graphical representation of the data.

Note: Even though a date range can be entered, the graph only displays data for a 24-hour period. It is recommended you limit your report range to a 24-hour period.

Times of day a user browses and the categories browsed

The **Times of day a user browses and the categories browsed** report provides a graphical representation of the data. The categories they have browsed, is displayed in the **Per hour** table.

Note: Even though a date range can be entered, the graph only displays data for a 24-hour period. It is recommended you limit your report range to a 24-hour period.

Times of day an IP address browses a specific URL

The **Times of day an IP address browses a specific URL** report provides a graphical representation of the data.

Note: An IP address does not necessarily denote a particular user, as multiple users can use the same device depending on the setup.

Note: Even though a date range can be entered, the graph only displays data for a 24-hour period. It is recommended you limit your report range to a 24-hour period.

Times of day an IP address browses and the categories browsed

The **Times of day an IP address browses and the categories browsed** report provides a graphical representation of the data. The categories they have browsed, is displayed in the **Per hour** table.

Note: An IP address does not necessarily denote a particular user, as multiple users can use the same device depending on the setup.

Note: Even though a date range can be entered, the graph only displays data for a 24-hour period. It is recommended you limit your report range to a 24-hour period.

Times of day members of a group browses and the categories browsed

The **Times of day members of a group browses and the categories browsed** report provides a graphical representation of the data. The categories browsed, is displayed in the **Per hour** table.

Note: Even though a date range can be entered, the graph only displays data for a 24-hour period. It is recommended you limit your report range to a 24-hour period.

Top blocked domains by hits

The **Top blocked domains by hits** report lists the top 20 blocked domains for the specified time period. By clicking a domain, you can use drill down reports to report on that domain specifically. The data is also presented as a graph, and pie chart.

Top blocked users by hits

The **Top blocked users by hits** report lists the top 20 blocked users for the specified time period.

Top categories by hits and bandwidth

The **Top categories by hits and bandwidth** report provides a graphical representation of the top 20 most frequently accessed categories. The top 20 categories are also listed according to the

amount of bandwidth used. By clicking a category, you can use drill down reports to report on that category specifically.

Top categories by hits and bandwidth - with options

The **Top categories by hits and bandwidth - with options** report is exactly the same as the *Top categories by hits and bandwidth* report, except that you can customize the report for your own operational needs. Available options are:

- **Display top** — Change the number of categories to display. Valid values are: **10**, **20**, **50**, **100**, **200**, or **500**
- **Client IP** — Enter a valid IP address to only report on the top categories browsed from that address
- **Group** — From the drop down list, choose a group to only report on the top categories browsed from that group
- **Username** — Enter a valid username to only report on the top categories browsed by that username
- **URL** — Enter a URL to only report on the top categories that the URL belongs to
- **Denied** — Select this option to only report on the top categories where browsing was blocked due to URL, or search term or phrase, filtering
- **Denied POST** — Select this option to only report on the top categories where a message, or similar, upload was blocked due to banned words or phrases

Top client IPs by hits and bandwidth

The **Top client IPs by hits and bandwidth** report provides a graphical representation of the top 20 busiest IP addresses. The top 20 IP addresses are also listed according to the amount of bandwidth used. By clicking an IP address, you can use drill down reports to report on that IP address specifically.

Top client IPs by hits and bandwidth - with options

The **Top client IPs by hits and bandwidth - with options** report is exactly the same as the *Top client IPs by hits and bandwidth* report, except that you can customize the report for your own operational needs. Available options are:

- **Display top** — Change the number of client IP addresses to display. Valid values are: **10**, **20**, **50**, **100**, **200**, or **500**
- **Category** — Enter a category to only report on those IP address that have browsed domains in that category

- **Group** — From the drop down list, choose a group to only report on those IP addresses belonging to that group
- **Exclude adverts** — Select this option to ignore hits and bandwidth used by adverts received
- **URL** — Enter a URL to only report on those IP addresses that have visited the URL
- **Denied** — Select this option to only report on the top IP addresses where browsing was blocked due to URL, or search term or phrase, filtering
- **Denied POST** — Select this option to only report on the top IP addresses where a message, or similar, upload was blocked due to banned words or phrases

Top domains by hits and bandwidth

The **Top domains by hits and bandwidth** report provides a graphical representation of the top 20 most requested domains. The top 20 domains are also listed according to the amount of bandwidth used. By clicking a domain, you can use drill down reports to report on that domain specifically.

Top domains by hits and bandwidth - with options

The **Top domains by hits and bandwidth - with options** report is exactly the same as the *Top domains by hits and bandwidth* report, except that you can customize the report for your own operational needs. Available options are:

- **Display top** — Change the number of domains to display. Valid values are: **10**, **20**, **50**, **100**, **200**, or **500**
- **Category** — Enter a category to only report on those domains in that category
- **Client IP** — Enter a valid IP address to only report on those domains requested by the IP address
- **Group** — From the drop down list, choose a group to only report on those domains visited by that group
- **Username** — Enter a valid username to only report on those domains visited by that user
- **Exclude adverts** — Select this option to ignore hits and bandwidth used by adverts received
- **Denied** — Select this option to only report on the top IP addresses where browsing was blocked due to URL, or search term or phrase, filtering
- **Denied POST** — Select this option to only report on the top IP addresses where a message, or similar, upload was blocked due to banned words or phrases

Top search terms

The **Top search terms** report lists the top 20 most frequently searched for terms or phrases.

Top search terms and the searches they were used in for a specific user

The **Top search terms and the searches they were used in for a specific user** report lists the top 50 search terms or phrases, excluding common words, used by a specific user. The searches the terms were used in is also shown.

Top users by hits and bandwidth

The **Top users by hits and bandwidth** report provides a graphical representation of the top 20 most active users by individual web page visits. The top 20 users are also listed according to the amount of bandwidth used. By clicking a username, you can use drill down reports to report on that domain specifically.

Top users by hits and bandwidth - with options

The **Top users by hits and bandwidth - with options** report is exactly the same as the *Top users by hits and bandwidth* report, except that you can customize the report for your own operational needs. Available options are:

- **Display top** — Change the number of usernames to display. Valid values are: **10**, **20**, **50**, **100**, **200**, or **500**
- **Category** — Enter a category to only report on those categories visited by the user
- **Client IP** — Enter a valid IP address to only report on web traffic originating from that IP address. Note that an IP address does not necessarily denote a particular user, as multiple users can use the same device depending on the setup.
- **Group** — From the drop down list, choose a group to only report on those members of that group
- **Exclude adverts** — Select this option to ignore hits and bandwidth used by adverts received
- **URL** — Enter a valid URL to only report on those users that have visited this particular URL
- **Denied** — Select this option to only report on the top IP addresses where browsing was blocked due to URL, or search term or phrase, filtering
- **Denied POST** — Select this option to only report on the top IP addresses where a message, or similar, upload was blocked due to banned words or phrases

Top users using banned search terms

The **Top users using banned search terms** report lists the top 20 users who have used banned search terms or phrases.

Updates

The **Updates** report displays whether updates are needed for your Smoothwall System, and the last time the blocklists were installed or updated.

VPN status and history

The **VPN status and history** report provides statistical, and historical information about the status of configured VPN tunnels. A table for each type of VPN tunnel is available, that is, IPSec, L2TP road warrior, and SSL road warrior.

To run the report, enter the required date range and click **Run report**.

Web filter statistics

The **Web filter statistics** report provides statistical information about the performance of the HTTP proxy service, and web content filter, including:

- Web cache graphs
- Web cache statistics
- Median services times for the last five minutes
- Median services times for the last 60 minutes
- The last time the blocklists were installed or updated

Appendix B: Application Groups

This appendix lists the available application groups for Bandwidth, including:

Application Groups

Application groups are classified as follows

Application Group	Applications
Databases	• Microsoft SQL • MySQL • PostgreSQL
File Transfer	• FTP
Infrastructure	• DHCP • DNS • ICMP • IGMP • Internet printing (IPP) • LDAP • Microsoft • NTP • RPC/SMB/CIFS • SNMP • Sun RPC/NFS
Mail	• IMAP • POP • SMTP
Messaging	• IRC
News	• NNTP

Application Group	Applications
Proxies	• SOCK proxy • Web proxy
Remote Access	• Remote Desktop • SSH • Telnet • VNC
Streaming Media	• SIP (VoIP)
VPN/Tunneling	• IPsec tunneling • IPv6 tunneling
Web browsing	• HTTP • HTTPS (unencryoted)

Deep Packet Inspection Application Groups

If deep packet inspection (DPI) is licensed for Bandwidth, the following additional application groups are also defined:

Application Group	Applications
Collaboration	• Citrix • Citrix GoToMyPC • GoToMeeting • Groupwise • HL7 • Lotus Notes • Lync • Meeting Maker • Microsoft ActiveSync • NetMeeting • SAP • SharePoint • WebEx
Databases	• BLIDM • CLDAP • dBase • INGRES-NET • LDAP • MaxDB • Mini SQL • MS SQL • Oracle • RIS • SVN • Sybase SQL • TDS

Application Group	Applications	
File Transfer	• ACR-NEMA • AFP • Akamai Netsession • Apple Update • AppleJuice • Ares • Astraweb • auditd • AVG • Avira • BitDefender • BitTorrent • BITS • BlazeFS • CFDPTKT • CIFS • Clubbox • Commvault • DirectConnect • Dropbox • eDonkey • Eset • FASP • F-Prot • Freenet • Giganews • Gnutella • GPFS • Google Talk File Transfer • HiveStor • iCloud • iMesh • Kaspersky • Manolito • McAfee	• MC-FTP • McIDAS • MUTE-net • NateOn File • NFA • NFS • NNTP • NovaBACKUP • OFTP • OFTPS • Paltalk File Transfer • Panda • Pando • PDbox • PDbox P2P • PFTP • Qik Upload • SBNTBCST • SFTP • Share P2P • Shareman • Skype File Transfer • SuperNews • TFTP • Usenet • Vegaa • WebDAV • WinMX • Winny • Windows Update • Xunlei • Yahoo Msg File Transfer • ZanNet
Games	• Battle.net • Quake Live	• Steam • XBox
Mail	• Exchange • gmail • InfoStore • Microsoft Mail API • Microsoft Mail Transfer Agent • Microsoft RFR • MS IMAP	• NI Mail • PCMAIL • POP2 • POP3 • Store Admin • SMTP • System Attendant

Application Group	Applications	
Messaging	• 050Plus • Aliwangwan • AIM • APNS • BaiduHi • C2DM • CISCOUC • CISUCAUD • CISUCVID • DeNA Comm • eBuddy • eBuddy XMS • Fring • Google Hangouts • Google Helpouts • Google Talk • iCall • ICQ • ISCHAT • Kakao • Kakao Audio • LINE	• Line2 • Meebo • MMS • MSMQ • MSNP • NateOn • NateOn Phone • Nokia Message • OSCAR • Paltalk • Pinger • QQ • Skype Video • Skype Voice • Snapchat • Tango • Viber • WeChat • XMPP • YiXin • Yahoo Messenger

Application Group	Applications
Networking	• Active Directory • Apple ARP • Apple • AppleShare • AppleTalk • BGMP • BGP • BJNP • Cableport AX • Cisco DRP • Cisco FNATIVE • Cisco GDP • Cisco SYSMAINT • Cisoc TNATIVE • Clearcase • DASP • DCAP • DCCP • DCE/RPC • DHCP • DHCPv6 • Diameter • DNS • FIX • GPRS Tunneling Protocol Control • GPRS Tunneling Protocol Prime • GPRS Tunneling Protocol User • FINTA • HDAP • HTTP • Ident • IGMP • ISAKMP • Java RMI • Kerberos • LLMNR • MDNS • MFTP • Microsoft Spooler Subsystem • MobileIP • MortgageWare • MUMPS • NDS Auth • Netware • NSS • NSSTP • NetBIOS Datagram Distribution Service • NetBIOS Name Service • NetBIOS Session Service • NTP • OCS • OCSP • ODMR • OSPF • PIM • PKIX Timestamp • PPP Discovery • PPP Session • Printer • PTP • RADIUS • RADIUS-ACCT • RAP • RPC2PMAP • RSVP • Rsync • SCCM • SCCP • SCTP • SEND • SSDP • SSL • STUN • Sun RPC • SVRLOC • TACACS • Teredo • Timbuktu • WCCP • WebSocket • Whois • Wyse TCX • XNS

Application Group	Applications	
Network Monitoring	• Chargen • Daytime • Discard • Echo • Finger • ICMP • ICMPv6 • Naverisk	• SMUX • SNMP • Syslog • Systat • Tivoli • Tripwire • UMA • Zabbix
Proxies	• Avocent • Freegate • Hopster • Jondo	• Privax • SOCKS • Tor • Ultrasurf
Remote Access	• Citrix CGP • Citrix ICA • Citrix IMA • Citrix Licensing • Citrix RTMPL • Citrix SLG • Citrix WANScaler • ERPC • GOM Remote • HP VMM	• KWDB • LogMeIn • PCoIP • RDP • SCCM Remote Control • ShowMyPC • Sophos RED • TeamViewer

Application Group	Applications	
Streaming Media	• Adobe Flash • FaceTime • Fring A/V • Google Talk Audio • Google Talk Video • Google Video • H.225 • H.245 • H.248 • H.323 • Hulu • Instagram Video • iTunes • Kugou • Lync Audio • Lync Media • Lync Video • MagicJack • Nate Video • NetFlix • Paltalk Video • Paltalk Voice • Pandora • PPTV • QIK • QIK Chat	• QIK Video • QuickTime • RTCP • RTMP • RTP • RTSP • RTSPS • SHOUTcast • Silverlight • Sina Video • SIP • Skype • Sopcast • Spotify • Secure RTCP • SRTP • STRP Audio • SRTP Video • T-Mobile • UltraViolet • Vonage • WhatsApp • Windows Media • Yahoo Messenger Audio • Yahoo Messenger Video
VPN/Tunneling	• AH • CyberGhost • DynGate • ESP • GRE • Hamachi • Hotspot Shield • IPComp	• IPIP • IPsec • L2TP • OpenVPN • PPTP • RSVP Tunnel • SecurityKISS • VPNReactor

Index


smoothwall®
The Web You Want