Cisco Secure Network Analytics

Desktop Client User Guide 7.4

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2021 Cisco Systems, Inc. and/or its affiliates. All Rights Reserved.

CONTENTS

1-ABOUT THIS GUIDE 11
Overview 11
How to Access Documentation for the Stealthwatch Web App 11
About the Stealthwatch Desktop Client 12
Stealthwatch Interfaces 12
How to Use This Guide 13
Documentation Icons 14
Abbreviations 15
Contacting Support 17

2-NAVIGATING THE STEALTHWATCH DESKTOP CLIENT 19
Overview 19
Client Memory Allocation 21
Your Point of View 22
Enterprise Tree and Tool Tips 23
Searching Through the Tree 24
Tree Branches 24
Alarm Severity Levels 25
Enterprise Tree Indicators 26
Tool Tips 27
Opening SMC Documents 28
Main Menu 28
File Menu 29
Edit Menu 29
View Menu 30
TTop Menu 30
Status Menu 30
Security Menu 31
Hosts Menu 31
Traffic Menu 32
Reports Menu 33
Flows Menu 33
Configuration Menu 34
Help Menu 34
Working with Documents 35
Displaying Live Data vs. Static Data 35
Tabs and Moving from One Document to Another 36

Changing Document Orientation . . . 37
Document Header . . . 39
Go to Document Buttons . . . 39
In Document Headers . . . 39
In Document Tool Bars . . . 40
Right-Clicking for Quick Focus . . . 41
Double-Clicking for Selected Documents . . . 43
Searching Documents . . . 44
Closing Documents . . . 46
Working with Tables . . . 47
Sorting Columns . . . 47
Moving and Resizing Columns . . . 48
Hiding and Showing Columns . . . 49
Exporting Data . . . 50
Multi-Section Pop-Up Menus . . . 51
Quick View . . . 52
Working with Charts . . . 54
Filtering Document Data . . . 57
Date/Time . . . 58
Hosts . . . 58
Interfaces . . . 59
Services & Applications . . . 59
Other Filter Options . . . 60
Dashboard Filters . . . 60
Printing Documents . . . 65
Print Preview . . . 65
Print Settings . . . 66
Print . . . 67
Saving Documents . . . 68
Saving Document Layouts For Future Use . . . 68
Save Document as a PDF File . . . 71
Online Help . . . 72
Contents . . . 73
Index . . . 73
Search . . . 73
Glossary . . . 74
Favorites . . . 75
Quick Search . . . 75
Keyboard Shortcuts . . . 77

3-HOST MANAGEMENT . . . 83
Overview . . . 83
Host Groups . . . 84

Catch All Host Group . . . 85
Threat Intelligence Feed Host Groups . . . 87
Information Reports Up . . . 88
Strategies for Creating Host Groups . . . 88
Creating Host Groups . . . 88
IP Addresses . . . 90
Host Group Membership . . . 92
Relational Flow Maps . . . 93

4-VIEWS AND DASHBOARDS . . . 95
Overview . . . 95
Default Dashboards in the SMC . . . 96
Host Group Dashboard . . . 99
Host Group Dashboard - Network Page . . . 100
Host Group Dashboard - Security Page . . . 101
Host Group Dashboard - Alarm Summary Page . . . 102
Building Your Own Dashboards . . . 103

5-INDEXES: RANKING BEHAVIOR CHANGES . . . 109
Overview . . . 109
Concern Index . . . 111
Target Index . . . 114
File Sharing Index . . . 116

6-MONITORING TRAFFIC AND NETWORK PERFORMANCE. 119
Overview . . . 119
Monitoring Traffic . . . 120
Internet Traffic Overview . . . 120
Corporate Network Overview . . . 122
Exporters/Network devices . . . 125
Network Performance . . . 129
Round-Trip Time . . . 130
Server Response Time . . . 131
TCP Retransmission Ratio . . . 131
Table . . . 133

7-ANALYZING FLOWS . . . 135
Overview . . . 135
Flow Filter . . . 136

Entering Flow Queries 136
Flow Table Tabs 151
Table Tab 151
Short List Tab 152
Quick View 154
Flow Analysis Scenarios 155
High Concern Index Hosts 155
Workflow Overview 155
Examining Security Event Activity (Host Snapshot) 156
Examining User Identity Information (Host Snapshot) 158
Spike in Application Traffic 159
Workflow Overview 160
Identifying the Direction of Traffic 161
Identifying the Hosts Involved 162
Identifying the Users Involved 162
Overloaded Interface 164
Workflow Overview 164
Identifying an Overloaded Interface (Interface Status) 165
Network Slow 167
Workflow Overview 167
Using the Stealthwatch IDentity to Locate an IP Address 168
Checking for Over-Utilized Interfaces (Host Snapshot) 170
Finding High Bandwidth Hosts (Interface Summary Dashboard) 172
Identifying Users Logged In to a High Bandwidth Host 172
Reviewing Top Active Flows 173
External Lookup 176
Configuring External Lookup 176
Performing an External Lookup 182

8- STEALTHWATCH THREAT INTELLIGENCE FEED 185
Overview 185
About Threat Intelligence Feed 186
How Threat Intelligence Feed Functions 187
Threat Intelligence Feed Host Groups 187
Enabling Threat Intelligence Feed 189
Threat Intelligence Security Events 190

9-FINDING THE CULPRIT 193
Overview 193
Identification Process 194
Alarm Summary 195

Alarm Table 197
Global Search 199
Getting Details from the Host Snapshot 201
Has the Host Caused Other Alarms? 203
How Widespread is the Threat? 204
Is the Behavior Normal? 208
Which Hosts Share the Same Characteristics? 209

10-RESPONDING TO ALARMS. 211
Overview 211
How to Respond to an Alarm 213
Acknowledging Alarms 213
Unacknowledging Alarms 215
Closing Alarms 215
Reopening Closed Alarms 218
Stealthwatch Mitigation Feature 219
Configuring the Mitigation Devices 220
Enabling the Mitigation Feature for Policies 223
Defining Mitigation Actions for Alarms 225
Mitigation and the Alarm Table 227
Authorize (Manual) Mode 227
Automatic Mode 228
Mitigation Actions Document 229

11-REDUCING UNNECESSARY ALARMS 231
Overview 231
Baselining 232
Host Policy Management 237
Editing Inside Hosts/Outside Hosts Default Policies 239
Effective Host Policy 241
Alarm Categories 243
Configuring Alarm Categories in Host Policies 245
Security Events 247
Configuring Security Events in Host Policies 248
Creating and Editing Policies 251
Assigning Hosts to a Pre-defined Group 252
Creating Role Policies 253
Editing Role Policies 258
Creating Host Policies 260
Editing Host Policies 264
Alarms 266

Variance-based Alarms vs. On/Off Alarms . . . 266
Settings for Variance-based Alarms . . . 269
Recommendations . . . 272
High File Sharing Index . . . 272
High Total Traffic . . . 272
High Traffic . . . 273
ICMP Flood . . . 274
Low Traffic . . . 274
Mail Relay . . . 274
Max Flows Initiated . . . 275
Max Flows Served . . . 276
New Flows Initiated . . . 276
New Flows Served . . . 277
Spam Source . . . 277
Suspect Data Loss . . . 278
Suspect Long Flow . . . 278
Suspect UDP Activity . . . 279
SYN Flood . . . 280
SYNs Received . . . 280
UDP Flood . . . 281
Worm Activity . . . 281

12-WORKING WITH DOCUMENTS . . . 283
Overview . . . 283
Saving Documents . . . 284
Login Documents . . . 286
Sharing Documents . . . 289
DAR Files . . . 289
Exporting DAR Files . . . 289
Importing DAR Files . . . 290
Public Documents . . . 291
Scheduling Documents . . . 292
Adding a New Schedule . . . 292
Editing an Existing Schedule . . . 294
Adding a Document to a Schedule . . . 295
Emailing a Scheduled Document . . . 297
Adding the Email Server to the SMC . . . 297
Adding a User's Email Address to a Schedule . . . 298
Pre-Filtering Shared Documents . . . 298
Retrieving Archived Documents . . . 301

13-DESKTOP CLIENT ROLES . . . 303
Overview . . . 303

Desktop Client Roles 304
Adding and Editing a Desktop Client role 305

INDEX 307

1

About This Guide

Overview

The primary audience for this guide is anyone who uses the Stealthwatch Desktop Client, from daily users to administrators. We assume that you already have some general understanding of networking concepts.This guide provides “best practice” guidelines for using the Stealthwatch Desktop Client to minimize network performance issues and security risks. Due to the many complexities and varieties of networks, this guide is not meant to be a comprehensive user’s guide. Rather, the intent is to provide guidance on the best ways to use the SMC software to handle and/or prevent network performance issues or threats to your network.

This chapter includes the following topics:

- How to Access Documentation for the Stealthwatch Web App
- About the Stealthwatch Desktop Client
- How to Use This Guide
- Documentation Icons
- Abbreviations

How to Access Documentation for the Stealthwatch Web App

To view documentation for the Stealthwatch Web App, you must view the online help in the Stealthwatch Web App interface.

To access the Stealthwatch Web App online help, from any page in the Stealthwatch Web App, click the User icon ( ) in the toolbar in the upper right corner of any page and choose **Stealthwatch Online Help**.

About the Stealthwatch Desktop Client

The Stealthwatch Desktop Client is an enterprise-level security management system that allows network administrators to define, configure, and monitor multiple distributed Stealthwatch Flow Collectors from a single location. This system provides flow-based security, network, and application performance monitoring across physical and virtual environments. With Stealthwatch, network operations and security teams can see who is using the network, what applications and services are in use, and how well they are performing.

Using tables, pie charts, graphs, and reports, administrators can rapidly detect and prioritize security threats, pinpoint network misuse and suboptimal performance, and manage event response across the enterprise –all from a single control center. Stealthwatch quickly zooms in on any unusual behavior and immediately sends an alarm to the SMC with the contextual information necessary for security personnel to take quick, decisive action to mitigate any potential damage.

Note:

Use the Stealthwatch Web App to monitor and configure your Stealthwatch installation if you deploy a Data Store. The Stealthwatch Desktop Client is incompatible with a Data Store. If your system contains Data Store domains, these will not appear in the Desktop Client.

Stealthwatch Interfaces

As of v6.5.0, Stealthwatch will use two user interfaces (i.e., management consoles) for a period of time to display data from sensors and to provide management functions, such as defining policies. The existing interface will continue to be available, but will gradually be phased out. Its functionality is being moved to the new Stealthwatch Web App interface. During the transition, you will need to use both UIs. The online Help for each UI will alert you to the need to switch from one to the other, when necessary.

Stealthwatch Desktop Client: This interface provides information in graphs, tables, and filters. The filters consist of separate, sometimes multiple, pages or dialogs.

Stealthwatch Web App: The new format uses a more visual approach, including elements you find on commercial websites, such as filter panes that you use to narrow the focus of your queries. This interface opens when you launch Stealthwatch.

How to Use This Guide

In addition to this introduction, we have divided this guide into the following chapters, as well as an index:

This Chapter...	Describes How to...
2 - Navigating the Stealthwatch Desktop Client	Use the common navigational elements within the SMC.
3 - Host Management	Group hosts so you can control their behavior through the use of policies.
4 - Views and Dashboards	View the various tabular and graphical displays of data that represent the most important activity within the SMC.
5 - Indexes: Ranking Behavior Changes	Use indexes to track anomalous behavior.
6 - Monitoring Traffic and Network Performance	Monitor traffic, as well as server and network response times.
7 - Analyzing Flows	Analyze flows to and from hosts in order to determine trends.
8 - Stealthwatch Threat Intelligence Feed (formally Stealthwatch Labs Intelligence Center, or SLIC)	A service from Cisco that delivers frequently updated information from the global threat intelligence feed about threats to your network.
9 - Finding the Culprit	Acknowledge and close alarms, use the automatic mitigation feature, and manually block a source.
10 - Responding to Alarms	Tune policies to reduce the number of unnecessary alarms you see.
11 - Reducing Unnecessary Alarms	Locate the first host that caused an alarm and the hosts it has affected.
12 - Working with Documents	Save, share, and schedule custom documents that contain components you specify.
13 - Desktop Client Roles	Create desktop client roles to control which functionality (e.g., flow search, policy management, reports, etc.) users can view and configure in the Stealthwatch Desktop Client.

DOCUMENTATION ICONS

This document uses the following icons to denote significant information:

Icon	Meaning	Includes Information...
	Tip	Such as a shortcut or an easier way of performing a certain task.
	Note	You may find useful as you use this document or Stealthwatch.
	Important	You must observe to prevent significant consequences, such as the malfunction of software.
	Caution	You must observe to prevent loss of data or damage to hardware.

ABBREVIATIONS

The following abbreviations appear in this guide:

Abbreviation	Definition
AS (Number)	Autonomous System
CI	Concern Index
CIDR	Classless Inter-Domain Routing
CSV	Comma-Separated-Value
DAR	Disk Archive
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System (Service or Server)
DoS	Denial of Service
DSCP	Differentiated Services Code Point
FSI	File Sharing Index
IANA	Internet Assigned Numbers Authority
ID	Identifier
IM	Instant Messaging
IP	Internet Protocol
MAC	Media Access Control
MPLS	Multiprotocol Label Switching
PDF	Portable Document Format
P2P	Peer-to-Peer
RADIUS	Remote Authentication Dial-in User Service
RFC	Request for Comment
RTT	Round Trip Time
SMC	Stealthwatch Management Console
SNMP	Simple Network Management Protocol
SRT	Server Response Time
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TI	Target Index
UDP	User Datagram Protocol

Abbreviation	Definition
UI	User Interface
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

CONTACTING SUPPORT

If you need technical support, do one of the following:

Call

- Your local Cisco Partner
- Cisco Stealthwatch Support
  - (U.S.) 1-800-553-2447
  - Worldwide support number: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Open a case

- By web: http://www.cisco.com/c/en/us/support/index.html
- By email: tac@cisco.com

2

Navigating the Stealthwatch Desktop Client

Overview

The Stealthwatch Desktop Client contains a large collection of documents to assist you in monitoring, protecting, and analyzing your network. Familiarizing yourself with the common navigational elements of these documents and the interface in general will help you become more proficient with Stealthwatch and more efficient when analyzing events in your network.

This chapter includes the following topics:

- Client Memory Allocation
- Your Point of View
- Enterprise Tree and Tool Tips
- Opening SMC Documents
- Working with Documents
- Working with Tables
- Working with Charts
- Filtering Document Data
- Printing Documents
- Saving Documents
- Online Help

- Keyboard Shortcuts

CLIENT MEMORY ALLOCATION

You can change how much Random Access Memory (RAM) to allocate on your client computer to run the Stealthwatch Desktop Client. Consider a larger memory allocation if you work with many open documents or large data sets (such as flow queries with over 100k records).

1. **Using Windows:**

   a. In Windows Explorer, go to your home directory.

   b. Open the Stealthwatch folder using this path: AppData > Roaming > Stealthwatch.

   Using macOS

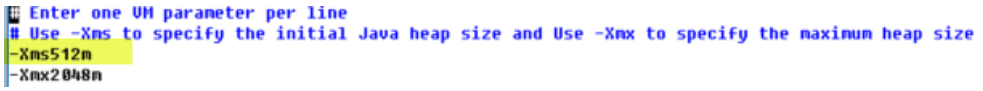
   a. In Finder, go to your home directory.

   b. Open the Stealtwatch folder.

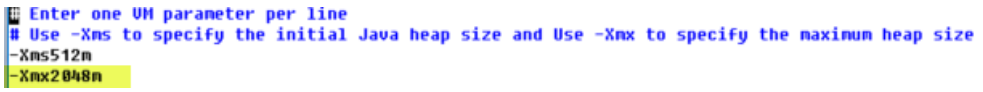
2. In the Stealthwatch directory, open the folder that contains the desired Stealthwatch version.

3. Open the application.vmoptions file using an appropriate editing application to begin editing. (This file is created after you open the Stealthwatch Desktop Client for the first time.)

   - For the minimum memory size, we recommend that you allocate no less than 512 MB. This number is listed in the third line of the file. For editors that display the content in one continuous line, refer to the number highlighted in the image below to see which number represents the minimum memory size.



   - You can allocate up to half the size of your computer's RAM for the maximum memory size. This number is listed in the fourth line of the file. For editors that display the content in one continuous line, refer to the number highlighted in the image below to see which number represents the maximum memory size.



Use whole numbers. For example, enter Xmx512m, not Xmx0.5m.

YOUR POINT OF VIEW

After you log in to the Stealthwatch Desktop Client, the view you see will depend on your login privileges (i.e., your point of view). For this reason, what you see on the Stealthwatch Desktop Client in your office may differ somewhat from what you see in this guide.

Your Stealthwatch administrator defines your login privileges on the User & Role Management dialog. For more information, see Chapter 13, "Desktop Client Roles."

You can create your own custom dashboard and make it a login document, or you can choose a dashboard that has already been set up within the SMC. You can create as many custom dashboards as you want. A dashboard is a collection of different reports that contain any SMC component you want with the data you want to see. This allows you to focus on the primary information you are interested in viewing.

Notes:

- For information about setting up login documents, refer to Chapter 12, "Working with Documents."
- For information about building dashboards, refer to Chapter 4, "Views and Dashboards."

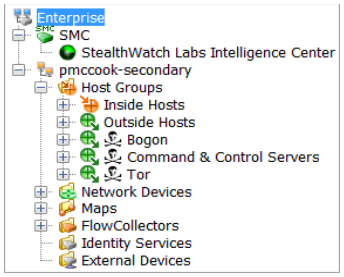
The Domain Dashboard is an example of a document that you may decide to have as a login document since it provides graphical and tabular data about important activity in the domain. This data is collected from the SMC every five minutes. By default, the Domain Dashboard is automatically configured to be a login document for the admin user. It is also available immediately as a scheduled document for new users; all you have to do is enable the StealthwatchStealthwatch Daily Reports schedule and include this document.

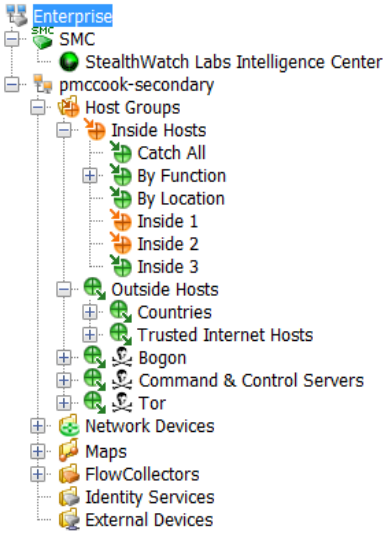
Note:

For information about enabling and scheduling documents, refer to Chapter 12, "Working with Documents."

ENTERPRISE TREE AND TOOL TIPS

The list of items in the left navigation pane of the Stealthwatch Desktop Client is often called the Enterprise tree. You may also hear it called the Enterprise page or the Host Group tree. This tree essentially shows you the structure of your monitored network.





By default, the options in the Enterprise tree are collapsed. To expand all options in the tree simultaneously, right-click any item in the tree and select **Expand All**. To collapse all items simultaneously, right-click any item and select **Collapse All**. To hide the Enterprise tree completely, go to the Main Menu and click **View > Hide Tree**, or press **Ctrl+T** on your keyboard. The SMC saves the expanded and collapsed folder settings. So the next time you log in, the Enterprise tree appears just the way you left it.

Searching Through the Tree

To search for an item in the Enterprise tree, type the desired text in the Find field

at the bottom of the Enterprise tree.

Note:

The Find field is hidden by default. You must click **CTRL+F** to open it the first time, and then thereafter it will display each time you open the SMC.

You can search forward and backward through the tree for additional instances of the desired text by using any of the following methods:

- Click the down and up buttons to the right of the Find field.
- Press the down ( ) and up ( ) arrow keys on your keyboard.

Tip:

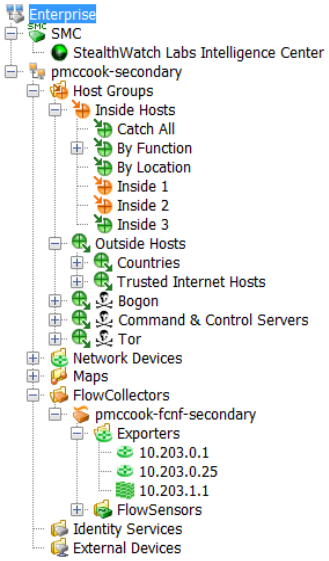
You can continue to perform other operations in the SMC while a search is being processed.

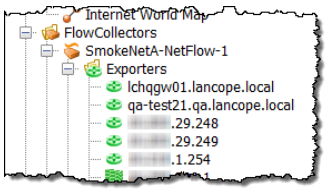
Tree Branches

The Enterprise tree branch, highlighted in this example, is always present in the Enterprise tree. This branch represents the top collection point for all SMC management options, encompassing all of the domains monitored by the SMC.

Depending on your point of view, the SMC branch may or may not be present. This branch represents the SMC appliance itself. If your system is using a failover SMC, you will see both the primary and the secondary SMC branches.

The other tree branches represent the domains that the SMC appliance is monitoring, along with the associated host groups, Stealthwatch Flow Collectors, Stealthwatch FlowSensors, maps, peripheral devices, and external devices.





To expand a branch, click the associated plus sign . One of the branches you will see is the Flow Collectors branch. To see the list of Flow Collectors that are sending information to the SMC appliance on the selected domain, expand the Flow Collectors branch by clicking the associated plus sign. If you expand the branch for a particular Flow Collector, you can see its associated FlowSensor appliances, exporters, and firewalls.

Alarm Severity Levels

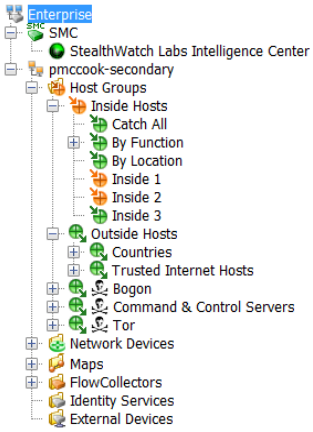
The Enterprise tree branch enables you to immediately see if you have an alarm condition somewhere in your network, because an icon will change its color depending on the degree of alarm severity level that is indicated. The SMC comes with default severity levels already assigned to each alarm. However, depending on your login privileges, you can use the Alarm Configuration dialog to change these severity level assignments to suit the needs of your network environment. The following table lists the different types of severity levels, each indicated by a specific color:

Severity Level	Associated Color
Critical	Red
Major	Orange
Minor	Yellow
Trivial	Blue
Informational	Light Blue
No Alarm Exists	Green

Note:

The top-level branch icon displays the color for the highest-severity alarm occurring for any lower-level branch.

As you look at the menu, ask yourself the following questions:

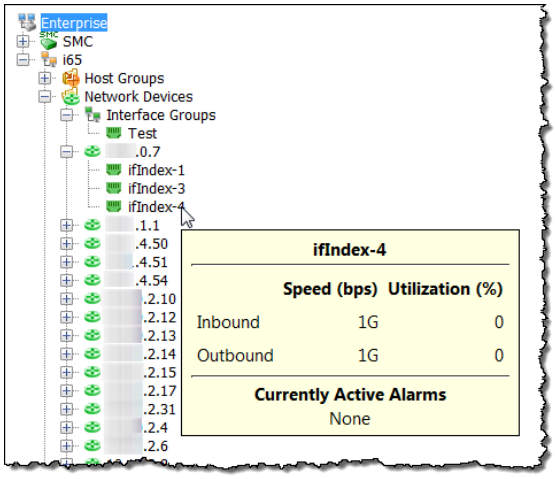


- Are any of the icons red or orange? If so, you know that critical or major alarm conditions exist.
- Do you see this icon? If so, the connection to the device this icon is beside has been lost.
  - You may want to expand the Inside Hosts subtree to find out whether alarms exist in your most important or sensitive host groups.
  - From the Host Groups subtree, you may want to open one of the Host Group Dashboard documents (discussed later in this chapter) for more information.
- What color is the SMC icon? Any color except green or gray indicates that system alarms exist for the SMC appliance.

Note:

The system updates the Enterprise tree once every minute. However, you can refresh it at any time to see the most up-to-date information by going to the Main Menu and clicking **View > Refresh Tree**. You can also right-click anywhere in the Enterprise tree and select **Refresh Tree**.

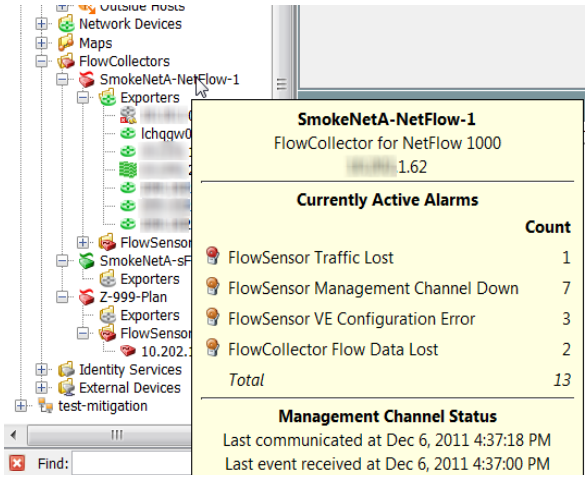
Enterprise Tree Indicators



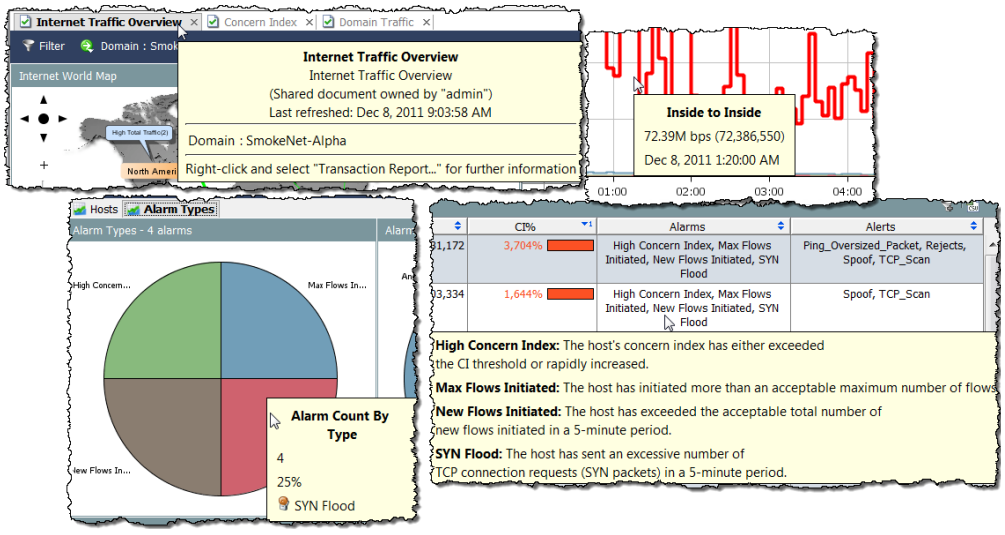
If you hover the cursor over a branch, a tool tip appears, showing you the total number of alarms that object is experiencing, including the severity levels of each. In the case of the Flow Collectors branch, you will see alarm information and the identity of the Stealthwatch appliance. In addition, you will see when the SMC last tried to communicate with the appliance, when the SMC received a response, and when the appliance last reported an event.

Tool Tips

You can hover the cursor over various elements in the Stealthwatch Desktop Client to display summary information about the element in a tool tip. For example, if you hover the cursor over a Flow Collector name in the Enterprise tree, you will see identifying information, along with communications status and any alarms that the Flow Collector has triggered.



Tool tips are virtually everywhere in the Stealthwatch Desktop Client. Simply hover the cursor over an element (e.g., a tab, graph, chart, or table cell) to see its corresponding tool tip.



OPENING SMC DOCUMENTS

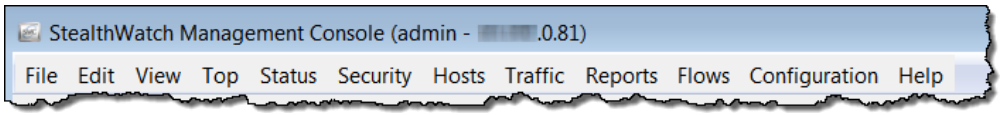
The Stealthwatch Desktop Client allows you to open documents in several ways, such as through the Main Menu and right-click functionality.

Note:

Documents are also referred to as reports. There are instances within this user guide where these terms are used interchangeably.

Main Menu

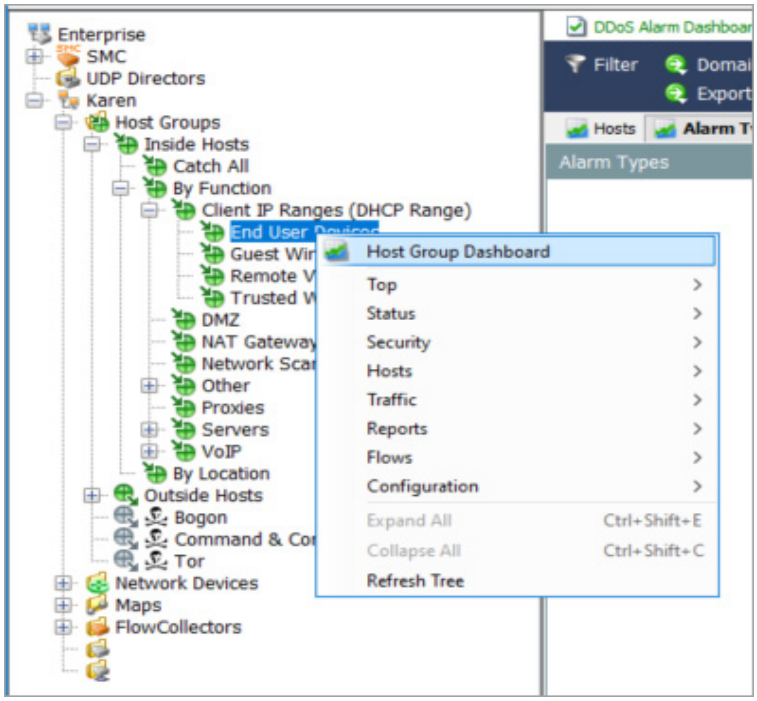
You can click menu items from the Main Menu to open documents.



The options available will depend on the following three primary factors:

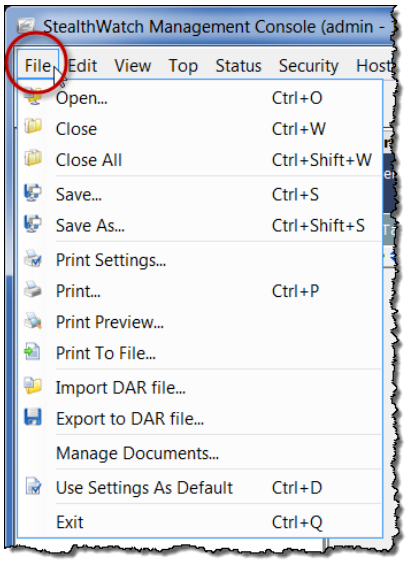
- What you have clicked in the Enterprise tree
- What you have clicked in a particular SMC document
- Your login privileges

For example, if you click a host group in the Enterprise tree, and then right-click **Host Group Dashboard**, you will see data only for that host group.



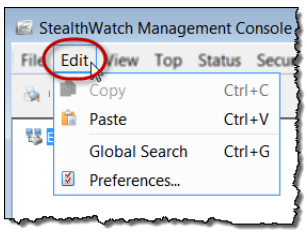
File Menu

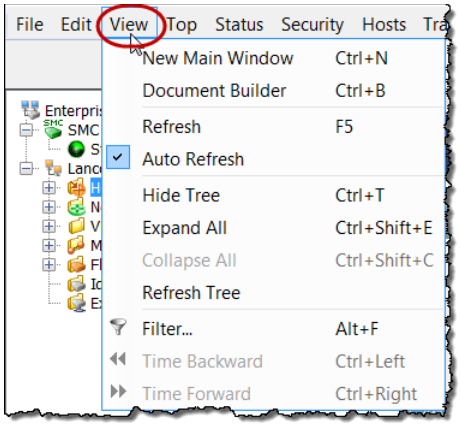
The File menu provides options for working with SMC documents, such as opening, closing, saving, printing, and sharing documents with other users.



Edit Menu

The Edit menu provides options for copying, pasting, and searching for data, as well as for defining certain display preferences.





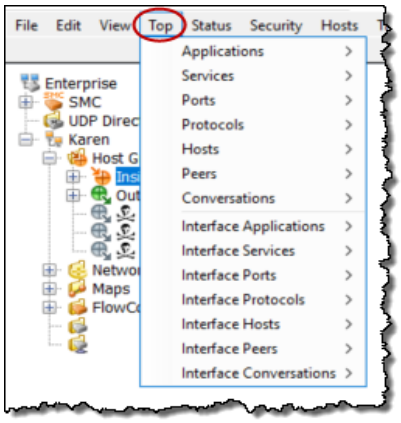
View Menu

With the View menu, you can open a new instance of the SMC user interface, build custom dashboards, stop or start the automatic refresh feature, manually refresh data, show the Enterprise Tree in various ways or hide it altogether, Filter data, or display data for earlier or later time frames.

T

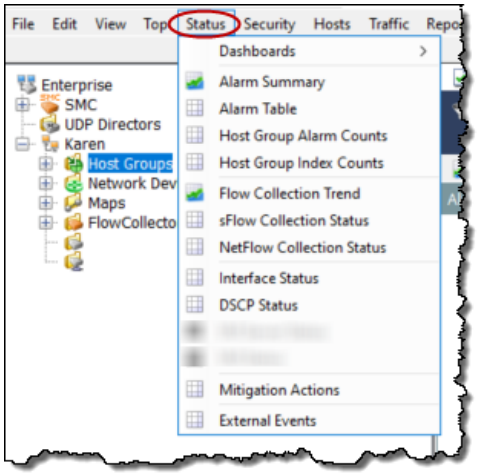
Top Menu

The Top menu allows you to display the most prevalent data based on specific criteria, such as applications used most often, services used most often, ports used most often, most active hosts, etc. You can view this data across the entire network or break it down according to inbound traffic, outbound traffic, traffic within a domain or host group, or traffic crossing a specific interface.



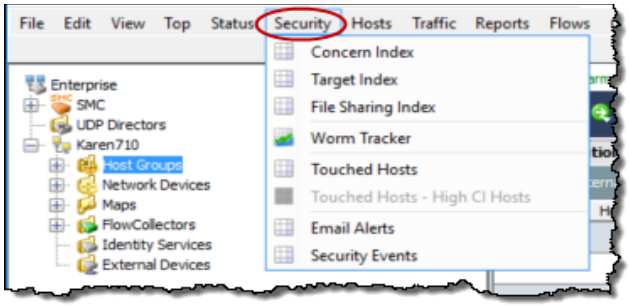
Status Menu

The Status menu provides options for displaying the status of various parts of the network based on specific criteria such as alarms, traffic, possible data loss, interfaces, external events, etc.



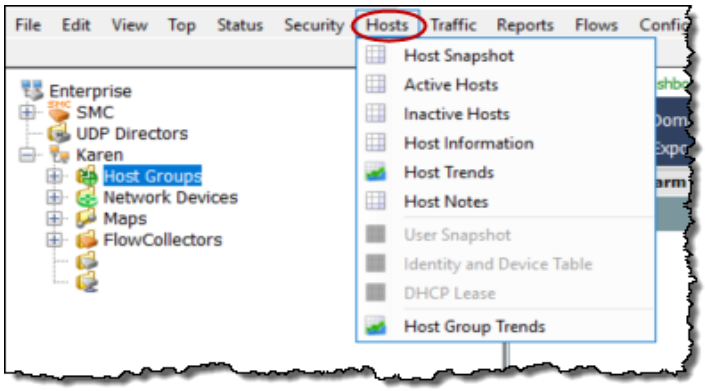
Security Menu

Use the Security menu to see data related to security concerns, such as high concern hosts, targeted hosts, file sharing activity, worm activity, and unusual Email traffic.



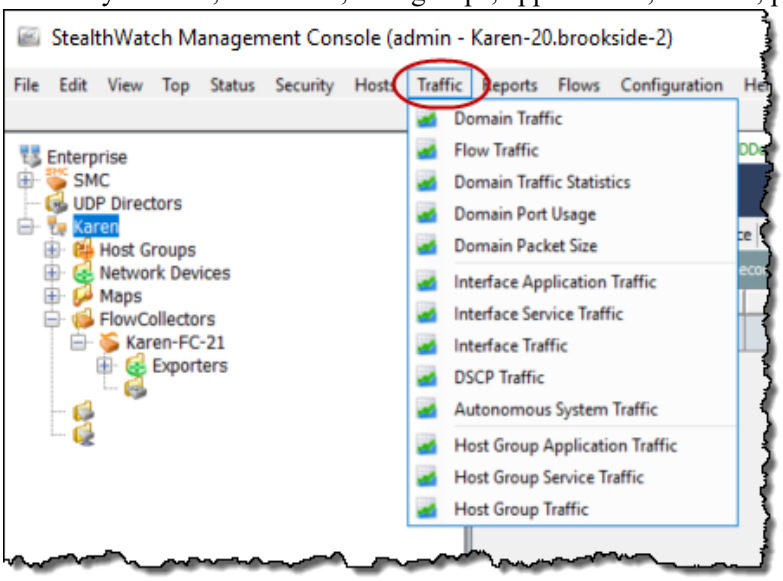
Hosts Menu

The Hosts menu provides options for displaying data related to hosts, such as individual host activity, trends in host behavior, active or inactive hosts, host user identity, etc.



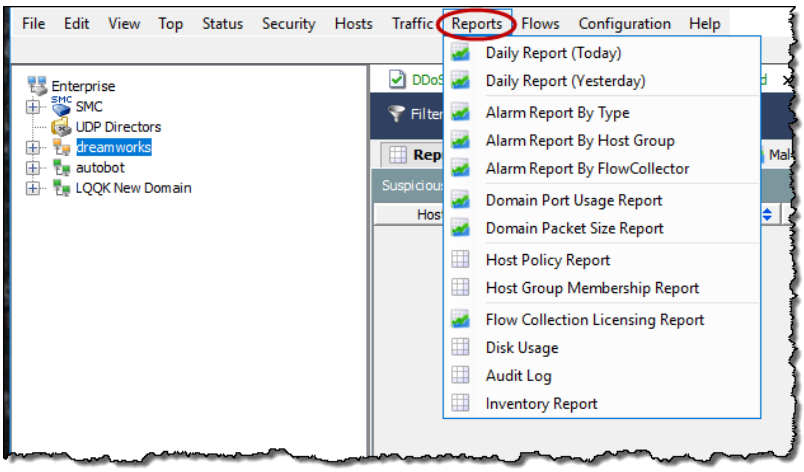
Traffic Menu

The Traffic menu allows you to see traffic information broken down in a wide variety of ways, such as by domain, interfaces, host groups, applications, services, ports, etc.



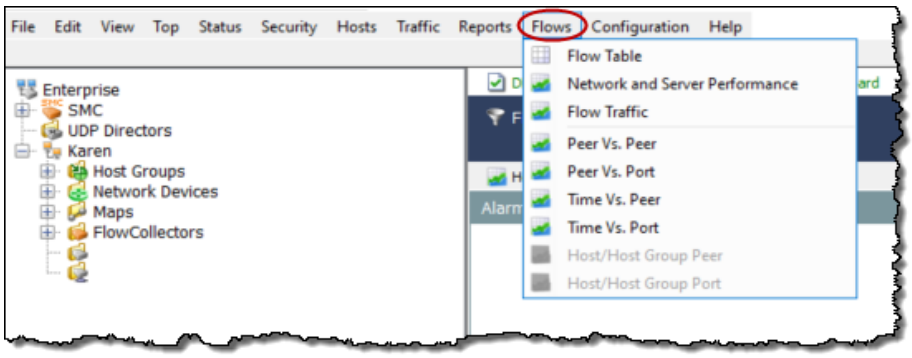
Reports Menu

The Reports menu permits you to run queries against the Stealthwatch database, such as for a daily summary of domain activity or a report of alarms that have occurred according to type, host group, or Flow Collector.



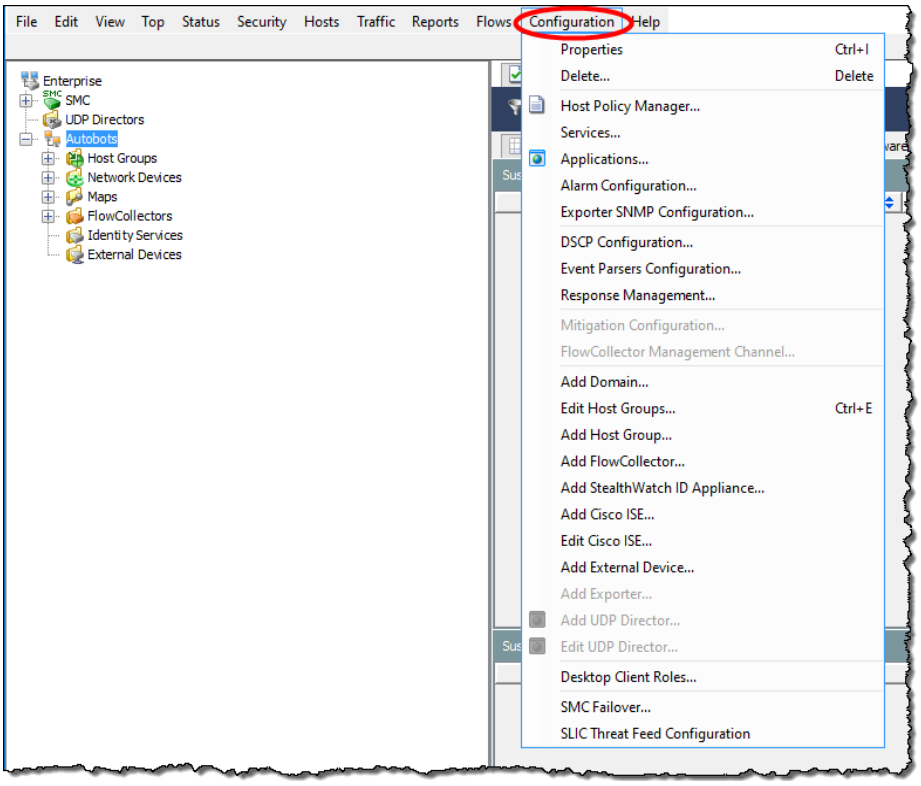
Flows Menu

Just as the name indicates, the Flows menu provides various ways for you to analyze flows, including network and server performance flow data.



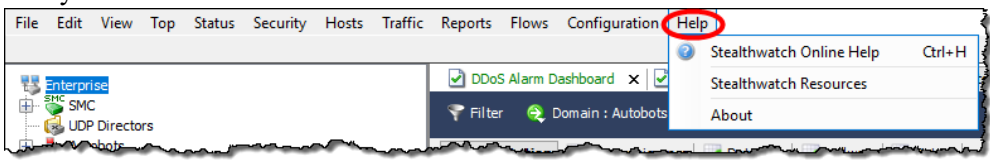
Configuration Menu

The Configuration menu contains the majority of the configuration options available in Stealthwatch. You can structure or refine your monitored network as desired by adding, editing, or deleting domains, appliances, host groups, policies, application, or service definitions. You can also restrict access by adding, editing, or deleting users and their login privileges. Stealthwatch uses a default set of alarm severity levels. If desired, you can change these according to your organizational needs.



Help Menu

The Help menu contains the *Stealthwatch Desktop Client Online Help* and information related to the version and description of the Stealthwatch Desktop Client software. We will discuss the advantages of using the online Help in more detail shortly.

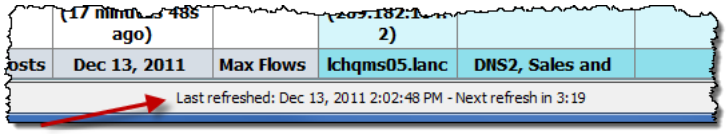


WORKING WITH DOCUMENTS

Let's take a look at some common navigational elements that appear on SMC documents.

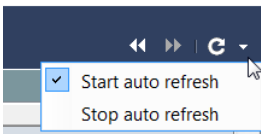
Displaying Live Data vs. Static Data

The SMC appliance collects data from the Stealthwatch Flow Collectors and automatically refreshes the data on most SMC documents, so you will always view relatively current information. You can see when the next automatic refresh is going to occur by looking at the counter at the bottom of the window.



The Refresh button is located at the far right side of the document header. When you click this button, the active document is refreshed (and becomes live) with the latest data, and the automatic refresh feature is reset.

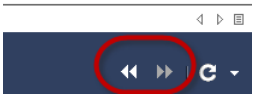
If you need to study the information for a longer period of time, you will want to make the document static.



You can make the document static or live by clicking one of the following options from the drop-down menu:

- Start auto refresh - The document is now live (active). When the auto-refresh interval expires, the SMC software updates the document with new data.
- Stop auto refresh - The document is now static (inactive).

Tip:
Click the **Refresh** button at any time to trigger a data update.



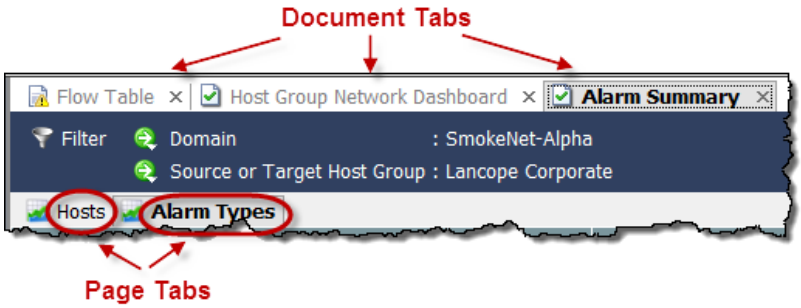
The View Earlier Data button and the View Later Data button are also located at the far right side of the document header. When you click these buttons, you can move through data backward or forward, respectively, according to the time increment set in the Filter dialog.

Tips:

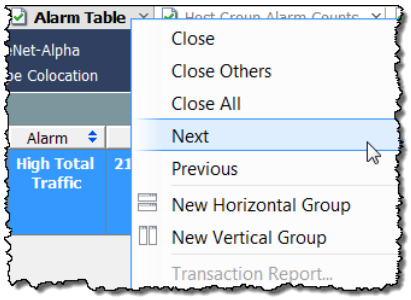
- Press **Ctrl+Left Arrow** to quickly move backward in time through the data.
- Press **Ctrl+Right Arrow** to quickly move forward in time through the data.

Tabs and Moving from One Document to Another

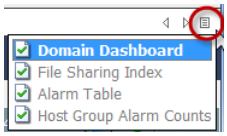
You can have multiple documents open simultaneously in the Stealthwatch Desktop Client. Each document is separated from the others by a tab. Some documents, like the Alarm Summary shown in the following example, have multiple pages, which also are separated by tabs.



You can move from one document to the next in several ways. You can click the desired document tab, right-click the document tab and select **Next** or **Previous**, or simultaneously press the **Alt** key and either the left ← or right → arrow key on your keyboard.

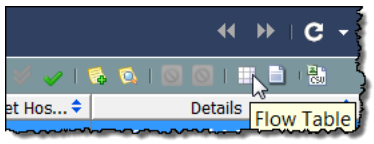


If you have too many documents open to be able to see all of the tabs, you can move from one document to another by clicking the right ▶ or left ◀ arrows to the right of the tabs. You can also click the List button ☰ to click an open document from the dropdown list.



The active document is the document you are currently viewing. The title for the active document is always black and bold. Active documents refresh automatically based on the corresponding refresh interval. Inactive documents do not refresh automatically. You must make an inactive document active, and then refresh it manually. Once a refresh begins, you can navigate to other documents without waiting for the refresh to finish.

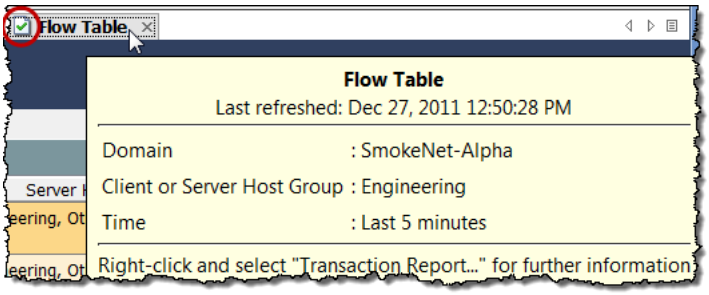
Many documents contain their own tool bar with buttons that have specific functions for that document. You can hover the cursor over any button to see a tool tip that describes the button.



Each document tab contains an icon that indicates the refresh status of the document (refer to the circled area in the following example). When an inactive document completes a refresh, the tab text changes color to indicate the refresh status. The following icons indicate the different refresh statuses available:

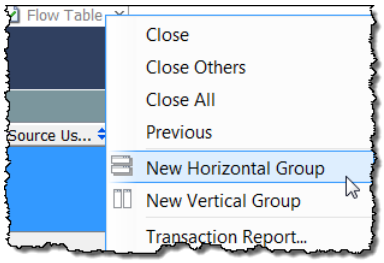
- Busy – The document is in the process of refreshing or performing some other action.
- Refreshing complete – The last refresh completed successfully; inactive tab text is green.
- Refreshing complete (with errors) – The last refresh completed successfully, but errors occurred or more information is available; inactive tab text is yellow.
- Error – The last refresh failed to complete; inactive tab text is red.

If you hover the cursor over a document tab, you will see a tool tip providing you with summary information about that document.



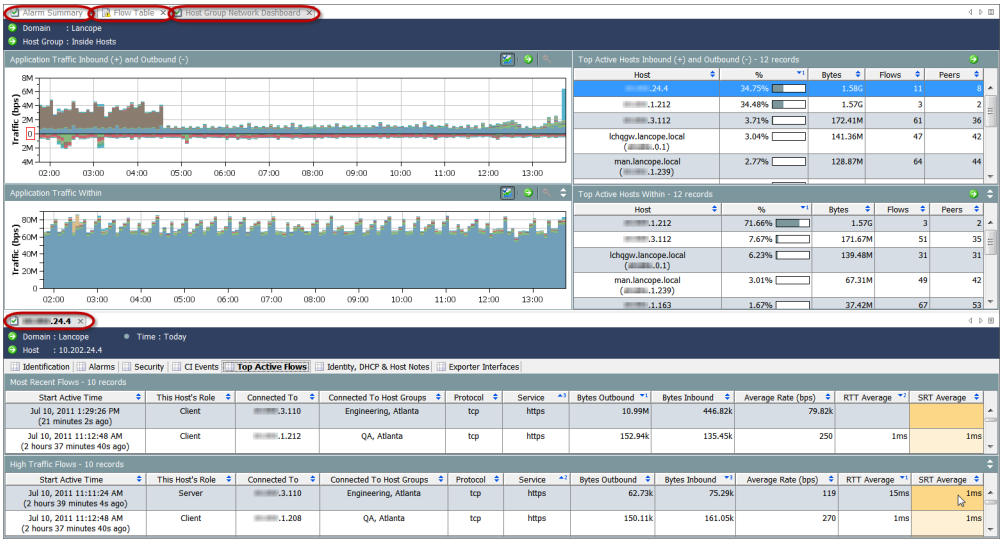
Changing Document Orientation

By default, when you open multiple documents, they display one behind the other, offset by tabs. If desired, you can change this orientation so they display either under each other, horizontally, or next to each other, vertically. Choose the orientation you want by right-clicking the document tab and clicking either **New Horizontal Group** or **New Vertical Group**.

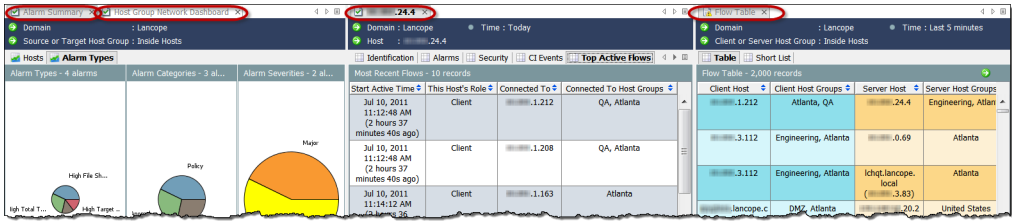


The result will look similar to one of the following examples.

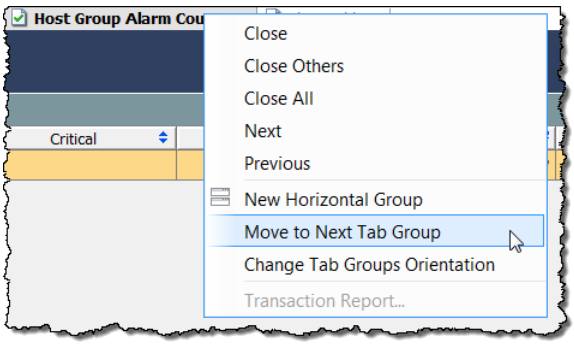
Horizontal Group



Vertical Group



Depending on the current orientation, you can move documents from one tab group to another by right-clicking the document tab and selecting **Move to Next Tab Group**, **Move to Previous Tab Group**, or **Change Tab Groups Orientation** until you achieve the desired arrangement. You can also click and drag a document tab from one position to another among the open documents.



Document Header

The document header contains information about the data that the document is presenting.

A Flow Table header is shown in the previous example. The header lists the domain where the involved hosts are located, as well as the host group name. In addition, we see when the data being presented was captured.

So, the data we are viewing in this example is for flows occurring in the Inside Hosts host group of the SmokeNet-Alpha domain. The data we are seeing in the document was captured during the last 12 hours. You can change any of these parameters by using the filter, which we will discuss momentarily.

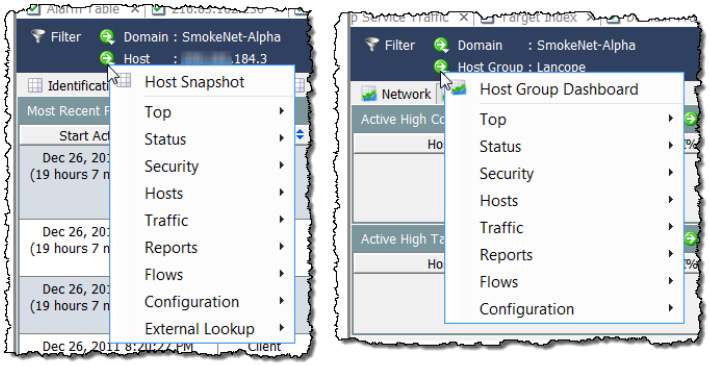
Go to Document Buttons

The Go to Document button displays in document headers and tool bars throughout the Stealthwatch Desktop Client. What you see when you click this button depends on the object associated with the button.

In Document Headers

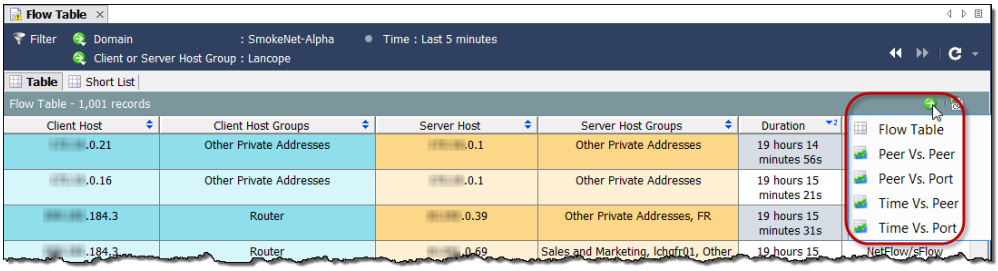
For example, if you click the **Go to Document** button next to the host IP address in a document header, you will see a list of document options that pertain to hosts. If you click one of those options, the data displayed will pertain only to that specific host.

Likewise, if you click the **Go to Document** button next to the host group name in the header, you will see a list of document options that pertain to host groups. If you click one of those options, the data displayed will pertain only to that specific host group.

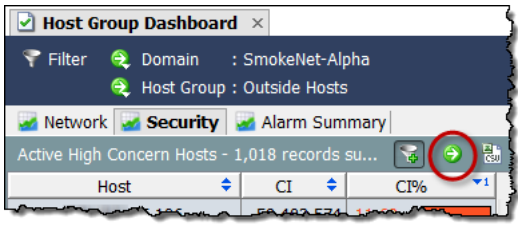


In Document Tool Bars

The Go to Document buttons that appear in document tool bars allow you to see the data you are viewing in different ways. For example, suppose you are looking at a Flow Table for a particular host group. If you click the **Go to Document** button that appears in the Flow Table tool bar, you will see a list of document options that pertain to flows. If you click one of these options, you will see this flow information displayed in a different format.

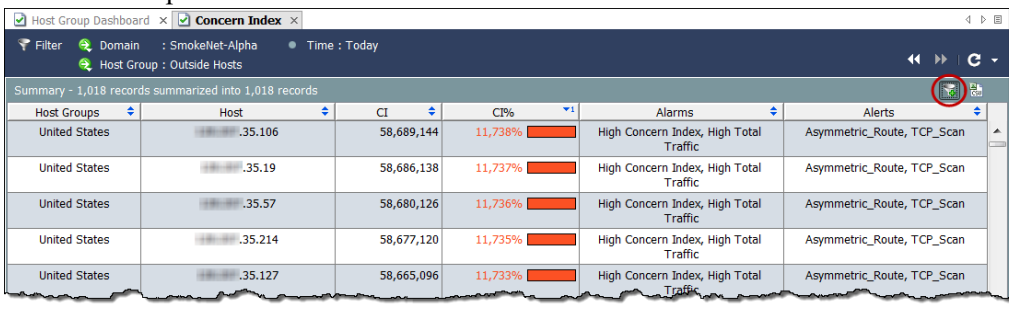


In some instances, there is only one document that would pertain to the data you are viewing. In that case, when you click the **Go to Document** button, that document will open immediately.



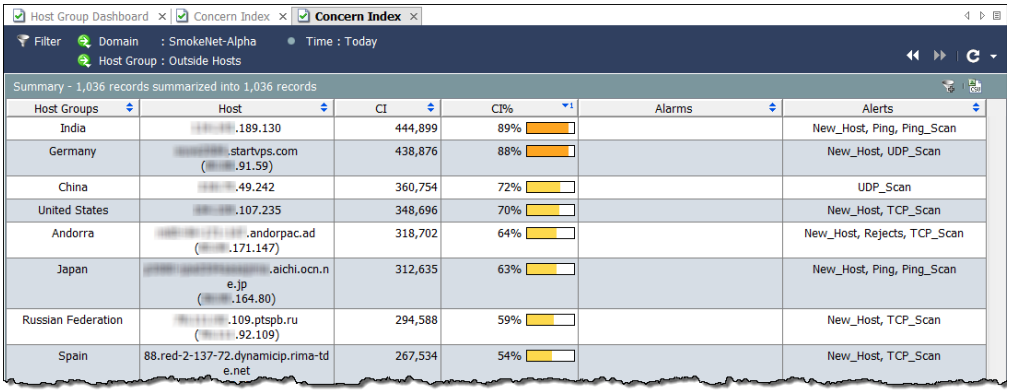
For example, each component on the Host Group Dashboard contains its own tool bar with a Go to Document button. If you click the button for the Active High Concern Hosts component, the SMC will immediately open the Concern Index document pre-filtered to shows data that pertains only to the information being shown in that component on the Host Group Dashboard.

The Concern Index document displays information for hosts that have had the highest number of CI points since the last archive hour.



When you open the Concern Index document, by default the Concern Index filter button (located in the upper right corner of the document), is activated, and the Concern Index shows only those hosts that have active High Concern Index alarms (i.e., that have a CI percent above 100). To see only hosts that have a CI percent greater than 50, click the **Concern Index filter** button.

The plus sign on the Concern Index filter button turns gray , and only hosts that have a CI percent greater than 50 appear.

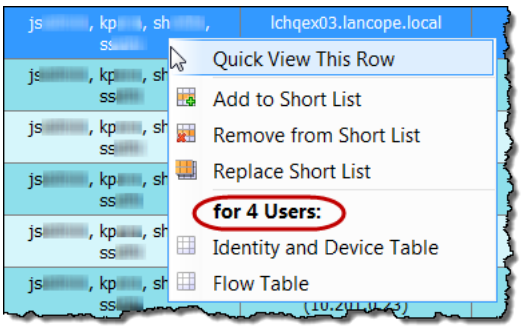


Right-Clicking for Quick Focus

The right-click functionality offered throughout the Stealthwatch Desktop Client provides an alternative means for opening documents. Often, the right-click menus help you find the most specific data more quickly than does the Main Menu.

Right-click an element in the Enterprise tree and select the desired document from the pop-up menu. The data displayed at that point will relate specifically to the element you clicked. For example, if you right-click a host group name in the Enterprise tree and select **Flows > Flow Traffic**, the flow traffic data displayed will relate specifically to that host group.

Another way to open documents is to right-click within a document and make the desired selection from the pop-up menu that appears. For example, when you right-click a user name (or multiple user names) within a column in a document, the following pop-up menu appears:



The label in the pop-up menu (circled in the previous image) indicates the number of users on which the documents listed below the label are available to be filtered. If only one name was clicked, then the label indicates the name of that user.

Note:

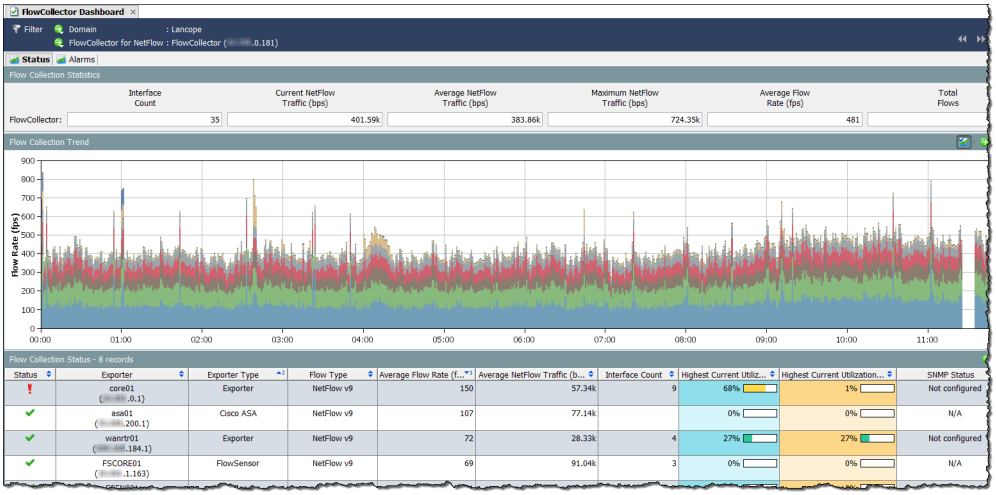
- You can also open documents by double-clicking items in table cells, and by using **Go to Document** buttons.

Double-Clicking for Selected Documents

The double-click functionality provides an alternative means for opening a select number of documents. Refer to the following table for documents that can be opened by double-clicking on a branch in the Enterprise Tree:

If you double-click this branch in the Enterprise tree...	Then this document opens.
the SMC folder	SMC Dashboard
a specific host group	Host Group Dashboard
the Inside/Outside Hosts folder	Host Group Dashboard
the Network Devices folder or a specific network device	Interface Status
the Exporters folder or a specific exporter	Interface Status
a specific interface	Interface Summary Dashboard
the Flow Sensors folder	Interface Status
A specific map	That specific map
a specific Cisco ASA exporter	The flow table for the last five minutes, filtered by that ASA
any firewall that is not a Cisco ASA firewall (e.g., Palo Alto firewall)	Interface Status
a firewall interface	Interface Summary Dashboard
a specific Flow Collector	Flow Collector Dashboard
a specific Cisco ISE	Identity and Device Table
a specific IDentity	The User Identity filter dialog
a specific external device	External Events

For example, if you double-click a Flow Collector, the Flow Collector Dashboard for that Flow Collector opens.



Searching Documents

In addition to searching for items in the Enterprise tree, the SMC allows you to search through all of its documents (across all domains) for certain items. In the Search field in the Main Tool Bar, you can search for the following items using a full string, partial string, or partial string with wild card (*):

- Alarm ID
- Host or exporter IP address
- The following names:
  - Exporter
  - Host group
  - Server
  - User

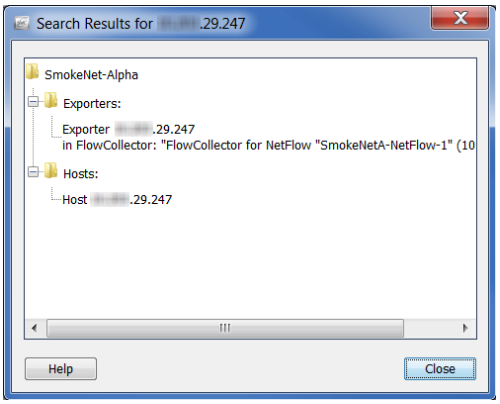
Note:

- The search results are limited according to the data role and functional role associated with your user name.

Tip:

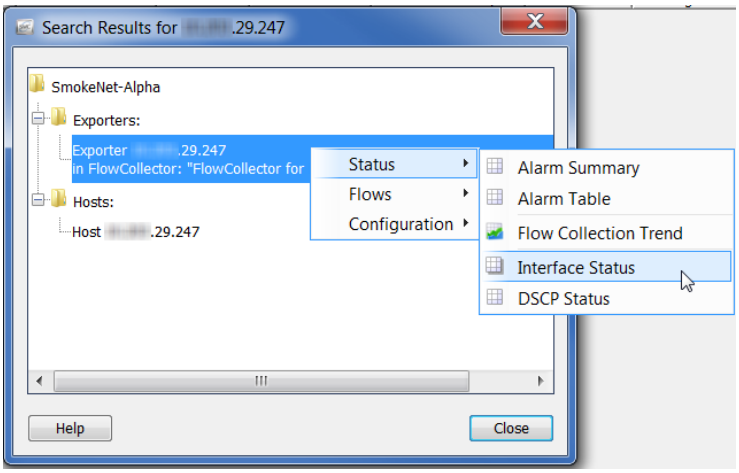
You can use the Search drop-down list box to select an item that you have previously searched for and then press **Enter** to execute the search.

For example, if you type the IP address of an exporter into the Search field and then press **Enter** on your keyboard, the Search Results dialog displays a list of the locations where that IP address appears in the SMC.

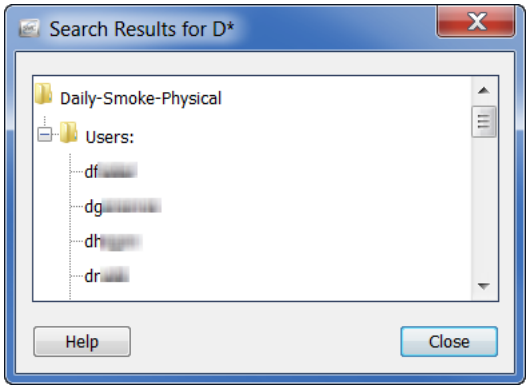


In many cases, you can double-click an IP address in the list to display a specific document about that item. For example, if you double-click the IP address under the Host entry, you will display the Host Snapshot for that IP address.

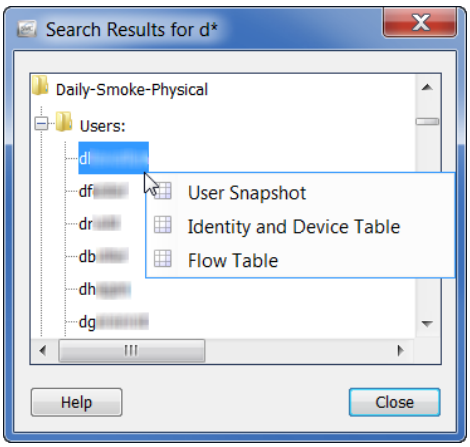
You can also right-click the IP address for a list of other informative documents that you can access related to that IP address.



When you perform a user name search, each user name will appear as a separate item within a folder entitled “Users” in the Search Results dialog.



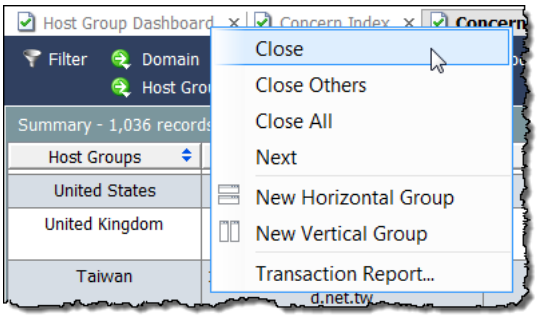
If you double-click a user name, the Identity and Device Table opens, pre-filtered on the user. If you right-click a user name, the following pop-up menu appears, from which you can select a document that will be pre-filtered for the corresponding user.



Closing Documents

Just as there are multiple ways to open an SMC document, there are several ways to close them. To close one document, simply click the **X** in the right corner of the document tab. Alternatively, from the Main Menu click **File > Close**, or press **Ctrl+W** on your keyboard.

To close all documents, from the Main Menu click **File > Close All**. You also can right-click the document tab and select the appropriate option from the pop-up menu.

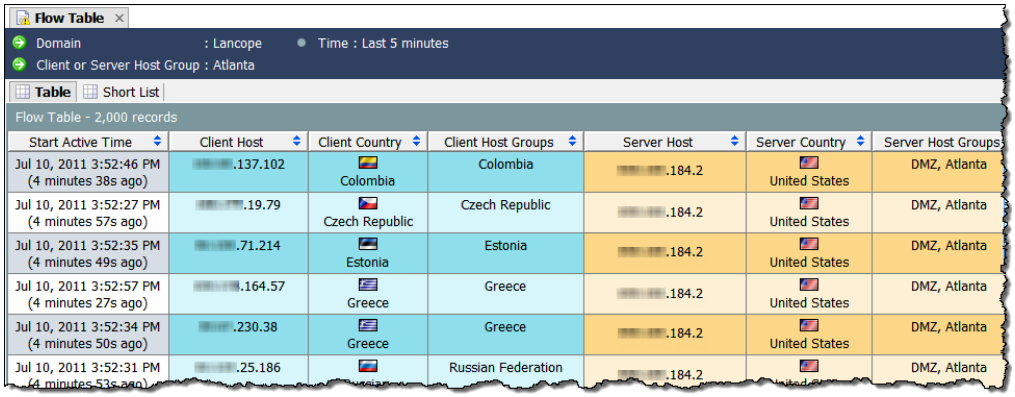


Note:

For a complete list of keyboard shortcuts that you can use with the SMC, refer to "Keyboard Shortcuts" on page 77.

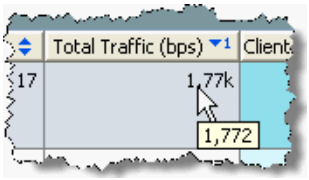
WORKING WITH TABLES

Documents that contain tables provide additional navigational elements. One key graphical cue is the use of colors in table rows, such as those shown in the following Flow Table.



- Blue indicates client-side data.
- Yellow-orange indicates server-side data.

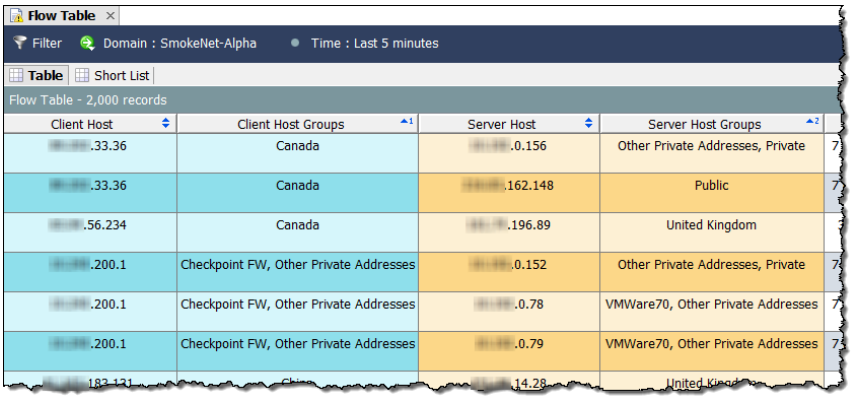
Units of measure are indicated in the column headings, such as *bps* for bits per second. Numerical values in the corresponding cells are rounded off. However, you can hover the cursor over the rounded value to reveal the exact value in a tool tip.



Sorting Columns

To sort a column in ascending or descending order, click the **Up/Down** button in the column heading. (This button toggles to indicate ascending or descending order.) You can sort a table by as many as three specific columns. When you sort a single column, the entire table sorts based on that column. If you sort a second column, the entire table will sort based on that column first, and will then sort based on the first column you sorted by, and so on.

In the following example, the first column sorted was the Server Host Groups column, in ascending alphanumeric order. When the Client Host Groups column was sorted next, in ascending alphanumeric order, this column became the first column sorted on, and the Server Host Groups column became the second column sorted on.

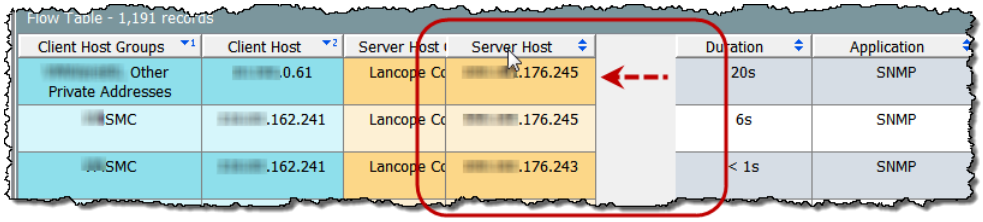


Note:

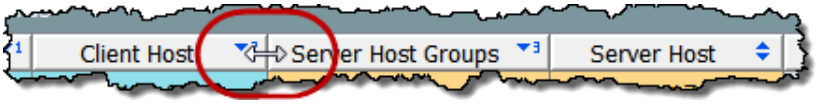
To remove the sorting behavior from a column, press the **Ctrl** key on your keyboard while you click the column header.

Moving and Resizing Columns

To move a column left or right, simply click the column heading and drag the column to the desired position.

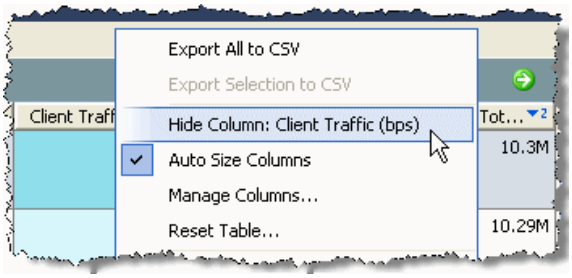


By default, column widths are adjusted automatically so that all columns display on your screen to the greatest extent possible. To widen or shrink the width of a column manually, click and drag the border of the column heading left or right to the desired width.

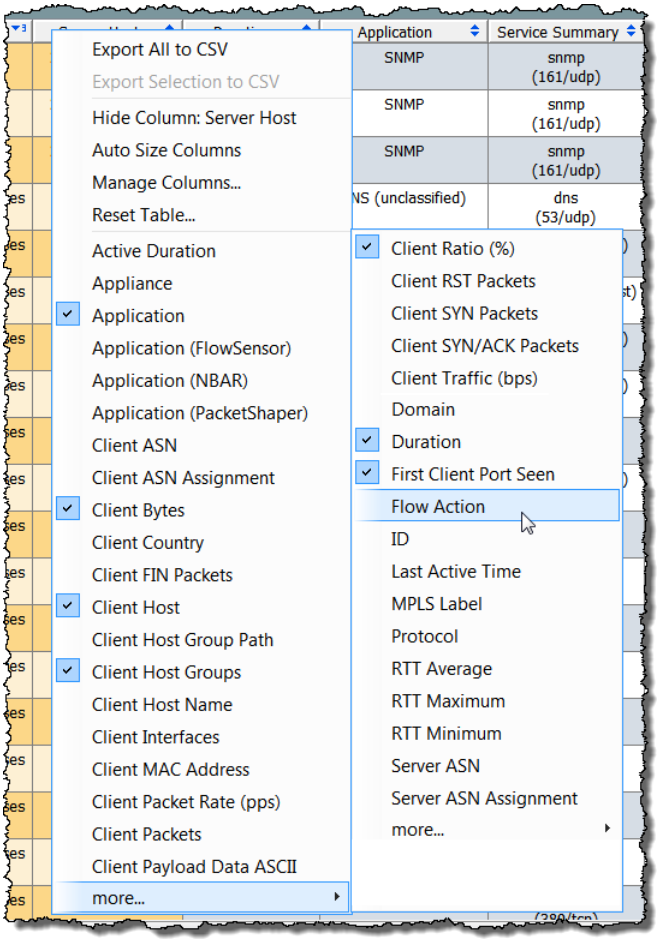


Hiding and Showing Columns

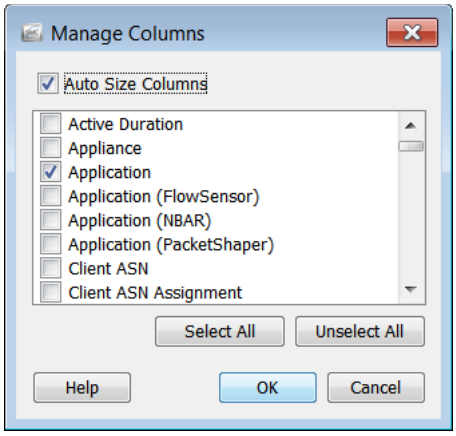
To hide a column, right-click the column heading and select **Hide Column: <Name>**.



To show more columns, right-click the column heading and select the columns you want to see from the pop-up menu.



Alternatively, you can go to the Manage Columns dialog to hide or show specific columns. Right-click a column heading and select **Manage Columns**. If you want a column to show on the corresponding document, click its check box to add a checkmark (if it does not already contain a checkmark). If you do not want a column to display on the corresponding document, click its check box to remove the checkmark (if a checkmark is still displayed).



To have the SMC resize columns automatically, ensure that the **Auto Size Columns** check box at the top of the dialog contains a checkmark. The SMC will automatically size columns so that they all appear on your screen, to the greatest extent possible, with no horizontal scroll bar. To resize all of the columns manually, ensure that the **Auto Size Columns** check box does not contain a checkmark.

When finished making changes, click **OK** to apply the changes and close the Manage Columns dialog.

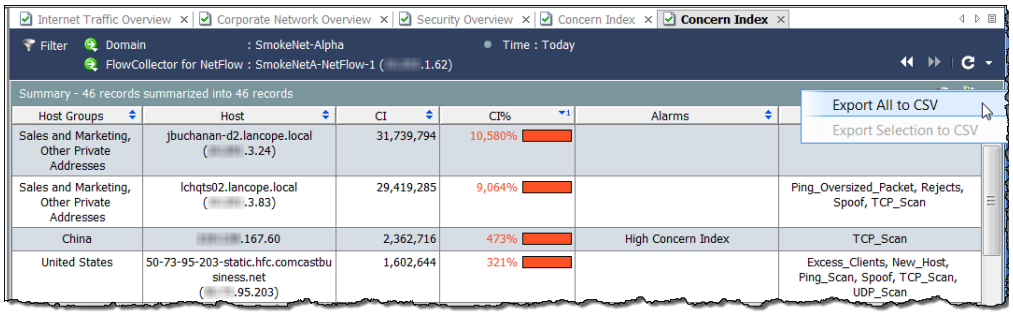
Tip:

To return the table to its default settings, right-click a column heading and select **Reset Table**.

Exporting Data

You can save data that appears in any SMC table to a comma-separated-value (CSV) file. You can then import the CSV file into most spreadsheet programs, such as Microsoft Excel, for later viewing. You can export all of the information in the table, or only a specific selection.

To export all of the information in a table, click the **Export to CSV** button in the upper right corner of the document, and then click **Export All to CSV**.



Note:

If you want to export only one row of the information in a table, click the row of data you want to export. If you want to select more than one row, press the **Shift** or **Ctrl** key as you make your selections, or simply drag the cursor to highlight the selections you want. Click the **Export to CSV** button in the upper right corner of the document and click **Export Selection to CSV**.

When the Save dialog opens, navigate to the directory where you want to save the information, and then enter the file name. (You must type **.csv** at the end of the file name so that the file is saved in this format.) Click **Save**. You can now open and view that information in the spreadsheet program of your choice.

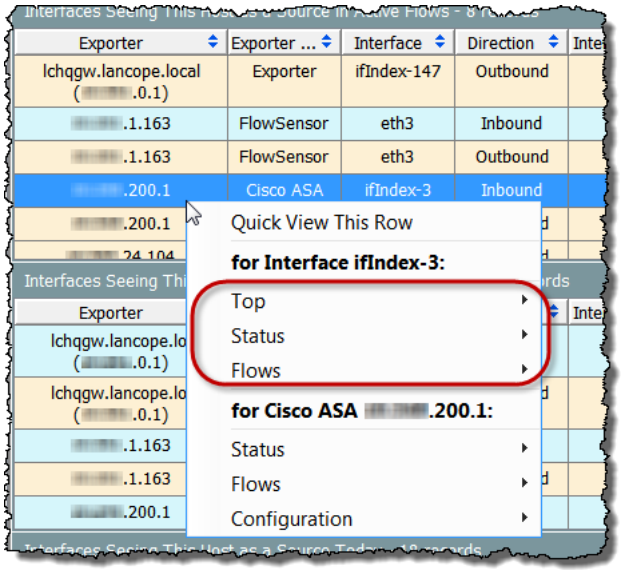
Tip:

You can also right-click any header in a table to access the Export to CSV options. (The options will appear in the pop-up menu.)

Multi-Section Pop-Up Menus

Thus far, the pop-up menus for tables that we've discussed have been fairly straightforward and have only one section of options. However, some pop-up menus have multiple sections based on how the selected row has been treated.

For instance, to view the pop-up menu shown in the following example, you would need to click an exporter on the Exporter Interfaces tab of a Host Snapshot, and then right-click.

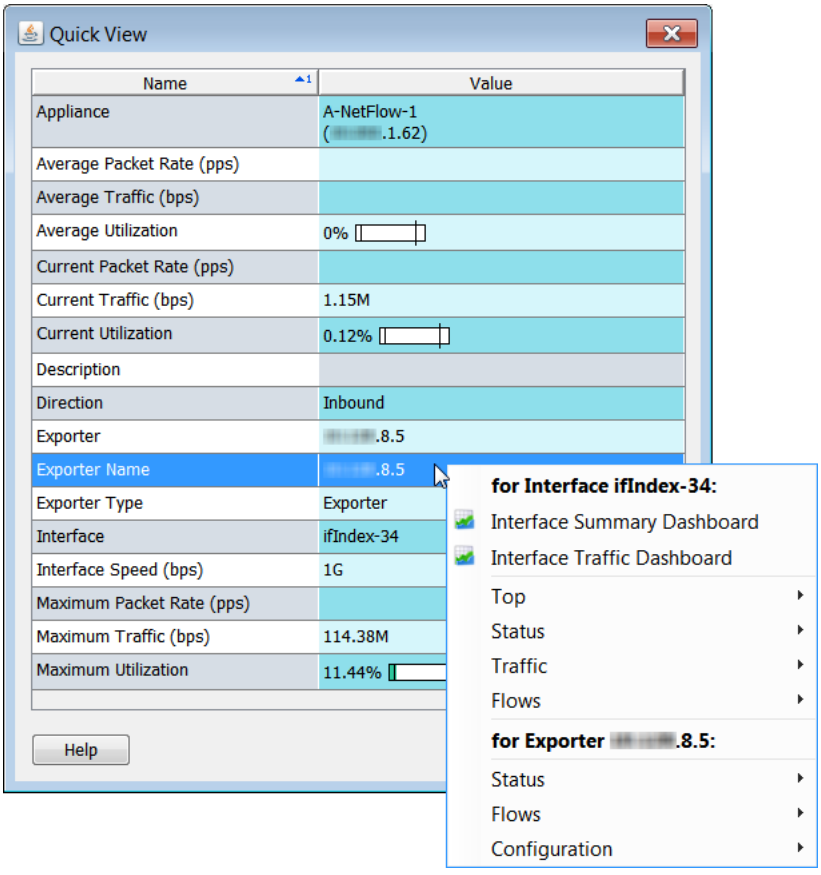


Options that appear at the very top of the pop-up menu apply to the row as a whole. The sections that appear next in the pop-up menu apply to specific cells in that row. In the previous example, you can view the following types of documents:

- Documents that pertain specifically to the ifIndex-3 interface (by clicking any of the options circled in the previous example).
- Documents that pertain specifically to the Cisco ASA xxx.xxx.200.1 exporter (the last three options on the pop-up menu).

Quick View

The Quick View dialog provides a fast and easy way to view data that appears in a particular row of a table. Simply click the desired row and press the spacebar on your keyboard. You can also right-click the row and select **Quick View This Row**.



In some cases, the Quick View provides navigation to filtered views of other documents. Right-click within a row to see any pop-up menu with related documents for more detail on the data in that row.

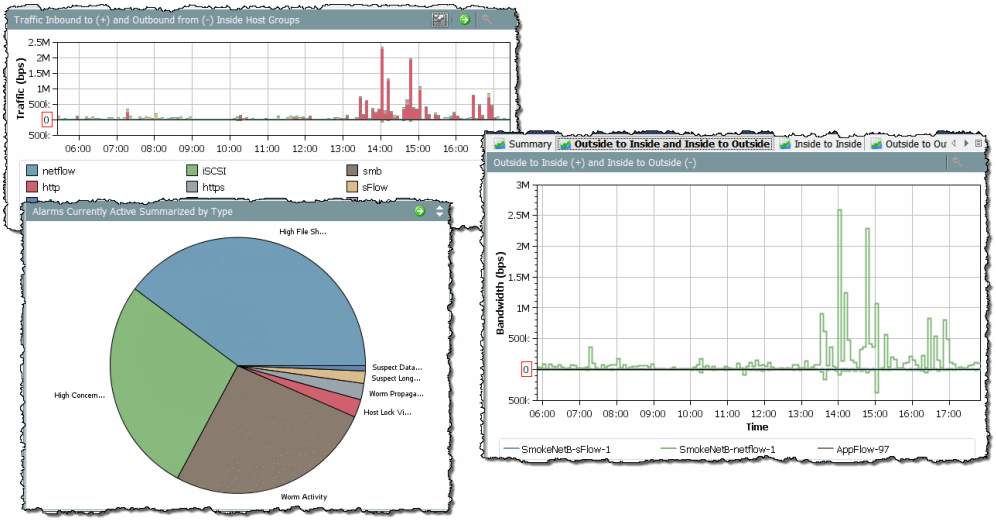
You can navigate from row to row in the associated document without closing the Quick View by pressing the **Alt** key simultaneously with the up or down key on your keyboard.

To close the Quick View dialog, do one of the following:

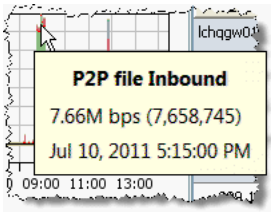
- Press the spacebar on your keyboard.
- Press the **Esc** key on your keyboard.
- Click the ❎ button in the upper right corner.

WORKING WITH CHARTS

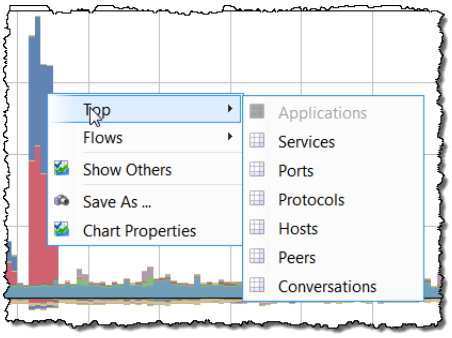
Some documents in the Stealthwatch Desktop Client contain either a bar, line, or pie chart, such as those shown in the following examples.



You can save any chart as a JPG or PNG file by right-clicking anywhere on the chart and selecting **Save As**. You can then import the graphic into another document as needed for analysis, reporting, or archiving purposes.



Each color on the chart represents a particular application, service, alarm type, or appliance, depending on the chart you are viewing. To see details about a particular item on a chart, hover the cursor over a colored area to see a tool tip with more information.



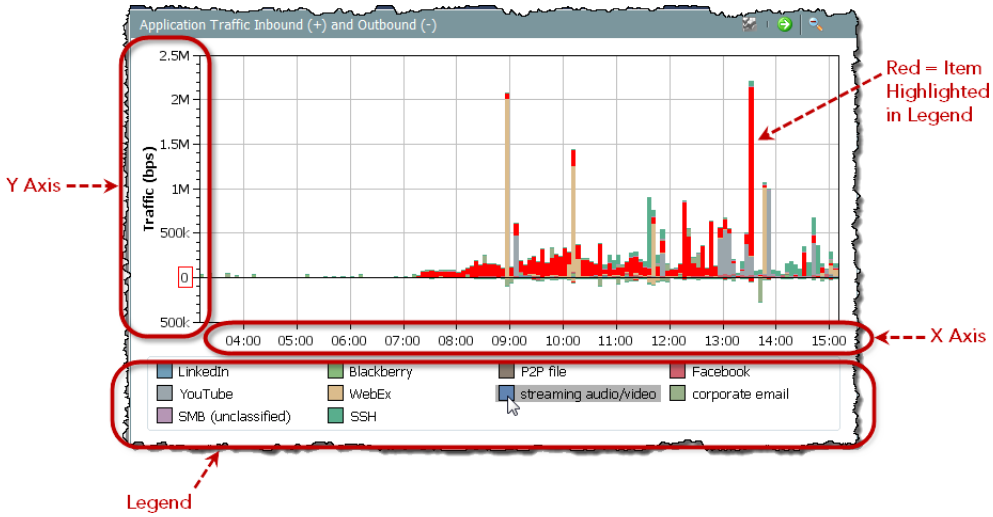
You can also right-click a colored area and click an option from the pop-up menu that appears. The document that opens will contain data that pertains specifically to the item you clicked on the chart.

You can zoom in on an area of a bar or line chart by holding and dragging the cursor across the area of interest. Once you have zoomed in, you can use the arrow keys on your keyboard to move up, down, or sideways in the chart to view different areas. To return to normal magnification, press the **F** key on your keyboard or click the **Zoom-out** button in the upper right corner of the chart.

Note:

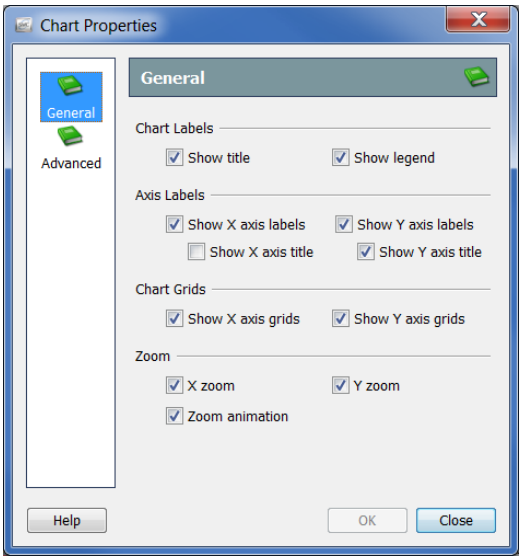
Charts that show service traffic data contain a Show/Hide button in the upper right corner to display or hide service traffic labeled generically as *Others*.

Bar and line charts are accompanied by a legend, which lists the various colors and what they represent. Hovering the cursor over an item in the legend will cause the associated data points in the chart to be highlighted in red.

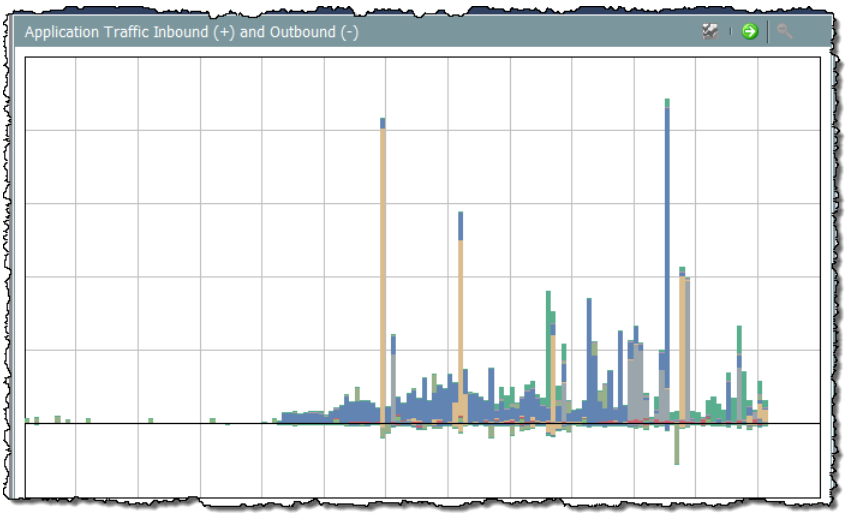


As you can see, these elements can take up a lot of space on the document. Since you can see most applicable information by hovering the cursor over a data point and looking at the tool tip, you may decide that you don't need to see the legend and axes.

To hide the legend or the axes, right-click anywhere on the chart and select **Chart Properties** to open the Chart Properties dialog. For any element that you do not want to see on the Chart Properties dialog, click its corresponding check box to remove the checkmark.



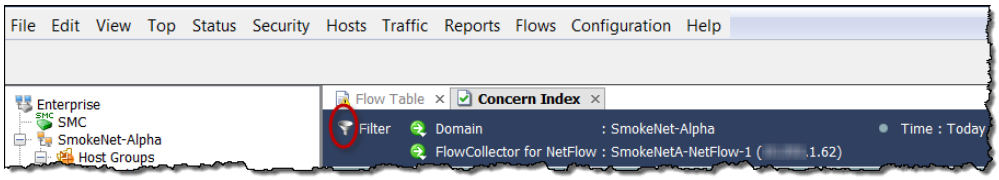
For example, if we hide the legend and axes labels on the Application Traffic Inbound and Outbound chart on the Host Group Network Dashboard, the result would look similar to the following example.



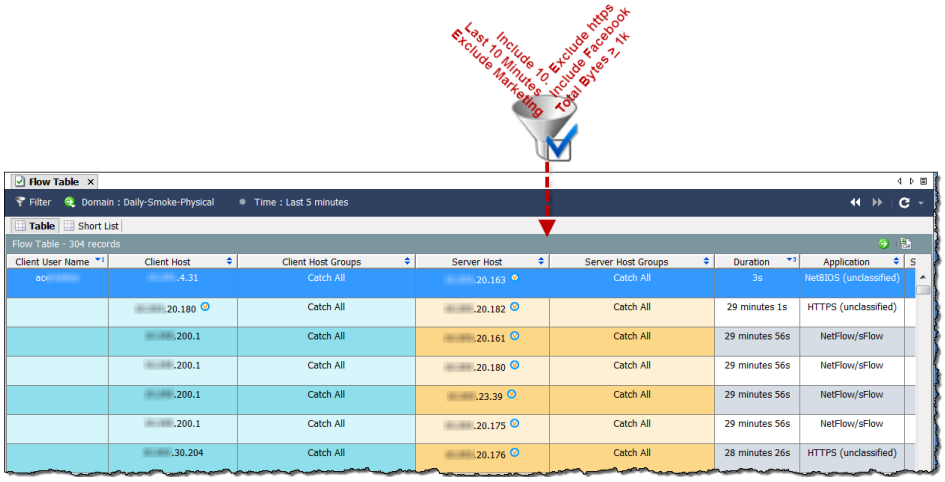
FILTERING DOCUMENT DATA

If you remember nothing else from this guide, remember this: *The filter is your friend!*

To open the filter for any active SMC document, simply click the **Filter** button on the document header.



Use the filter as a funnel to pull only the exact information you want from the vast amounts of data available from Stealthwatch.



You can filter virtually any SMC document. Filtering also allows you to view historical data, which can be very helpful from a forensic standpoint.

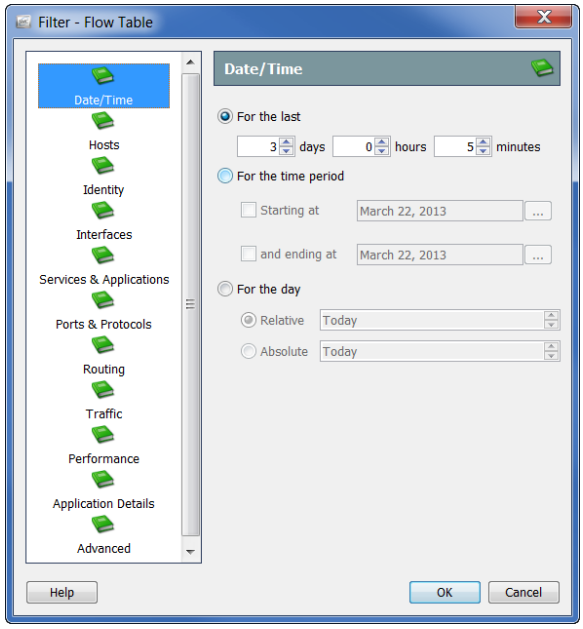
Note:

When you save a document as shared, you also save the filter settings. For more information about this, refer to "Saving Documents" on page 68.

All SMC documents have filters that operate in much the same way. Let's take a look at filtering the information you see on the Flow Table.

Date/Time

The Date/Time page allows you to filter the Flow Table to show you information for flows that occurred during specific dates and times, down to the last minute.



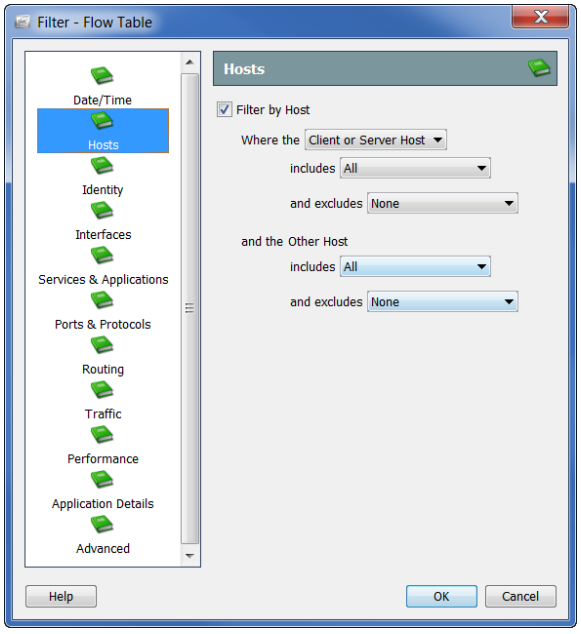
Tip:

To investigate flows that span over multiple days, use the Flow Traffic document rather than the Flow Table for a quicker response.

Hosts

The Hosts page of the Flow Table Filter allows you to display information for flows involving only specific hosts.

You can filter for server hosts, client hosts, or both. You can narrow your focus to a specific host group, range of IP addresses, or a specific IP address.



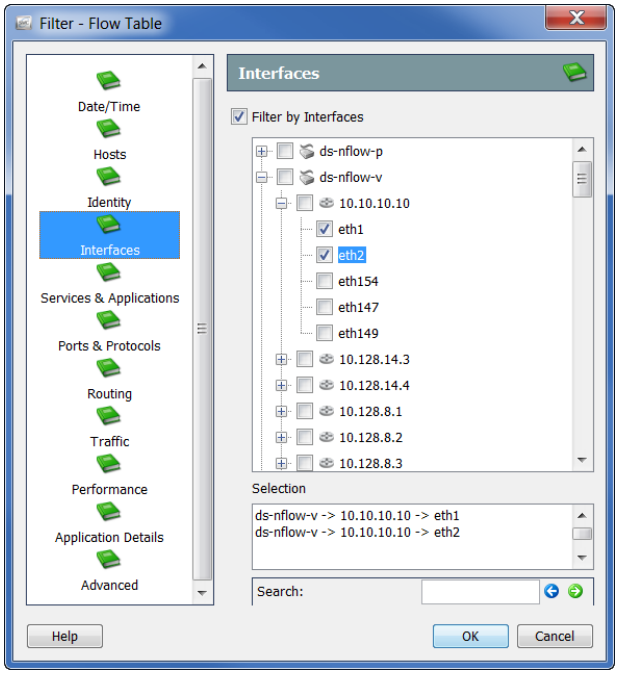
Tip:

To look for flows involving any internal host without showing NATed flows, go to the Flow Table Filter: Hosts page and specify that the broad internal IP Address Range that your network uses (e.g., 10.0.0.0/8) is to be included in the filtering process.

Interfaces

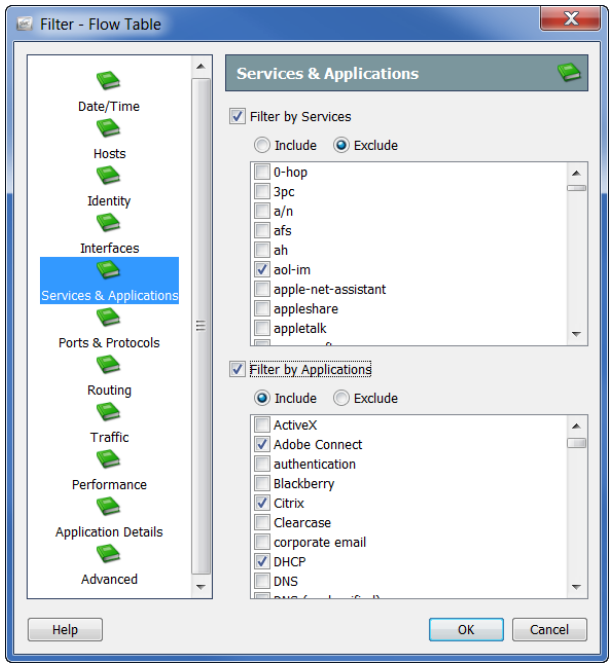
The Interfaces page of the Flow Table Filter allows you to display information for flows involving specific Flow Collectors, exporters, and/or interfaces. To choose all exporters for a Flow Collector, click that Flow Collector's corresponding check box to add a checkmark. This will also select all interfaces for those exporters.

The items you choose will appear in the Selection field of the filter. In addition, if you know a part of the item name, you can type it in the Search field at the bottom to locate it in the list of interfaces.



Services & Applications

The Services & Applications page of the Flow Table Filter allows you to display information for flows that used specific services and/or applications. You can also exclude flows that used specific services and/or applications.



Other Filter Options

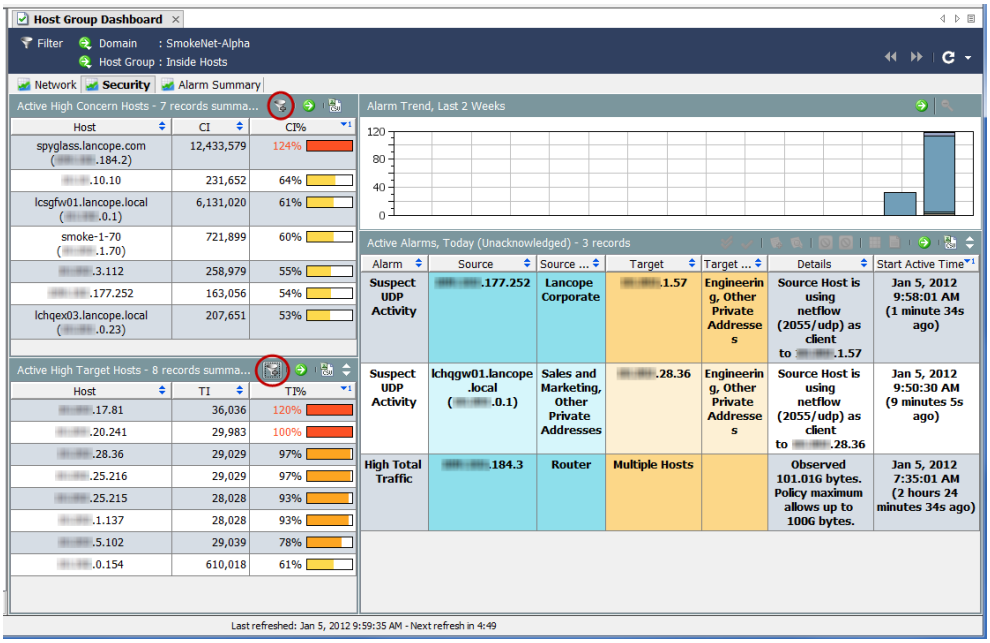
The other pages in the Flow Table Filter operate similarly to the filter pages we just covered. The following table provides brief descriptions of each of the remaining Flow Table Filter pages:

This Page...	Allows you to filter for flows based on...
Identity	user names.
Ports & Protocols	specific IANA-defined protocols, TCP/UDP ports, and/or the ports used by only clients.
Routing	DSCP points, autonomous system numbers, VLAN IDs, and/or MPLS labels.
Traffic	total bytes, total packets, client bytes, client packets, server bytes, and/or server packets, including specific value ranges, if desired. Note: The Flow Table shows raw traffic data.
Performance	total TCP connections, total TCP retransmissions, minimum/ maximum/average RTT, and/or minimum/maximum/average SRT, including specific value ranges, if desired.
Application Details	specific application details strings (included or excluded).
Advanced	maximum number of records, highest or lowest value for a specific flow record field (e.g., total bytes, client bytes, etc.), flow actions permitted/denied by a firewall, duplicate flows included or excluded, and/or interface data included or excluded, and faster querying (without sorting or grouping).

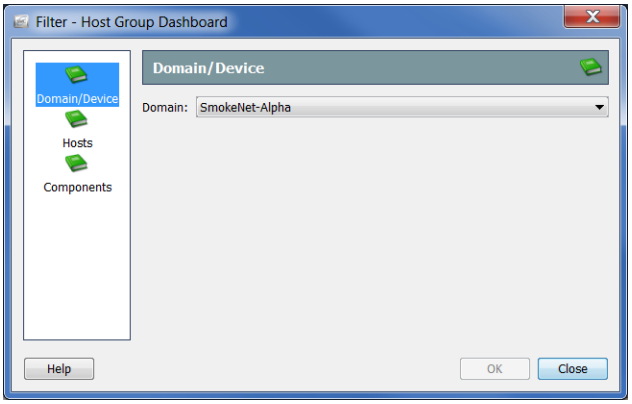
Remember, if you have questions about any document, dialog, or filter, you can always refer to the *Stealthwatch Desktop Client Online Help*.

Dashboard Filters

The filters for most SMC documents operate very similarly to the Flow Table Filter. However, the filters for dashboards are a little different. The Dashboard filters allow you to filter each component on the associated dashboard. As an example, let's take a look at how you can filter information on the Host Group Dashboard.



In the document header of the Host Group Dashboard, click the **Dashboard Filter** button to open the filter. In general, Dashboard filters contain three pages, as shown in the following three screens.

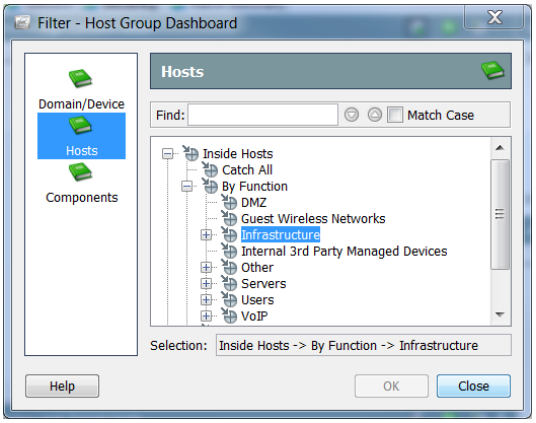


In this example, the Domain/Device page of the filter allows you to change only the domain for which you are viewing data. In the previous example, the SmokeNet-Alpha domain has been selected. Depending on the dashboard, you may also be able to choose a specific Flow Collector, exporter, and/or interface.

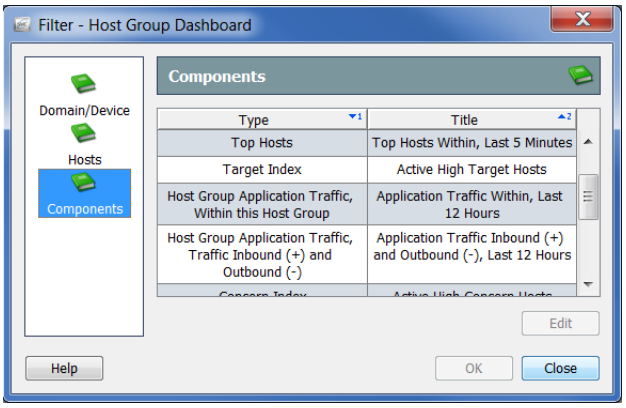
Note:

Whatever you specify on these three pages of the filter will override selections on a component filter, as we will see shortly.

To filter the dashboard to show data for a different host group, open the Hosts page. You can scroll through the list of host groups to make your selection. Alternatively, you can type all or a portion of the name for the host group in the Find field to automatically search through the list and locate the desired host group. The host group you click appears in the Selection field at the bottom of the screen. In this example, the Infrastructure host group under the By Function host group has been clicked.



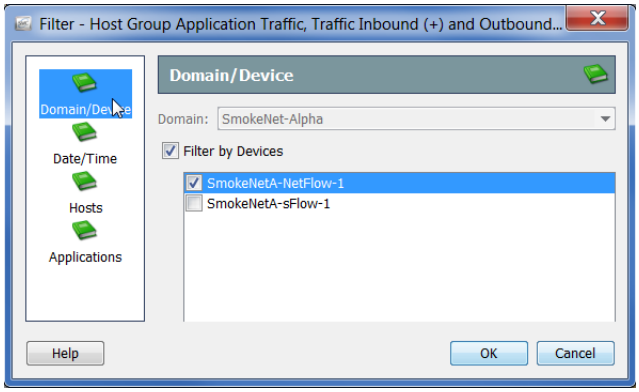
If you open the Components page of the filter, you can filter individual components on the dashboard.



Note:

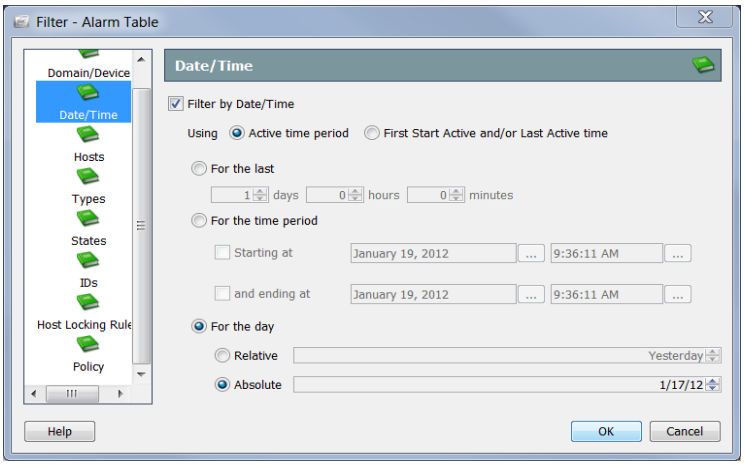
Double-click the title of a component to rename it as it appears on the dashboard.

For example, suppose you want to view any Facebook activity in the Private Addresses host group as observed by a specific Flow Collector during a specific time frame. In this case, you would click **Host Group Application Traffic, Traffic Inbound (+) and Outbound (-)** in the Type column, and then click **Edit**.



The filter dialog for that component opens. Since you already clicked the SmokeNet-Alpha domain in the dashboard filter, you cannot change it here. However, you can choose the Flow Collector whose data you want to see.

To specify the time frame you want to view, open the Date/Time page of the filter.

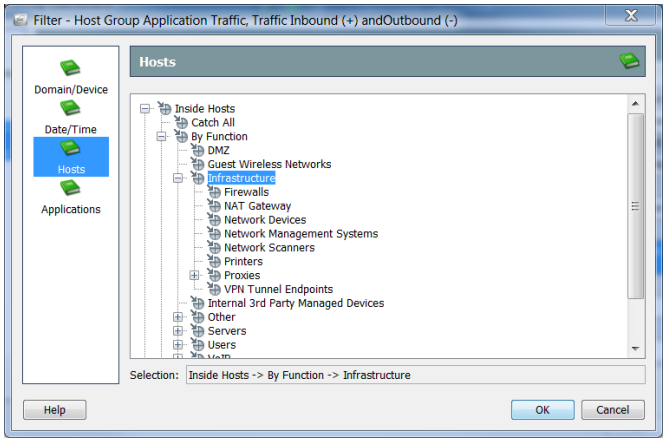


The Relative and Absolute For the day settings can be useful for documents that you want to save for future viewing with a particular layout and/or filter savings.

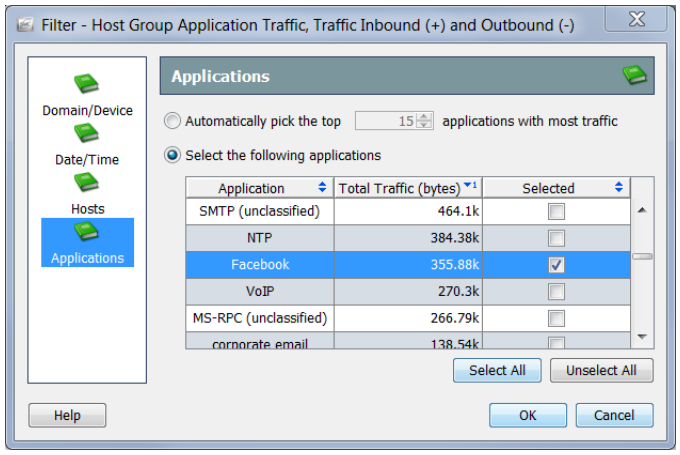
Suppose that under the "For the day" section you click **Relative**, and then select **Yesterday** from the list box. You then save the document as shared. No matter when you open that document, it will retain *Yesterday* as the selection. Thus, the document would always show you data for the day before the current day.

Now, suppose instead that under the "For the day" section you click **Absolute**, and then select **1/17/12** from the list box. You then save the document as shared. No matter when you open that document, it will retain *1/17/12* as the selection. Thus, the document will always show you the data for that date.

Since you already clicked the Infrastructure host group in the dashboard filter, you cannot change it on the Hosts page of the component filter. You can only view your selection.



To filter out all application except Facebook, open the Applications page of the component filter. By default, this filter automatically selects the top 10 applications causing the most traffic. Click the **Select the following applications** option, and then click **Unselect All** in the lower right corner to clear all selected applications. Finally, click the **Facebook** check box to add a checkmark.



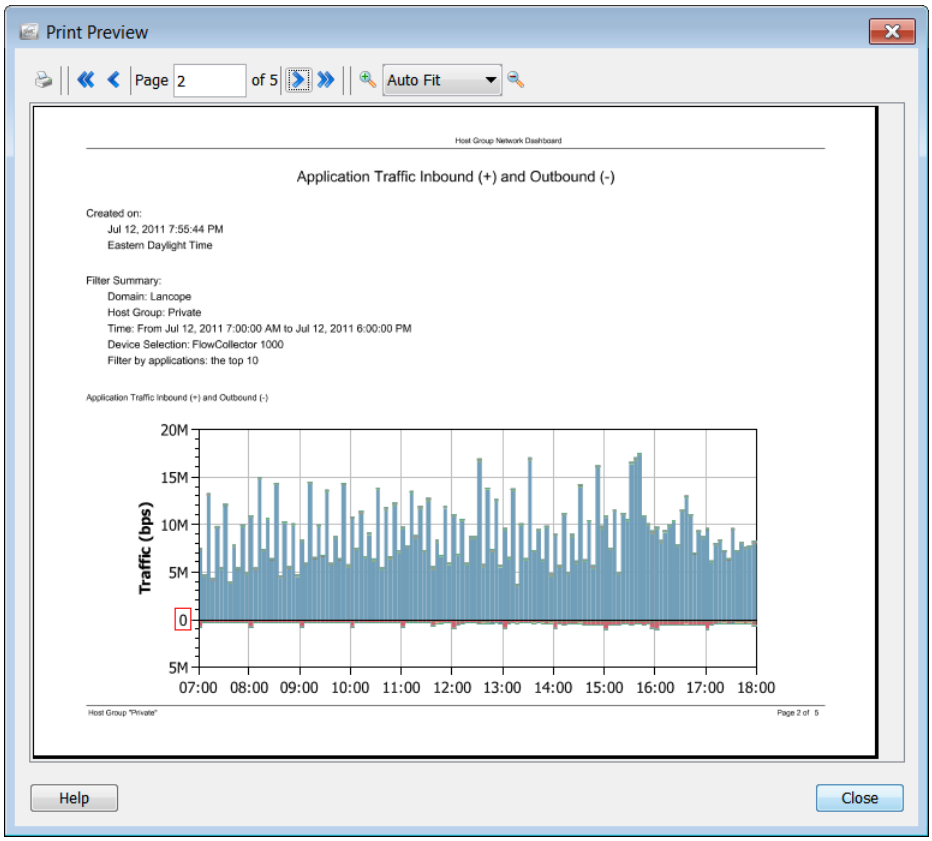
When finished, click **OK** to close the component filter and return to the dashboard filter. When finished making changes, if any, on the dashboard filter, click **OK** to refresh the dashboard with the data set you have chosen.

PRINTING DOCUMENTS

You may want to print an SMC document for archiving or reporting purposes, for later review, or to send to a colleague. The SMC allows you to preview a document, customize the print settings, print, and save a document as a PDF file.

Print Preview

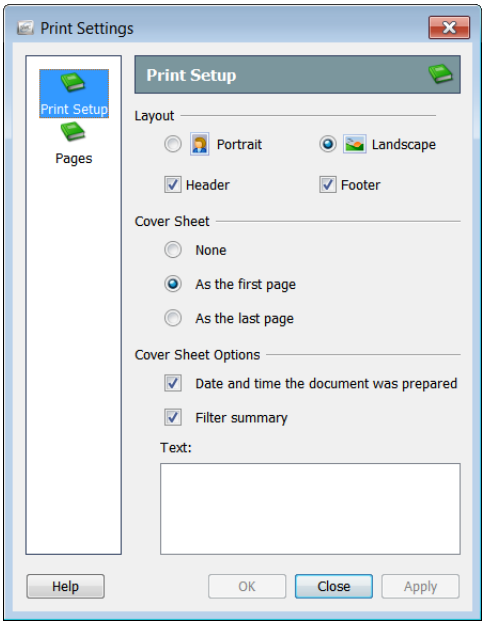
To preview how a document will look before you print it, from the Main Menu select **File > Print Preview**. The Print Preview dialog opens.



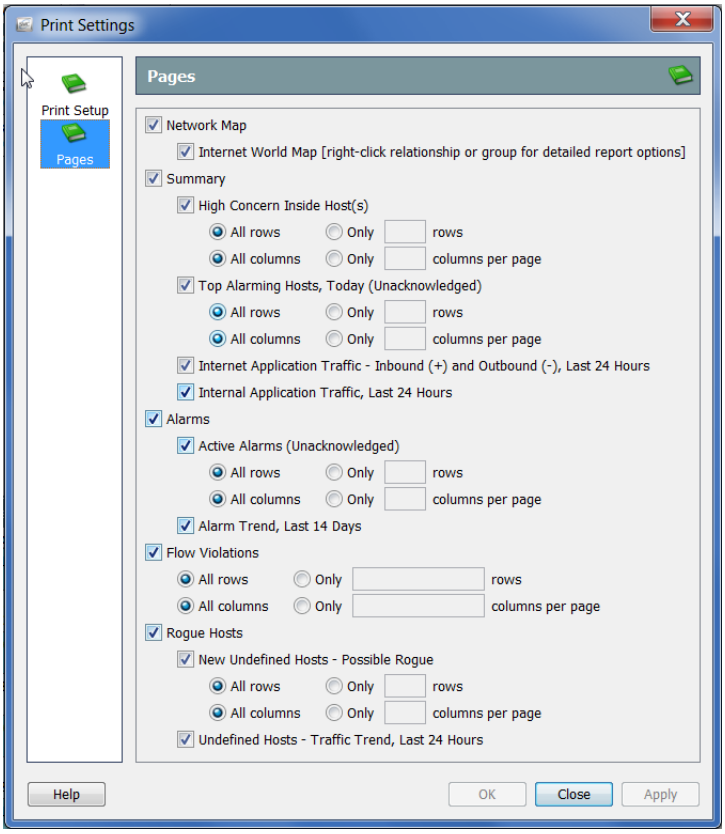
Print Settings

To customize the printed appearance of a document before you print it, use the Print Settings feature. From the Main Menu select **File > Print Settings** to open the Print Settings dialog.

On the Print Setup page you can define the layout of the page as Portrait or Landscape. You can also add a header, a footer, and even a cover sheet, if desired.

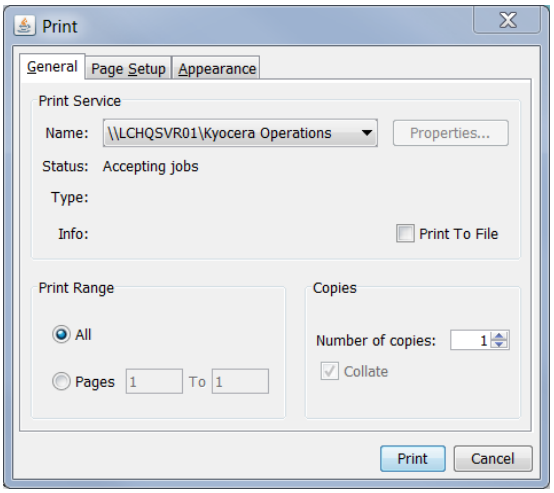


On the Pages page you can select which pages of the document you want to print, as well as which columns and/or rows.



Print

To print a document, from the Main Menu select **File > Print**. The Print dialog opens.



Note:

For higher quality fonts, set the path for an external PDF Viewer (such as Adobe Acrobat Reader) on the Preferences: PDF Viewer dialog, which you can access by selecting **Edit > Preferences** from the Main Menu.

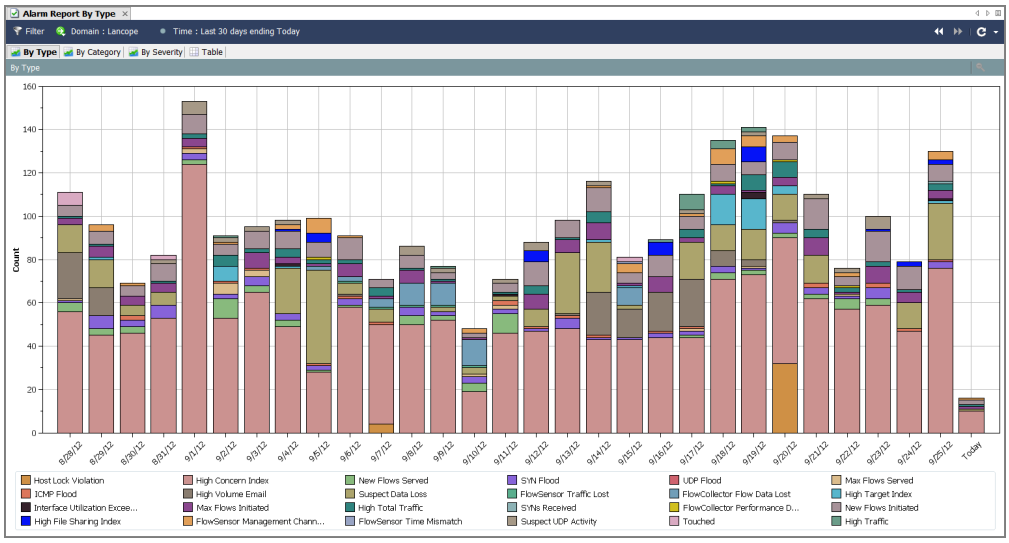
SAVING DOCUMENTS

Saving Document Layouts For Future Use

If you have rearranged the layout of an SMC document and you want to save that layout to be used later, save the document. When you save a document, it is saved to the SMC appliance for retrieval at any time.

To save a document, complete the following steps:

1. Open the document you want to save. As an example, we will open the Alarm Report By Type document.



2. Make any desired changes to the layout or filter settings.
3. (Optional) From the SMC Main Menu select **File > Print Settings**, and within the dialog that opens configure how you would like the document to look each time it is printed. Click **OK** to save changes.
4. (Optional) To see how the document would appear as a PDF, select **File >Print Preview**.

Note:

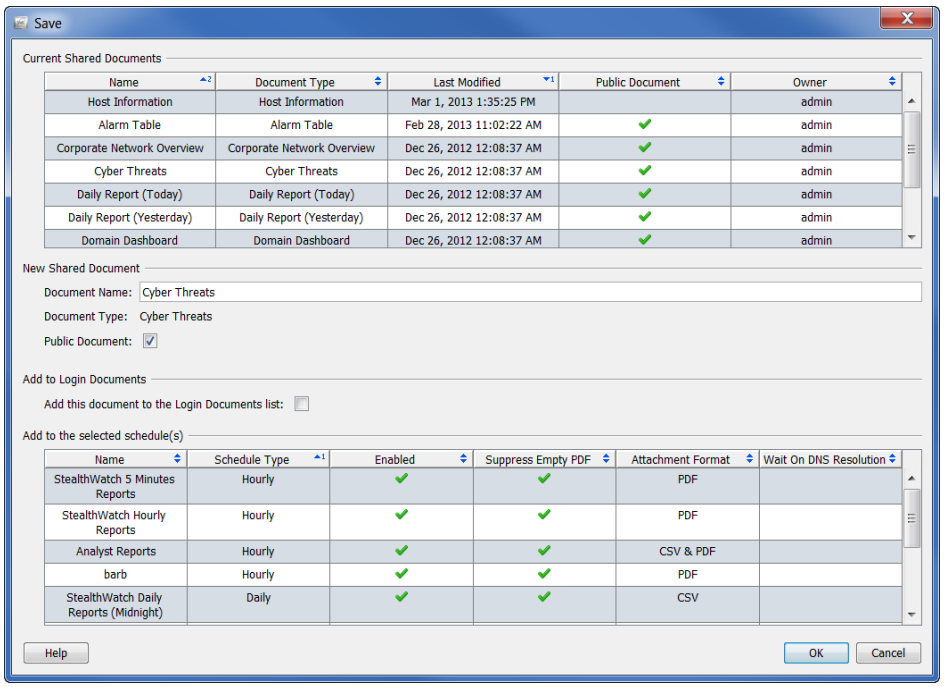
If you want to make and retain changes to the document layout (such as change the column positions or change which columns appear), select **File > Use Settings as Default**. These changes will be in effect the next time you open the document.

5. Do one of the following:

   - From the SMC Main Menu, select **File > Save** if you simply want to replace the previous version using the same name.

- From the SMC Main Menu, select **File > Save As** if any of the following situations are applicable:
  - If you want to save a copy of the document with a new name.
  - If you have created a new document and are saving the document for the first time.

    The Save dialog opens:



6. In the Name field, type a name for the document that you can easily recognize. (The system suggests a name for you.)
7. (Optional) If you want other users to be able to open this document under their user names, select the **Public** check box.

Note:

For more information about public documents, refer to "Public Documents" on page 291 in Chapter 12, "Working with Documents."

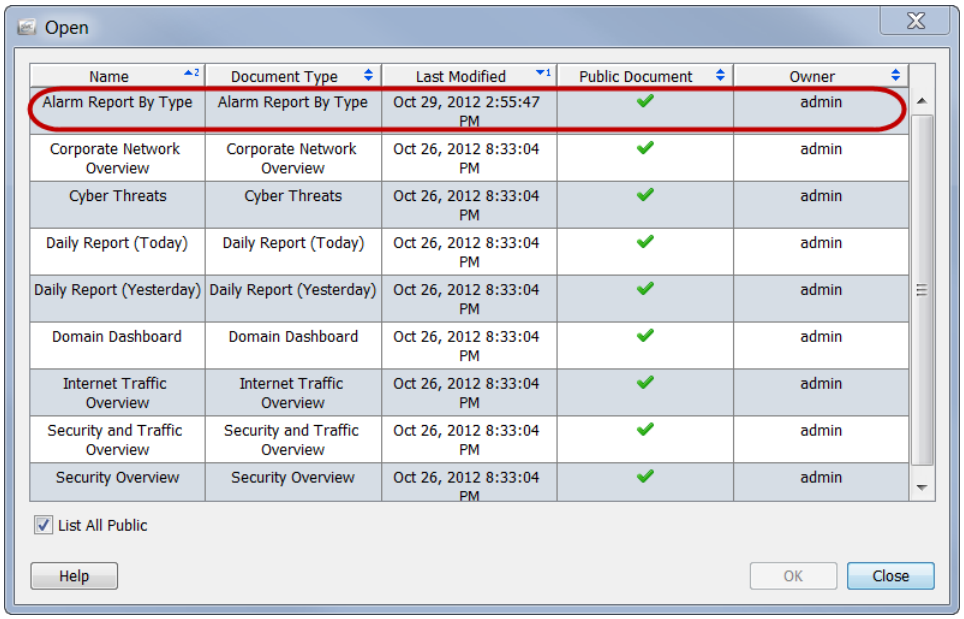
8. (Optional) If you want the document to open automatically every time you log in to the Stealthwatch Desktop Client under your user name, select the "Add this document to the Login Documents list" check box.

Note:

For more information about login documents, refer to "Login Documents" on page 286 in Chapter 12, "Working with Documents."

9. Click **OK**. The document is saved to the SMC appliance. You can now open this document under your user name, with the layout and/or filter settings you specified, on any computer with SMC access.

10. To open this document, from the SMC Main Menu select **File > Open**. The Open dialog opens.



11. Select the document and click **OK**.

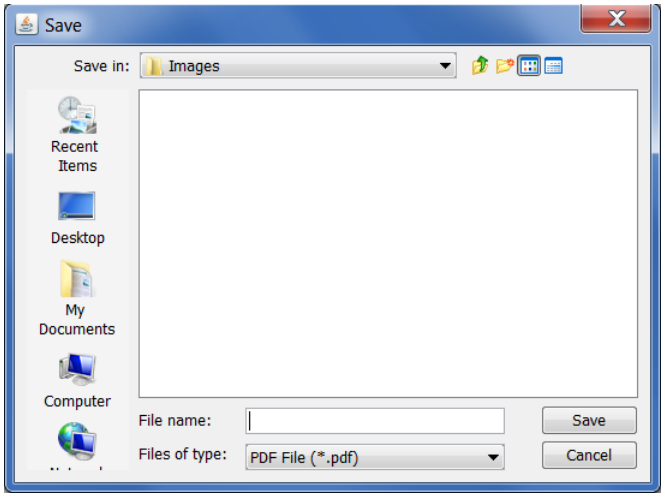
Note:

By default, only documents saved under your user name appear. To list all documents, including those created by other users, select the **List All Public** check box.

Save Document as a PDF File

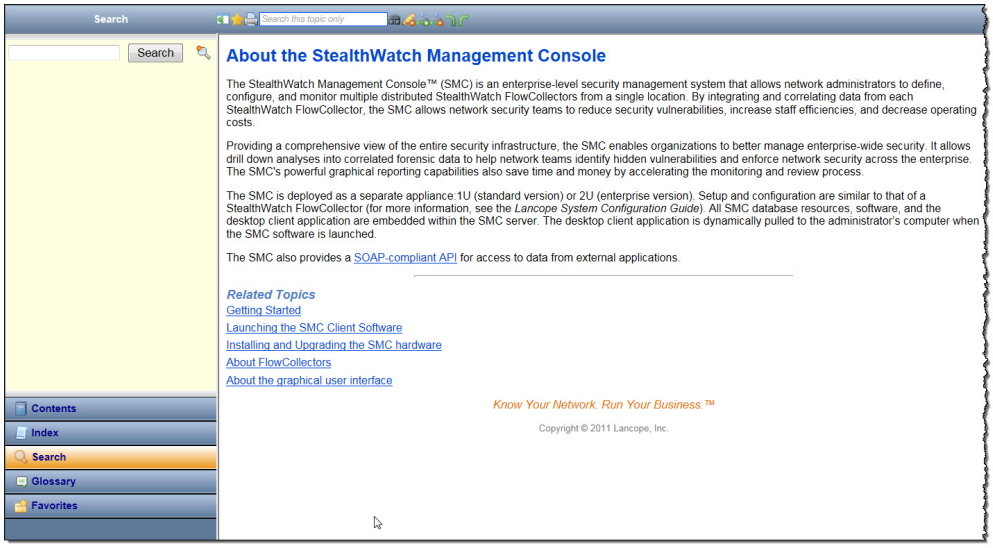
To save an active SMC document as a PDF file, from the Main Menu select **File > Print to File**. The Save dialog opens.

When the Save dialog opens, navigate to the directory and file name you want to save the document under, and then click **Save**. You can then open the document with any tool that can read PDF files.



ONLINE HELP

If you need more information about any SMC document, press the **F1** key or **Ctrl+H** on your keyboard to view the *Stealthwatch Desktop Client Online Help*. You can also go to the Main Menu and select **Help > Help**.



If you access the online Help while a document is active, you will see the Help topic pertaining to that document. If no documents are open, you will see the introductory Help topic, "About the Stealthwatch Management Console."

Note:

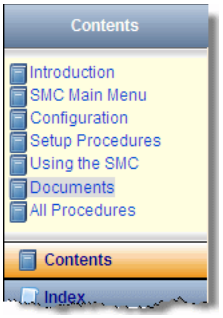
You may need to log in using the same credentials you used when you logged in to the Stealthwatch Desktop Client. If you do not see information for the active document, go back the Stealthwatch Desktop Client and press **F1** again.

After accessing the *Stealthwatch Desktop Client Online Help*, there are several ways to look for information using the following buttons at the bottom of the left navigation pane:

- Contents
- Index
- Search
- Glossary
- Favorites

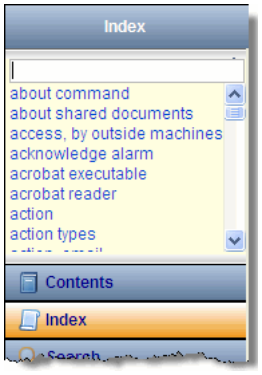
You can also use the Quick Search feature at the top of the topic area to search the open topic.

Contents



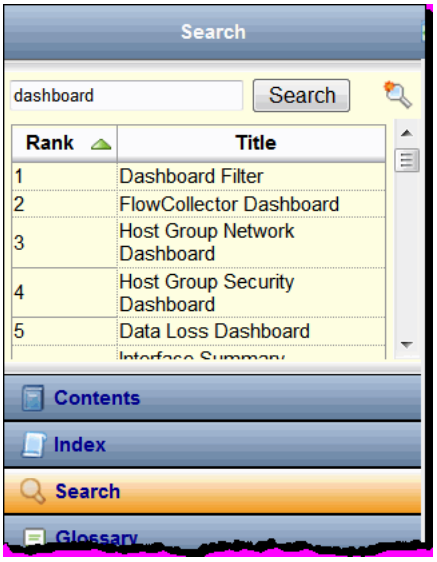
The Contents pane provides the table of contents for the online Help, organized much like the table of contents for a book. To view, click **Contents** at the bottom of the left navigation pane. Click an item in the list to view the corresponding Help topic.

Index



The Index pane provides a list of words that you can search through to find related topics. To view, click **Index** at the bottom of the left navigation pane. Click an item in the list to view that Help topic. You can scroll through the list and make a selection, or you can type text into the field at the top to go immediately to that text in the list. Then, make a selection to view the desired topic.

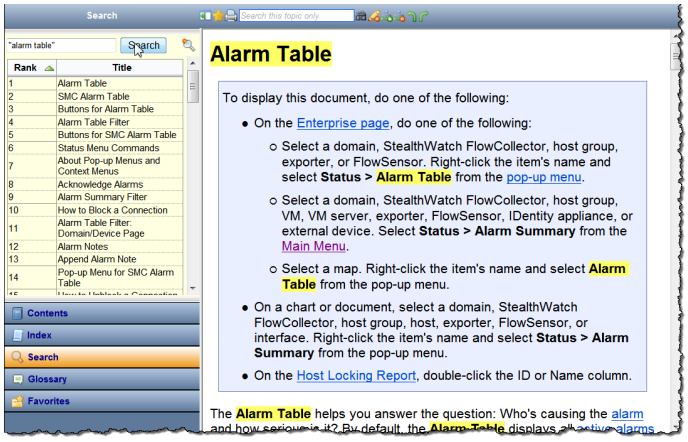
Search



The Search pane opens by default if no documents are open when you access the online Help. Type the text you are seeking in the field at the top, and then click **Search** at the bottom of the left navigation pane or press **Enter** on your keyboard. A list of topics appears, ranked according to relevance to the text you typed. Click an item to view that topic.

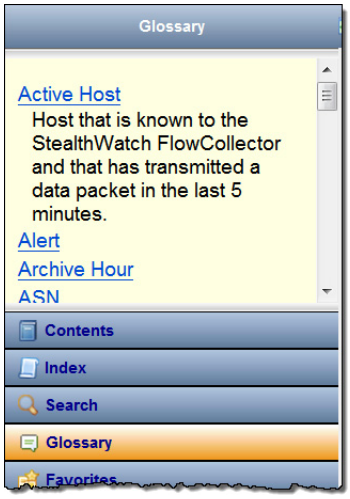
In addition to locating information in general, this feature can be handy if you need to know how to open a particular SMC document. Every Help topic pertaining to a specific document provides instructions in the first paragraph on how to access that document.

For example, suppose you need to open the Alarm Table, but you don't know or can't remember how. Simply type "alarm table" in the Search field, and then press **Enter**. When the Alarm Table Help topic appears in the Search results, click the topic name. When the Help topic appears, you will see instructions for accessing the Alarm Table.



If there is an item you frequently seek in the online Help, you can add the search text to your Favorites list. Simply type the text in the Search field, and then click the **Search Favorite** button. The next time you need to search for that text, you can simply go to your Favorites list and click it.

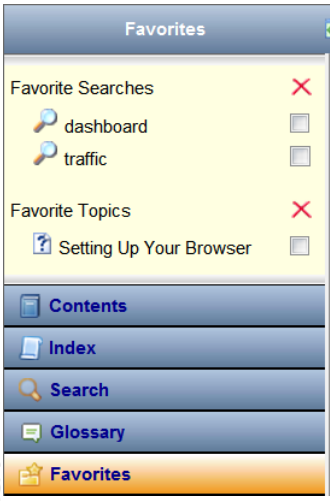
Glossary



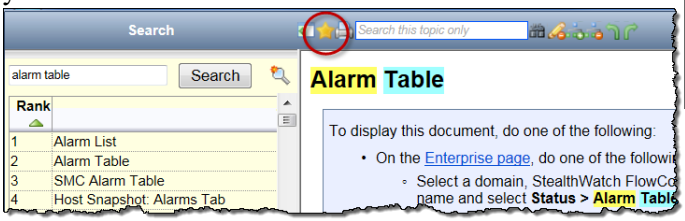
The Glossary pane provides definitions for words that are commonly used throughout Stealthwatch. To view, click **Glossary** at the bottom of the left navigation pane. Click a word in the list to view its definition.

Favorites

The Favorites pane includes any search item or topic that you have marked as a favorite. To view, click **Favorites** at the bottom of the left navigation pane.



We have already talked about how to add search text to your list of Favorites. You can also add topics to the list. This feature can be useful if you find that you need to refer to a specific topic frequently. Click the **Topic Favorite** ⭐ button in the Help tool bar above the topic that you want to add to your list of favorites. The next time you need to look at that topic, you can simply go to your Favorites list and click it.



If you click a Favorite Searches item, the Search pane will open, listing the topics that pertain to that item. Click an item in the list to view that Help topic.

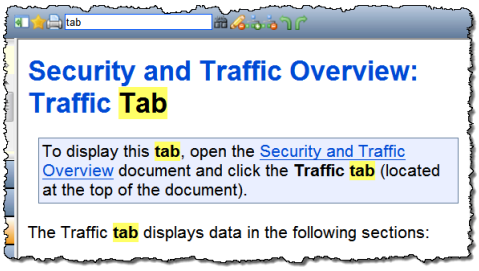
If you click a Favorite Topics item, that Help topic opens.

To remove an item from the Favorites list, click the corresponding check box ☑ to add a checkmark, and then click the ✕ button.

Quick Search

The Quick Search field is located above the Help topic in the Help tool bar.

This field allows you to search for text within the Help topic you are viewing. Simply type the text in the Quick Search field, and then click the **Search** button or press **Enter** on your keyboard. If the text you typed appears in the topic, it will be highlighted in yellow, as shown in the following example. To remove the highlighting, click the **Highlighter** button.



Note:

For more information on any of the buttons in the Help tool bar, hover the cursor over the button to view the tool tip.

KEYBOARD SHORTCUTS

The following table provides a list of many keyboard shortcuts you can use to perform various functions in the Stealthwatch Desktop Client. Many of these shortcuts equate to selections from the Main Menu:

Note:

We have not discussed all of the documents mentioned in this list, but this will serve as a handy reference for you as you become more familiar with the SMC.

Press	To...
←	On a chart: Move backward (left) on the zoomed-in area.
→	On a chart: Move forward (right) on the zoomed-in area.
↑	On a chart: Move up on the zoomed-in area. When using the Find field for a tree: Locate the previous item in the tree with the same text that is in the Find field.
↓	On a chart: Move down on the zoomed-in area. When using the Find field for a tree: Locate the next item in the tree with the same text that is in the Find field.
Alt + ←	When multiple documents are open, view the document that is to the left of the active document. On the Quick View for Flow dialog: Move left from tab to tab.
Alt + →	When multiple documents are open, view the document that is to the right of the active document. On the Quick View for Flow dialog: Move right from tab to tab.
Alt + ↑	On the Quick View dialog: Move up a row in the corresponding document table.
Alt + ↓	On the Quick View dialog: Move down a row in the corresponding document table.
- continued -	

Press	To...
Alt + F	When the Enterprise tree Find field is hidden: Display the Find field. When the Enterprise tree Find field is shown: Place the cursor in the Find field.
Ctrl	On a table, pressing this key while clicking a column heading removes any sort order from that column.
Ctrl + ←	Display data on the active document from an earlier time frame. This shortcut is the same as selecting **View > Time Backward** from the Main Menu. You can also click the **Time Backward** button on the Main Tool Bar.
Ctrl + →	Display data on the active document from a later time frame. This shortcut is the same as selecting **View > Time Forward** from the Main Menu. You can also click the **Time Forward** button on the Main Tool Bar.
Ctrl + B	Open the Document Builder so that you can create your own custom documents and layouts. This shortcut is the same as selecting **View > Document Builder** from the Main Menu. On the Document Builder, this shortcut is the same as selecting **View > New Document Builder**.
Ctrl + C	Copy selected text. This shortcut is the same as selecting **Edit > Copy** from the Main Menu.
Ctrl + D	Use the same layout settings each time you open a particular SMC document. This shortcut is the same as selecting **File > Use Settings As Default** from the Main Menu.
Ctrl + E	Open the Host Group Editor. This shortcut is the same as selecting **Configuration > Edit Host Groups** from the Main Menu.
Ctrl + F	When the Enterprise tree Find field is hidden: Display the Find field.

- continued -

Press	To...
Ctrl + G	Place the cursor in the global Search field to search all SMC documents for an IP address or an alarm ID. This shortcut is the same as selecting **Edit > Global Search** from the Main Menu.
Ctrl + H	Display the online Help that pertains to the active dialog or document. (You may need to log in first.) This shortcut is the same as selecting **Help > Help** from the Main Menu or from the Document Builder Main Menu.
Ctrl + I	Display the properties of the selected object. This shortcut is the same as selecting **Configuration > Properties** from the Main Menu.
Ctrl + N	Open a new instance of the Stealthwatch Desktop Client. This shortcut is the same as selecting **View > New Main Window** from the Main Menu.
Ctrl + O	Open a document that was saved as a DAR file. This shortcut is the same as selecting **File > Open** from the Main Menu.
Ctrl + P	Print the active document. This shortcut is the same as selecting **File > Print** from the Main Menu.
Ctrl + Q	Close the Stealthwatch Desktop Client (i.e., quit or exit). This shortcut is the same as selecting **File > Exit** from the Main Menu.
Ctrl + S	Save the active document with a specific set of layout and filter settings as a DAR file. This shortcut is the same as selecting **File > Save As** from the Main Menu.
Ctrl + T	Hide or show the Enterprise tree. This shortcut is the same as selecting **View > Hide/ Show Tree** from the Main Menu.
- continued -	
Ctrl + V	Insert (paste) copied text into an editable field. This shortcut is the same as selecting **Edit > Paste** from the Main Menu.

Press	To...
Ctrl + W	Close the active document. This shortcut is the same as selecting **File > Close** from the Main Menu.
Ctrl + Shift + C	Collapse the selected branch on the tree, or collapse all items on the tree if no branch is selected. This shortcut is the same as selecting **View > Collapse All** from the Main Menu or from the Document Builder Main Menu.
Ctrl + Shift + E	Expand the selected branch on the tree, or expand all items on the tree if no branch is selected. This shortcut is the same as selecting **View > Expand All** from the Main Menu or from the Document Builder Main Menu.
Ctrl + Shift + S	Save the active document with a specific set of layout and filter settings as a DAR file with a new name. This shortcut is the same as selecting **File > Save As** from the Main Menu.
Ctrl + Shift + W	Close all open documents. This shortcut is the same as selecting **File > Close All** from the Main Menu.
Delete	Delete the selected item. This shortcut is the same as selecting **Configuration > Delete** from the Main Menu.
Esc	Close the dialog window.
F	On a chart: Return to the original zoom level.
F1	See online Help that pertains to the active dialog or document. (You may need to log in first.)
- continued -	
F3	In the Document Builder: Find the next item in the search tree with the same text that is in the search field. This shortcut is the same as selecting **Edit > Find Next in Tree** in the Document Builder Main Menu.

Press	To...
F5	Refresh the data in the active document. This shortcut is the same as selecting **View > Refresh** from the Main Menu. You can also click the **Refresh** button on the Main Tool Bar.
Alt + ←	When an open document contains multiple tabs, view the tab that is to the left of the active tab.
Alt + →	When an open document contains multiple tabs, view the tab that is to the right of the active tab.
Shift + F3	In the Document Builder: Find the previous item in the search tree with the same text that is in the search field. This shortcut is the same as selecting **Edit > Find Previous in Tree** in the Document Builder Main Menu.
Spacebar	On some tables: Click within a row and press the spacebar to display the Quick View dialog for the selected item. If the Quick View dialog is open, press the spacebar to close it.
Z	On a chart: Zoom in on the X-axis.

3

HOST MANAGEMENT

OVERVIEW

Managing all of the hosts in a network individually would be a monumental task. However, Stealthwatch helps you reduce much of this labor by allowing you to organize your hosts into host groups.

Host groups offer flexibility in the way you can organize hosts. In general, hosts can belong to multiple groups. In addition, you can define policies per host group and/or per host.

In this chapter you will learn how to logically organize hosts into host groups so that you can monitor different areas of your network and manage host behavior more efficiently.

This chapter includes the following topics:

- Host Groups
- Relational Flow Maps

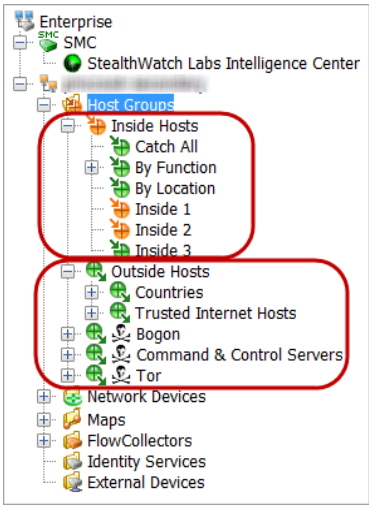
HOST GROUPS

A host group is essentially a virtual container of multiple host IP addresses or IP address ranges that have similar attributes, such as location, function, or topology. By grouping hosts into host groups, you can control how the Stealthwatch Flow Collectors monitor and respond to the behavior of those hosts as a group, rather than individually.

Administrators can organize hosts in any way that makes sense for their organization. With this freedom, reporting and traffic management gain unlimited flexibility. In addition, policy management is much easier, allowing administrators to set policies for hosts based on the roles those hosts play in the network.

The Stealthwatch Desktop Client displays the host group structure, as well as the network structure, in the Enterprise tree, as shown in the following example. By default, each domain contains the following top-level host groups to which you can add subordinate host groups:

- **Inside Hosts** – Contains all host groups whose hosts have been specifically defined as being a part of your network.
- **Outside Hosts** – Contains all host groups whose hosts have not been specifically defined as being a part of your network.



Note:
Your login privileges determine whether or not you see all of the host groups in the Enterprise tree.

Depending on your login privileges, you can add as many top-level host groups as desired, each containing as many sub-host groups as desired, which can also contain sub-host groups, etc. Any IP address that is not defined for a specific host group automatically falls into the Countries sub-host group of the Outside Hosts host group. You can use duplicate host group names, but not at the same host group level (i.e., below the same parent host group).

Note:
Although you can create host groups at any level under the Host Groups branch of the Enterprise tree, we recommend that you add them under the Inside Hosts or the Outside Hosts branches.

By default, Stealthwatch does not create policies for hosts that are outside your network. However, if you need to track outside hosts that cause traffic on your network on a regular basis, you can place them in an Outside Host host group and establish a policy for the group. Then, you can adjust settings just as you would for inside hosts.

Note:

You can also create a top-level host group (i.e., at the same level as Inside Hosts or Outside Hosts) if you have a need to do so for special reporting purposes.

Following are some situations for which you might want to track the behavior of specific outside hosts:

- When you are using outside DNS servers.
- When you have third-party consultants or vendors who regularly access your network.
- When you have partner firms that regularly access your network.

Catch All Host Group

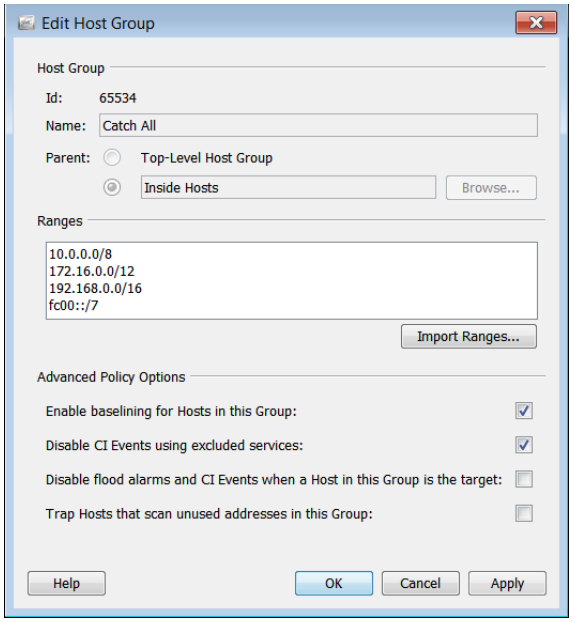
The Inside Hosts host group contains the default Catch All sub-host group. Administrators can use the Catch All host group to help refine the host group structure.

We recommend that you initially place all large IP ranges that correspond to your network in the Catch All host group. Then, as you create other host groups with more narrowly defined IP ranges or specific IP addresses, those ranges/addresses will move out of the Catch All host group automatically.

New SMC installations for Stealthwatch v6 place the following IP ranges (RFC 1918 and RFC 4193) into the Catch All host group by default:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- fc00::/7

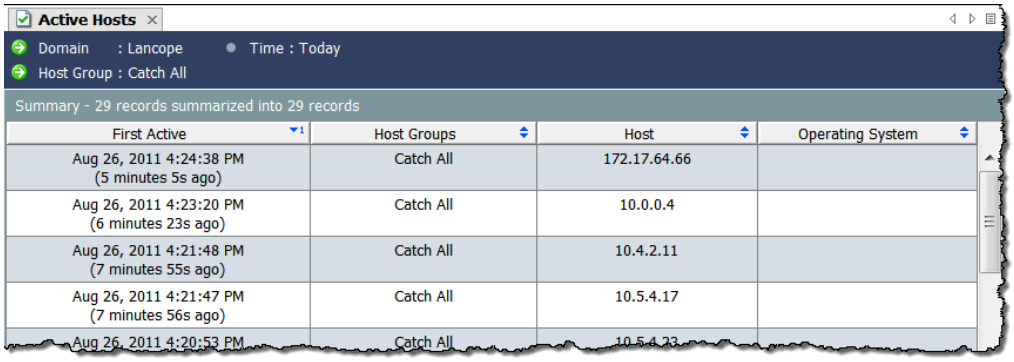
If you have registered any public IP addresses, we recommend that you also manually place these ranges in the Catch All host group. Depending on your login privileges, you can see which IP ranges/addresses have been defined in your Catch All host group by right-clicking the **Catch All** host group in the Enterprise tree and selecting **Configuration > Host Group Properties**.



Notes:

- To edit any host group, right-click the host group in the Enterprise tree and select **Configuration > Host Group Properties**.
- The host name can use alphanumeric characters including the following special characters: < , > . ? ” ‘ : ; | { [}] + = _ - ( ) * & ^ % $ # @ ! ~ ‘ and a “space.”

Ideally, when you finish defining your host group structure, there should be no more active IP addresses in the Catch All host group. To identify any rogue host IP addresses, you can look at the Active Hosts document for the Catch All host group. Simply right-click the **Catch All** host group in the Enterprise tree, and then select **Hosts > Active Hosts**.

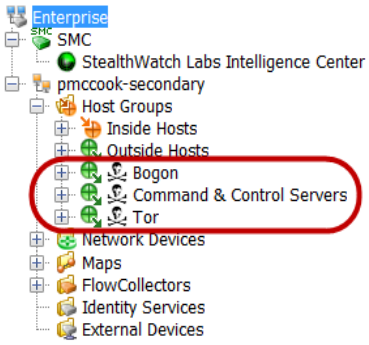


Every network is different, of course, but here are some things to consider when assigning hosts to the Catch All Host Group:

- Which areas within the network are more sensitive than others?
- Which areas of the network undergo change frequently vs. those areas that are fairly stable?
- Where are your critical assets?
- Which hosts perform similar functions?
- What are the different functions that your hosts perform?
- Do you have any hosts that are simply quirky and routinely behave "strangely"?

Threat Intelligence Feed Host Groups

Threat Intelligence Feed contains IP addresses, port numbers, protocols, host names, and URLs known to be used for malicious activity. The following host groups are included in Threat Intelligence Feed:



- Bogon - A bogon is an IP address that has not been officially assigned on the public Internet.
- Command & Control Servers - A C&C server is the centralized computer that issues commands to a botnet and receives reports back from the hijacked computers.
- Tor - Tor is an Internet anonymization service.

Note:

To detect URLs in Threat Intelligence Feed that may be contacting your hosts, you must have a FlowSensor or router installed that is configured to export IPFIX (vs. NetFlow). (By default, the FlowSensor is configured to export IPFIX.).

If you want to investigate a host that has communicated with a malicious host in one of the previously mentioned host groups, but the malicious host no longer appears in the relevant host group, go to the Alarm Table and filter on the following components:

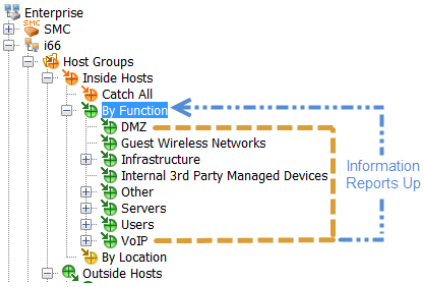
- Types - Select the applicable bogon, Command & Control, or Tor alarm(s), depending on which type of malicious host(s) you are wanting to filter on.
- Date/Time - Filter according to the time period for which you want to investigate.

Note:

The SLIC Threat Feed host group branches cannot be renamed, changed, moved, or deleted.

Information Reports Up

Any SMC document for a host group includes information for all hosts within its sub-host groups. For example, if you open the Host Information document for the By Function host group (without changing any of the filter settings), you will see information about all hosts in every sub-host group under it, as well as any hosts defined directly under the By Function host group.



Strategies for Creating Host Groups

At this point, your host groups are most likely already defined. But, to help you understand how host groups work, let's take a moment to look at some recommended strategies for creating them.

All Stealthwatch Flow Collectors ship with a default host group structure. Depending on your login privileges, you can modify the default host groups to suit the needs of your network. You can create additional host groups as well as delete any of the default host groups except for these: Inside Hosts, Catch All, Outside Hosts, Countries, and Command & Control Servers.

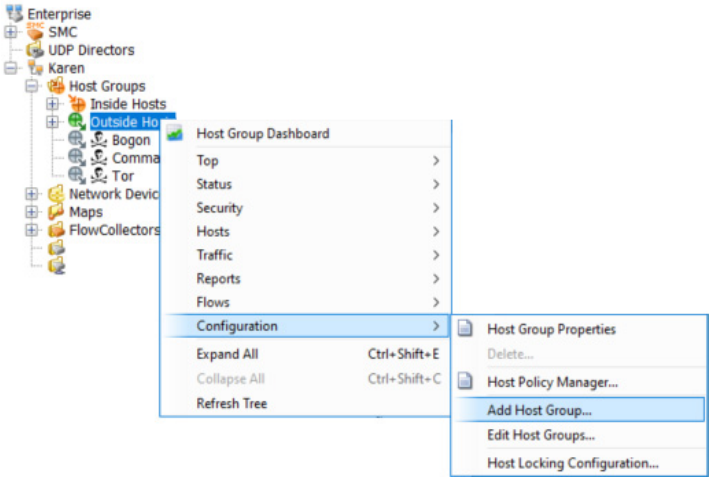
Earlier, we talked about recommendations for placing hosts initially in the Catch All host group. In addition, we recommend that hosts that behave similarly to each other be placed in a host group together. However, you could create different host groups for each department within your network, geographical regions, IP segments, or any other categories that makes sense for your organization.

Creating Host Groups

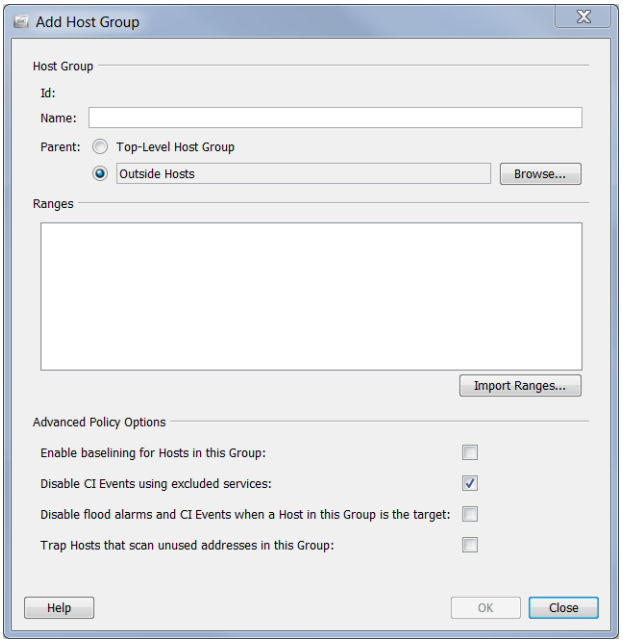
To create a host group, complete the following steps:

1. On the Enterprise page tree menu, click either the **Inside Hosts** or **Outside Hosts** folder (whichever one to which you are adding another host group).

2. Right-click either the **Inside Hosts** or the **Outside Hosts** host group (whichever is applicable), and then select **Configuration > Add Host Group**.



The Add Host Group dialog opens.



3. In the Name field, type a name for the host group you are adding (e.g., *Partners*).
4. In the Parent field, click the parent for the new host group if the default is not correct.
5. In the Ranges field, type the desired IP address ranges. Click **Import Ranges** if you have an existing file containing the IP addresses for this host group.
6. In the **Advanced Policy Options** section, click the options that you wish to apply to the new host group.
7. Click **OK** to close the Add Host Group dialog. The Enterprise page tree menu automatically updates to include your new host group.

IP Addresses

You can use either IPv4 or IPv6 IP addresses to include in each host group. If you enter IPv4 IP addresses, you must use the forms of notation described in the following table:

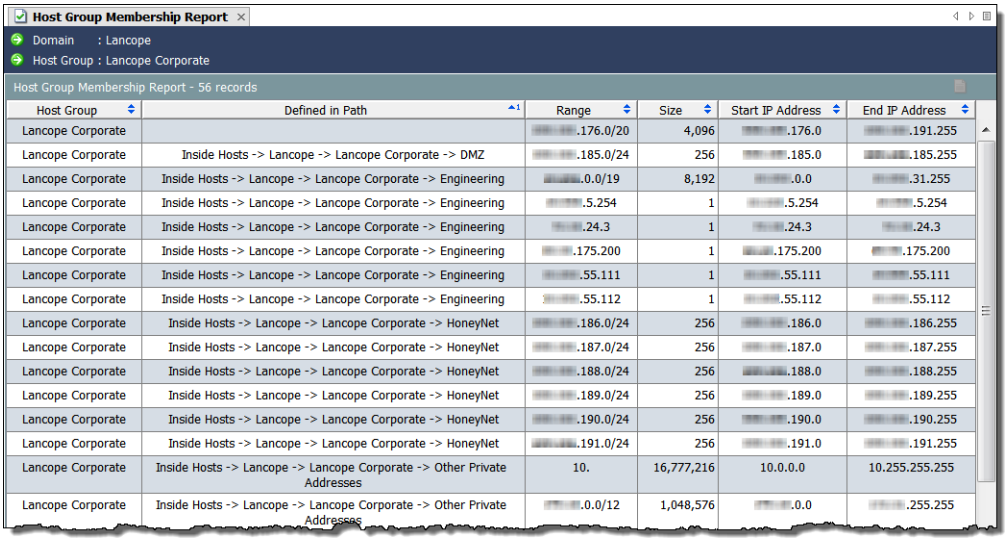
Notation	Examples
Single IP address	**10.52.1.55** Includes only the host at 10.52.1.55
Trailing dot subnet	**10.52.** Includes any IP address from 10.52.0.0 to 10.52.255.255 **Note:** You must include the trailing period (.) at the end.
Classless Inter-Domain Routing (CIDR) notation (i.e., using a "/" to indicate the masked bits)	**10.52.1.0/24** Includes any IP address from 10.52.1.0 to 10.52.1.255 **Note:** Use this notation if you prefer to enter the IP address using a "mask." The *Stealthwatch Desktop Client Online Help* provides more information on using CIDR notation. Use the **Search** function to locate references to **CIDR**.
Range of networks	**10-11.** Includes any IP address from 10.0.0.0 to 11.255.255.255 **10.52-53.** Includes any IP address from 10.52.0.0 to 10.52.255.255, and from 10.53.0.0 to 10.53.255.255 **10.52-55.3.** Includes any IP address from 10.52.3.0 to 10.52.3.255; from 10.53.3.0 to 10.53.3.255; from 10.54.3.0 to 10.54.3.255; and from 10.55.3.0 to 10.55.3.255 **Note:** Be sure to include the trailing period (.) at the end.
Range of hosts	**10.52.1.0-10** Includes any IP address from 10.52.1.0 to 10.52.1.10 **10.52.0.0-10.52.255.255** Includes any IP address from 10.52.0.0 to 10.52.255.255 **Note:** You can replace up to two octets in an IPv4 address with ranges (e.g., 10.52.100-255.15-255).
Multiple ranges	**10.52.100-255.15-255** **10.52.100-255.15-255.3** **1-2.3-4.5-6.7-8**
Comma-separated list	**10.52.1.10,10.52.1.50,10.100.1.20** Includes only these three hosts

If you enter IPv6 IP addresses, you must use the forms of notation described in the following table.

Notation	Examples
Single IP address	**2001:0DB8:0000:0056:0000:ABCD:EF12:3456** **2001:DB8:0:56:0:ABCD:EF12:3456** **2001:DB8::56:0:ABCD:EF12:3456** **2001:DB80:0:56::ABCD:EF12:3456** **2001:DB80:0:56::ABCD:239.18.52.86**
Global Routing Prefix subnet	**2001:DB8:0:56::/64**
Range of networks	**2001:DB8:0:56-58::/64**
Range of hosts	**2001:DB8:0:56:ABCD:EF12:3456:1-10** **2001:DB8:0:56:ABCD:EF12:3456:1-** **2001:DB8:0:56:ABCD:EF12:3456:10**
Multiple ranges	**2001:DB8:0:56-58:ABCD:EF12:3456:1-10** **2001:DB8:0:56-58:ABCD-ABCF:EF12:3456:1-10**

Host Group Membership

To see your host group structures, open the Host Group Membership Report. Generally, you can access this report by right-clicking any element in the Enterprise tree, then and selecting **Reports > Host Group Membership Report**.



Host Group Membership Report

Domain : Lancope

Host Group : Lancope Corporate

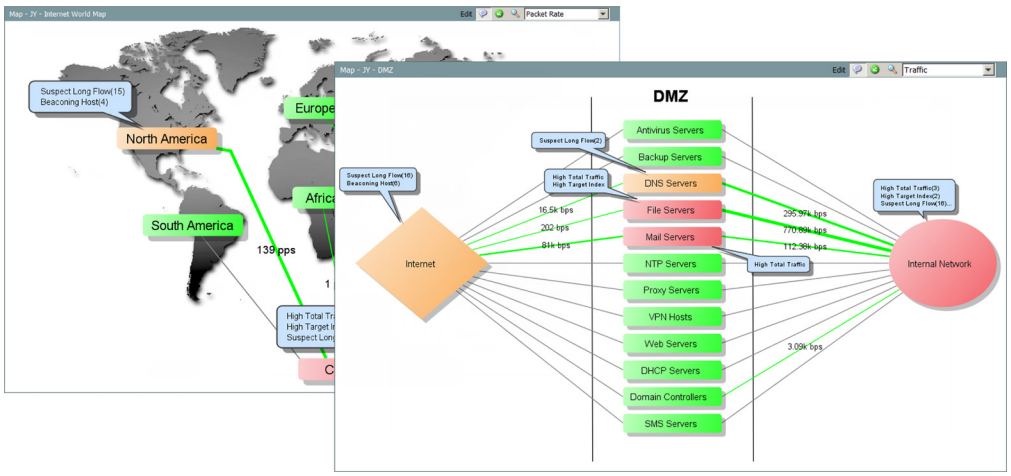
Host Group Membership Report - 56 records

Host Group	Defined in Path	Range	Size	Start IP Address	End IP Address
Lancope Corporate		.176.0/20	4,096	.176.0	.191.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> DMZ	.185.0/24	256	.185.0	.185.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.0.0/19	8,192	.0.0	.31.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.5.254	1	.5.254	.5.254
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.24.3	1	.24.3	.24.3
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.175.200	1	.175.200	.175.200
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.55.111	1	.55.111	.55.111
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.55.112	1	.55.112	.55.112
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.186.0/24	256	.186.0	.186.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.187.0/24	256	.187.0	.187.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.188.0/24	256	.188.0	.188.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.189.0/24	256	.189.0	.189.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.190.0/24	256	.190.0	.190.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.191.0/24	256	.191.0	.191.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Other Private Addresses	10.	16,777,216	10.0.0.0	10.255.255.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Other Private Addresses	.0.0/12	1,048,576	.0.0	.255.255

RELATIONAL FLOW MAPS

Relational flow maps give you a graphical view of the current state of traffic between host groups across your network, so you can see immediately where to focus your attention. Stealthwatch comes with several default maps, which administrators can customize as needed.

In addition, administrators can easily construct new relationship maps based on any criteria, such as location, function, or virtual environment, as shown in the following examples.



Maps help you answer key questions. By creating a relationship between two groups of hosts, you can analyze the traffic traveling between them. You can double-click a host group on the map to drill down and gain deeper insight into what is happening. When the relationship is created, you can right-click the relationship (the line between host groups), and then select **Relationship > Policy** to enable the baselining and alarming functionality between host groups.

4

VIEWS AND DASHBOARDS

OVERVIEW

By default, documents in the SMC show you information about every single activity that is occurring on your network. But, what if you care about only certain types of traffic or alarms? Or, what if you'd like to view only certain parts of a document rather than everything on that document? The SMC allows you to build your own dashboard, thereby permitting you to focus on the primary information you are interested in viewing.

This chapter includes the following topics:

- Default Dashboards in the SMC
- Host Group Dashboard
- Building Your Own Dashboards

DEFAULT DASHBOARDS IN THE SMC

The SMC console contains a number of default dashboards so that you can easily view different types of information in one document. To access these dashboards, from the Main Menu, select **Status > Dashboards > [default dashboard name]**.

Following is the list of default dashboards (in alphabetical order) in the SMC console and a description of each one:

Dashboard Name	Description
Alarm Dashboard	This dashboard displays alarm data for the selected domain. Data is displayed in the following sections: ▸ New Alarms ▸ Acknowledged Alarms
Cyber Threats Dashboard	This dashboard provides graphical and tabular data about cyber threats affecting the domain. Data is displayed on the following tabs: ▸ Reputation ▸ Reconnaissance ▸ Data Loss ▸ Malware ▸ Botnet
Data Loss Dashboard	This dashboard provides a display of data transfer activity in the selected domain. Data is displayed in the following sections: ▸ Data Loss Alarms (Today) ▸ Host Information for Active Data Loss Alarms ▸ Trend of Data Loss Alarms ▸ Top 20 Uploads (Today)
DDoS Alarm Dashboard	This dashboard provides the following information: ▸ Activity that might indicate a DDoS threat or a DDoS attack as it is starting to occur ▸ Detailed information about alarms that have occurred on your network
DDoS Traffic Dashboard	This dashboard provides information about spikes and changes in traffic patterns on your network that may indicate a DDoS attack.

Dashboard Name	Description
Flow Collector Dashboard	This dashboard provides a graphical display of the most important activity on the Stealthwatch Flow Collector. Data is displayed in the following sections: ▶ Status Tab • Flow Collection Statistics • Flow Collection Trend • Flow Collection Status ▶ Alarms Tab • Flow Collector Alarm Trend, Previous 30 Days • Flow Collector Alarms, Previous 30 Days
Host Group Dashboard	For information about the Host Group dashboard, refer to “Host Group Dashboard” on page 99.
Interface Summary Dashboard	This dashboard provides a variety of graphical and tabular data of the traffic for a selected interface. Data is displayed in the following sections: ▶ Traffic Statistics, Last 6 Hours ▶ Utilization Inbound and Outbound, Last 6 Hours ▶ Application Traffic Inbound and Outbound, Last 6 Hours ▶ Top Active Conversations, Inbound ▶ Top Active Conversations, Outbound
Interface Traffic Dashboard	This dashboard provides a variety of graphical and tabular data of the traffic for a selected interface. Data is displayed in the following sections: ▶ Interface Service Traffic ▶ Interface Application Traffic ▶ Interface Statistics ▶ Interface Utilization ▶ DSCP Traffic
Security Overview	This dashboard provides graphical and tabular data related to the security of your system. Data is displayed in the following sections: ▶ Inside Concern Hosts ▶ Outside Concern Hosts ▶ Top Alarming Hosts ▶ Alarms Currently Active Summarized by Type

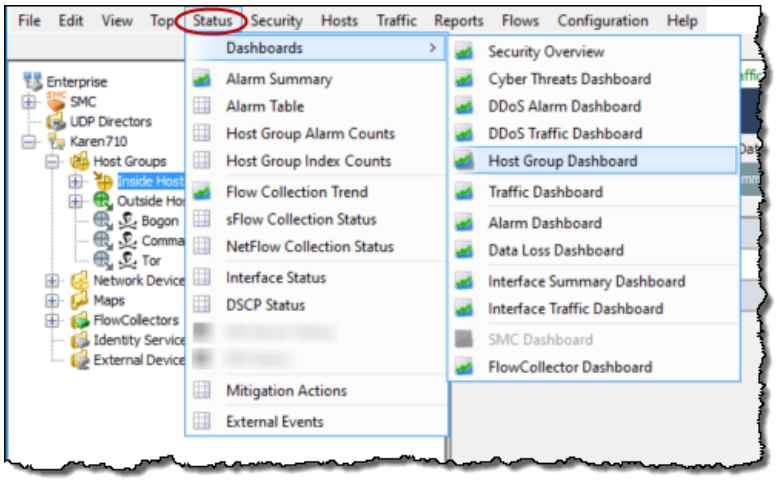
Dashboard Name	Description
SMC Dashboard	This dashboard provides a graphical display of the SMC console's most important activity. Data is displayed in the following sections: ▸ SMC Performance ▸ SMC Alarms ▸ SMC Event Processed
Traffic Dashboard	This dashboard provides a graphical display of traffic statistics for the selected domain. Data is displayed in the following sections: ▸ Protocols, Packets from Inside and Outside Hosts ▸ TCP Flags, Packets from Inside and Outside Hosts ▸ Active Flows Initiated by Inside and Outside Hosts ▸ Inside and Outside Active Hosts

Note:

For more information about these dashboards, refer to the *Stealthwatch Desktop Client Online Help*.

HOST GROUP DASHBOARD

The Host Group Dashboard provides graphical and tabular data of important network, security, and alarm activity for the selected host group. This data is collected from the SMC every five minutes. To display this document, first click the host in the Enterprise tree for which you want to view data, and then from the SMC Main Menu select **Status > Dashboards > Host Group Dashboard**.

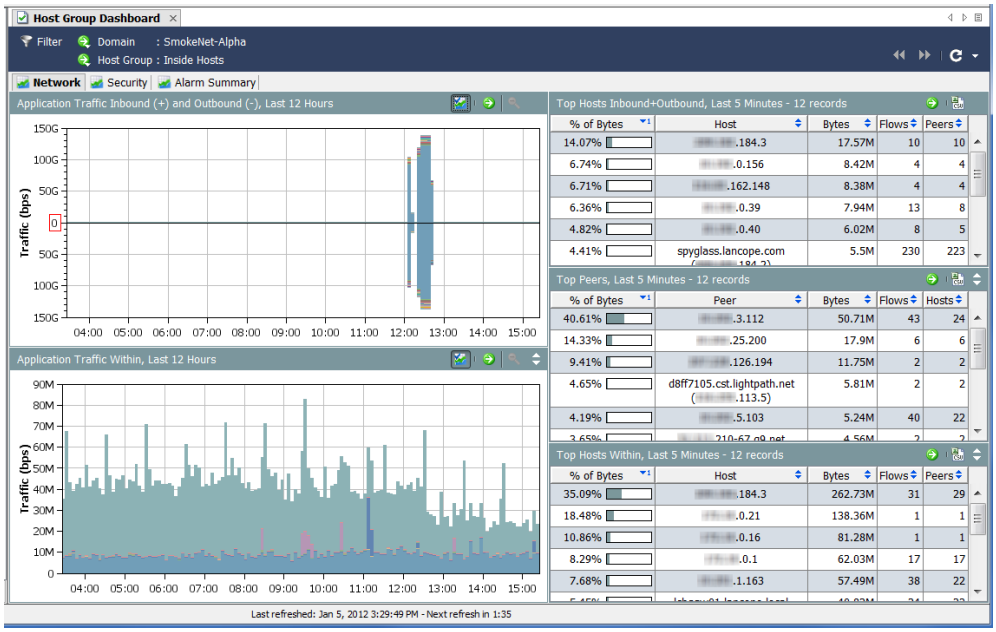


Go to the corresponding section in the remainder of this chapter for information on how to view the following pages within the Host Group Dashboard:

- Network page
- Security page
- Alarm Summary page

Host Group Dashboard - Network Page

The Host Group Dashboard: Network page provides graphical and tabular data of important network-related activity for the selected host group. To view this dashboard, click the **Network** tab.

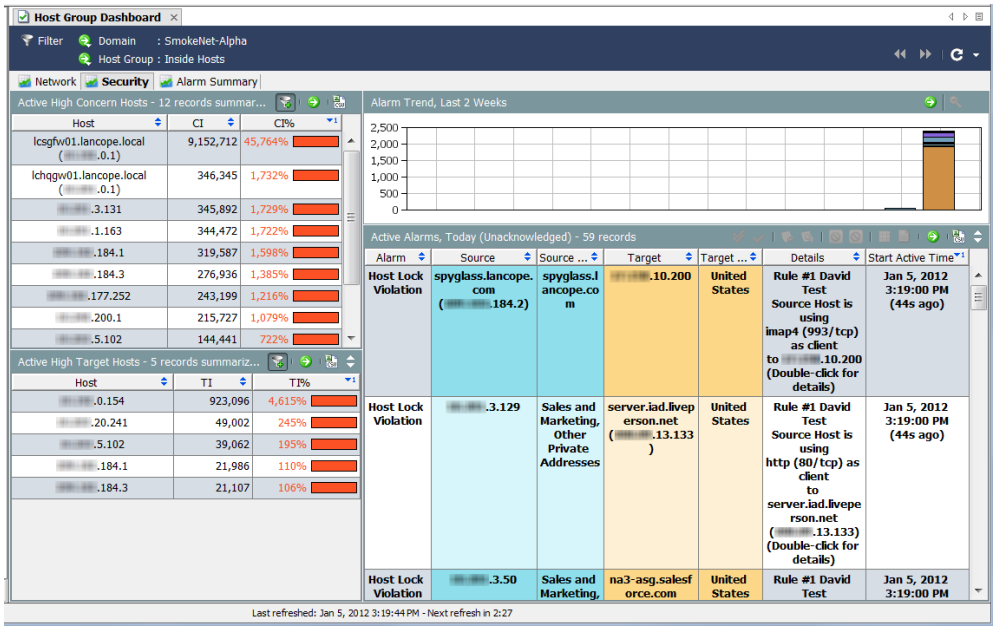


As you look at the Network page, ask yourself the following questions:

- Do the Application graphs show a large amount of traffic for applications not normally used within your organization?
- Do the Application graphs show a large amount of traffic for applications not normally used at certain times of the day (such as after normal office hours)?
- Do the Application graphs show a significant amount of traffic for the Undefined or Others applications? If so, you should configure more application definitions.
- Do the Top Active Hosts tables include hosts that should not normally be in the list of top active hosts?
- Do the Top Active Hosts tables show that a small number of hosts are accounting for extremely large percentages of traffic?

Host Group Dashboard - Security Page

The Host Group Dashboard: Security page is the first dashboard to appear. This document provides graphical and tabular data of important security-related activity for the selected host group.



Note:

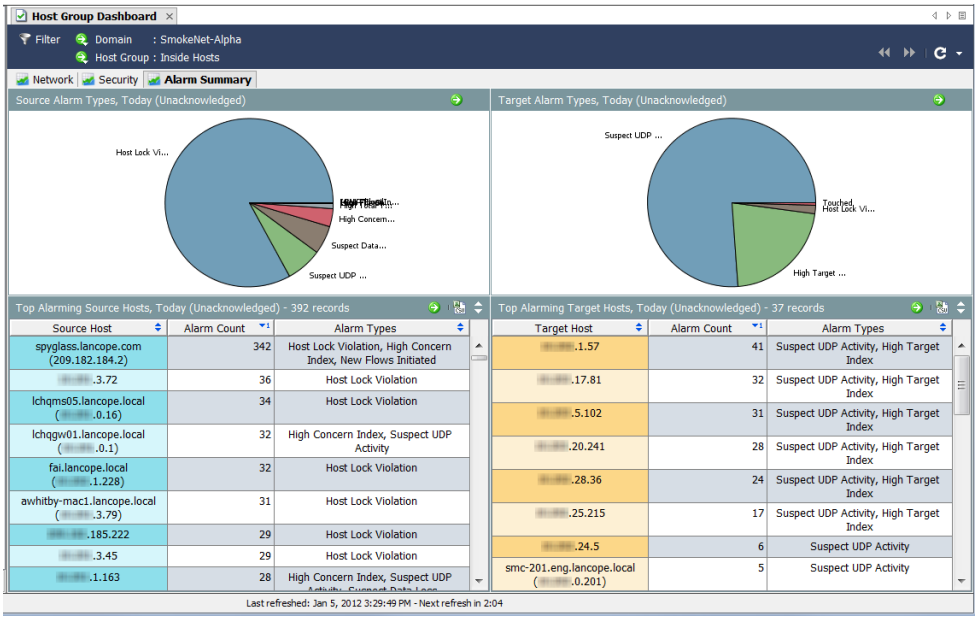
You can click the **Go to Document** button on each document header to open each component as a separate document.

As you look at the Security page, ask yourself the following questions:

- Does the High CI Hosts table show a high concern index for hosts that are important to your organization?
- Does the Alarm Report by Host Group table show high concern index alarms for sensitive host groups?
- Does the Alarm Report by Host Group table show a spike in high concern index alarms on any particular day?
- Does the Top Alarming Hosts table show a large number of alarms for hosts that are important to your organization?
- Does the Top Alarming Hosts table show types of alarms about which you are particularly concerned?
- Does the Top Scans table show a large number of TCP/UDP address scans for source hosts or target hosts that are important to your organization?

Host Group Dashboard - Alarm Summary Page

The Host Group Dashboard: Alarm Summary page provides a graphical summary as well as detailed table data of alarm activity for the selected host group. To view this dashboard, click the **Alarm Summary** tab.



As you look at the Alarms page, ask yourself the following questions:

- Do the tables show a large number of alarms for hosts or host groups that are important to your organization?
- Do the tables show types of alarms about which you are particularly concerned?

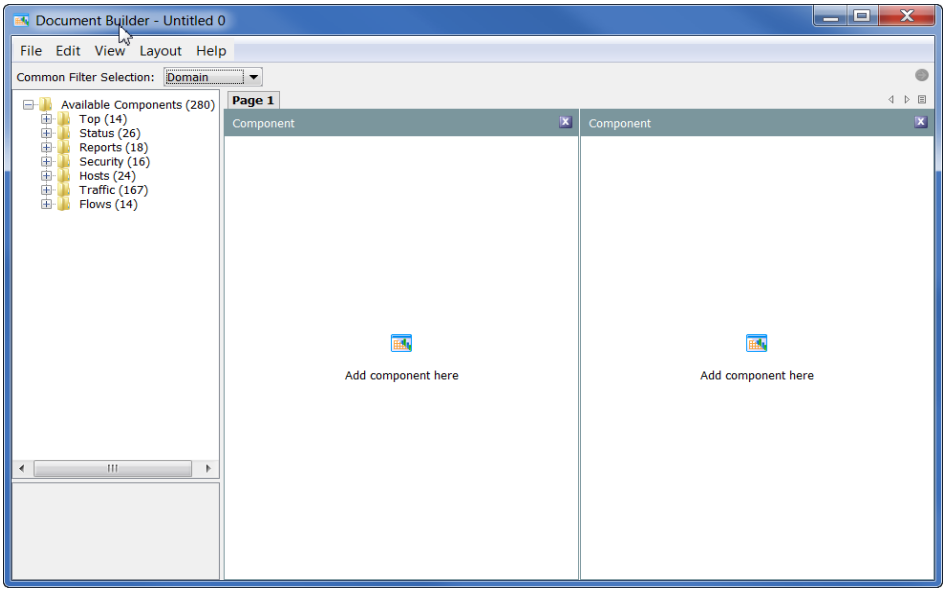
BUILDING YOUR OWN DASHBOARDS

The Document Builder allows you to create custom dashboards (a dashboard is a collection of different reports) that contain any SMC component you want with the data you want to see. You can even rename these components with text that makes more sense to you.

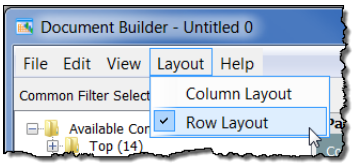
For purposes of illustration, we're going to build a Security Report dashboard that focuses solely on security alarms. Our example will have multiple tabs, each with multiple components. However, you can use these same principles to build any type of dashboard you need.

To build a custom dashboard of your own, complete the following steps:

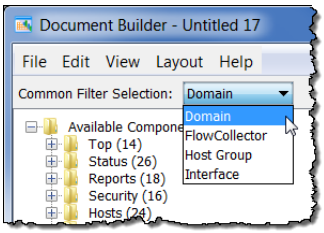
1. From the SMC Main Menu select **View > Document Builder**. The Document Builder dialog opens.



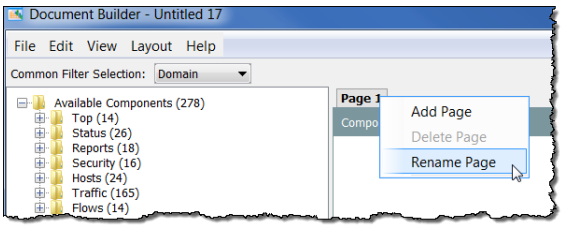
2. If you want your document to have a row format rather than a column format (default), from the Document Builder Main Menu, select **Layout > Row Layout**.

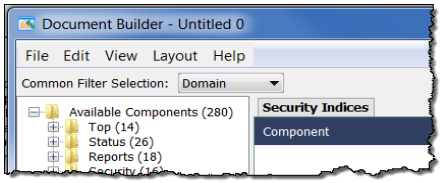


3. Click the arrow in the Common Filter Selection drop-down list and click the option by which you want this document to be filtered by default. In the example to the right, the document will be filtered by Domain.



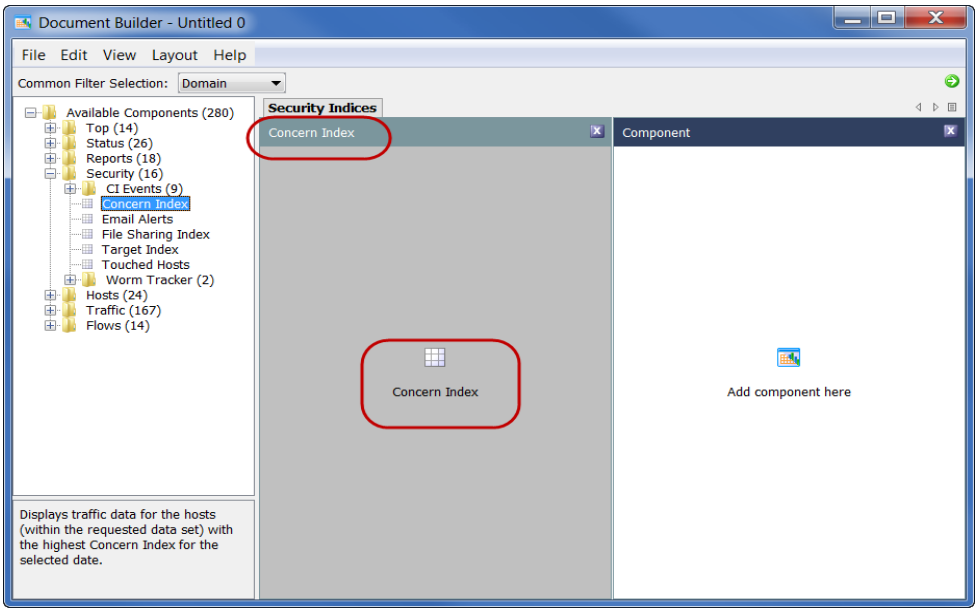
4. If you want to rename a page, right-click that page's tab and select **Rename Page**. (You also can double-click the tab to type the new page name directly on the tab.)





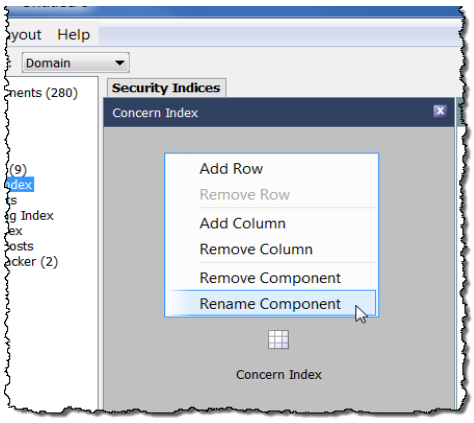
In the example to the left, we have changed the name on the page tab from *Page 1* to *Security Indices*.

5. Click the component you want to add from the left tree menu and drag it to the area on the page where you want it to be. In the following example, we dragged the Concern Index component to the left-hand column.

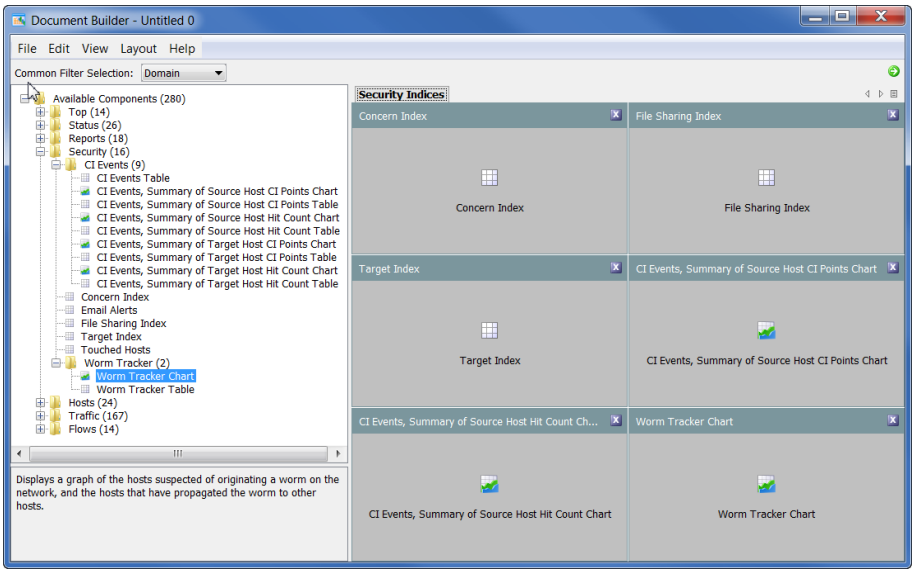


Note how the name of the component has changed from *Component* to *Concern Index*, which is the name of the component we just added. Note also that the name of the icon in the middle of that column has also changed to the name of the component we just added.

6. If you want to rename the component, right-click in the body of the component and select **Rename Component**.



7. Continue to add components to this page until you are finished. The default page shows only two areas for components. However, it will adjust accordingly if you add more than two. In the following example, there are six components. Each time we added a new component to a column, it displayed below the last entry in that column. If necessary, you can change the layout at any time.

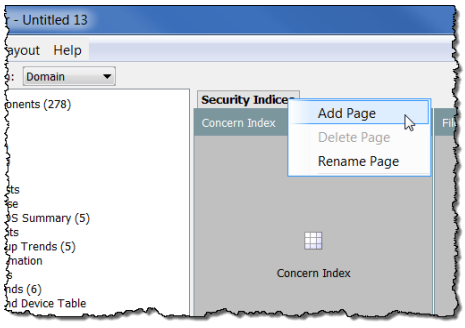


Notes:

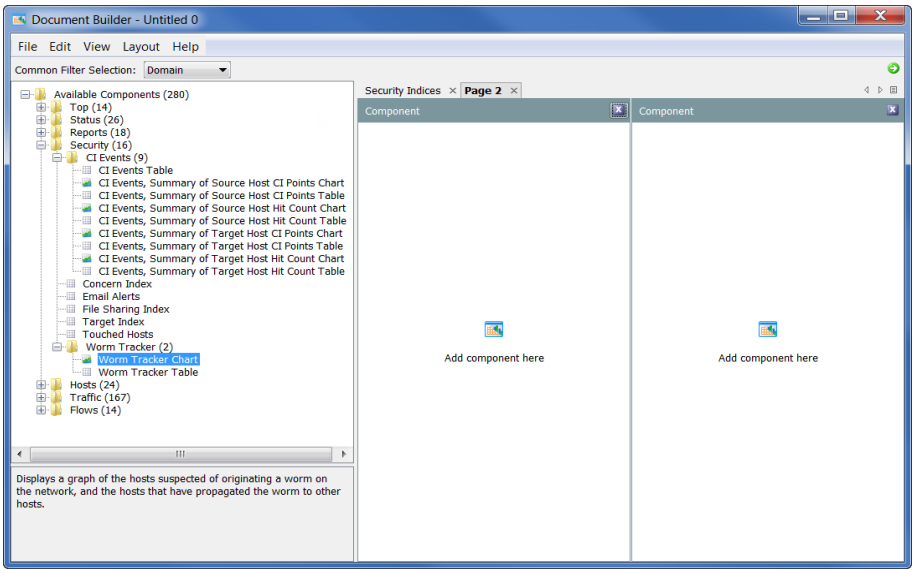
Click the button once to empty a component area.

Click the button twice to delete a component area completely.

8. If you want to add another page (tab) to your document, right-click the existing tab and select **Add Page**.



The new blank page opens.



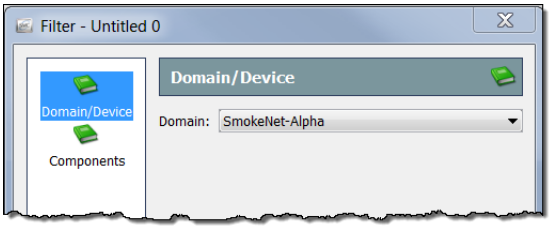
9. Drag components to where you want them on this page, just as you did for the first page.

10. When you are finished composing your document, click **File > Save As** to save it as an XML template on your hard drive.

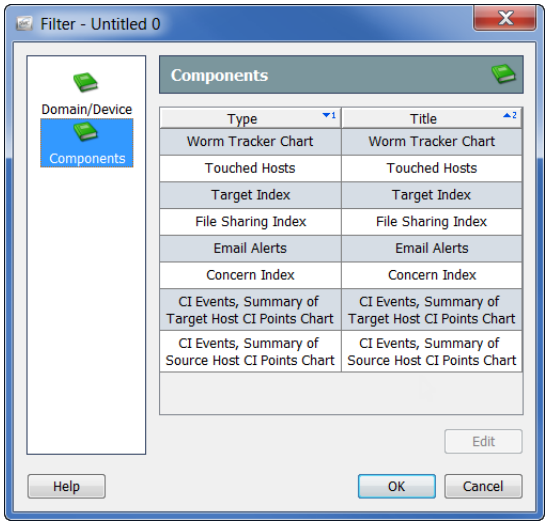
Note:

The file name will be your document name. For example, if you save the file name as *1234*, your document title will be *1234*. Therefore, be sure to give your document a meaningful file name (e.g., *Security Reports*).

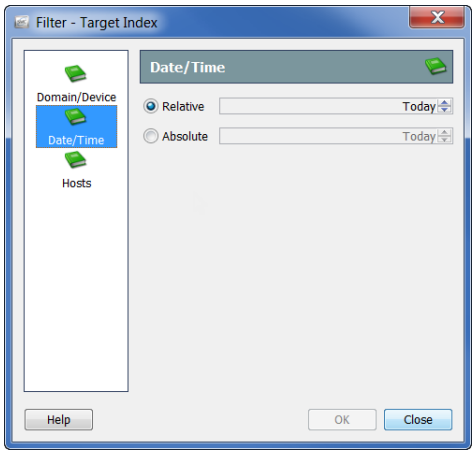
11. Launch your document in the Stealthwatch Desktop Client by clicking the **Go to Document** button in the upper right corner of the Document Builder dialog. The Filter dialog for the document opens. Click the **Domain/Device** button if it is not already highlighted. Ensure that the domain you want to filter on is selected.



12. Click the **Components** button. All the components contained in your document are listed.

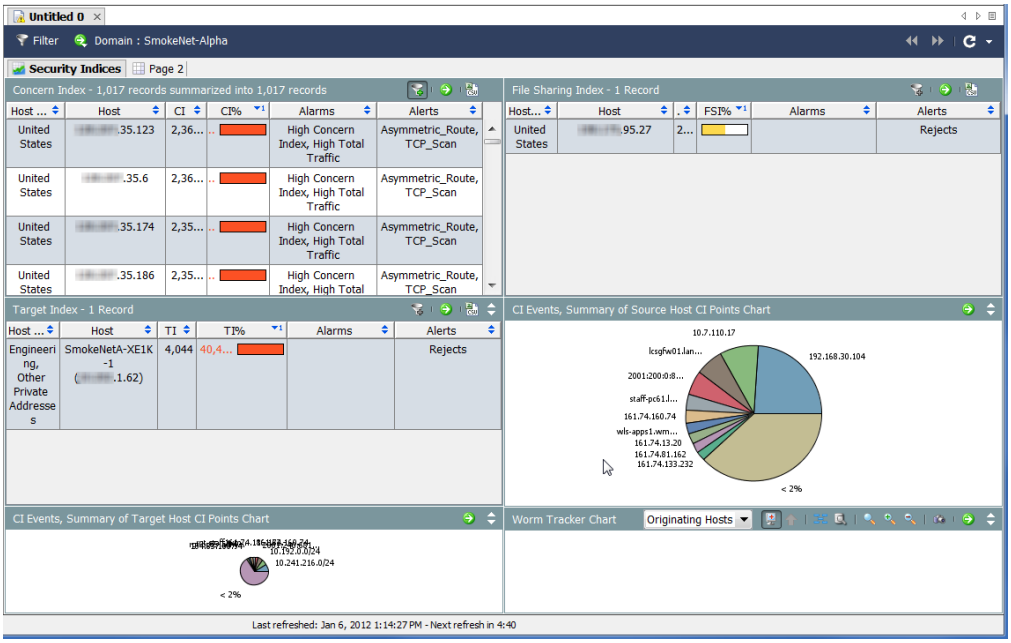


13. Click a component you want to filter on and click **Edit**. The Filter dialog for that component opens. (The options you are able to filter on will depend on which button you click on the left side of the dialog).



14. After you make your selections, click **OK**.

15. When your new document opens in the SMC GUI, it will look similar to the following example. Resize the columns and components as desired.



16. When finished, from the SMC Main Menu select **File > Save As** to save your document to the SMC server, enabling you to open it at will in the SMC.

Note:

The file name will be your document name. For example, if you save the file name as *1234*, your document title will be *1234*. Therefore, be sure to give your document a meaningful file name (e.g., *Security Reports*).

17. Close the Document Builder.

Note:

You can open previously saved XML and DAR files in the Document Builder to edit them whenever necessary.

5

INDEXES: RANKING BEHAVIOR CHANGES

OVERVIEW

Stealthwatch uses indexes to help detect host anomalies on the network. Using proprietary heuristics and algorithms to establish a baseline of normal behavior for your environment, the Stealthwatch Flow Collector adds Concern Index (CI) points to hosts for various unacceptable host behaviors. When the accumulated index points surpass the acceptable threshold, the Flow Collector raises an alarm.

Indexes help to indicate how anomalous a behavior is, as well as how confident Stealthwatch is that the anomalous activity is relevant. In other words, indexes help you prioritize your investigation.

For example, if a stranger rattles your front door and then says he has the wrong address, you might think that you have no reason to call the police. Your index of concern would be relatively low. However, if the stranger continues down the street doing the same thing at your neighbors' doors, his behavior becomes increasingly suspicious.

Your index of concern most likely would go up a point (or more) for every door you see the stranger approach. By the time he approaches the third door, you become concerned enough to call the police. In this case, the threshold for you to not worry about this behavior is two doors. At the third door, that threshold is surpassed and you are compelled to do something about it.

Stealthwatch indexes work in much the same way to protect your network, raising an alarm only when anomalous activity reaches an unacceptable level. Basically, anything red on these indexes means that a significant behavior change has occurred.

For example, a single TCP reset will not cause an alarm, even though Stealthwatch assigns it a CI point. However, numerous TCP resets might cause an alarm, based on the level defined as acceptable on your system.

Stealthwatch uses the following indexes to track anomalous behavior:

- Concern Index (CI) – Tracks hosts that appear to be performing activities that could compromise network integrity.
- Target Index (TI) – Tracks hosts that appear to be victims of the suspicious behavior of other hosts.
- File Sharing Index (FSI) – Tracks behavior that is indicative of peer-to-peer (P2P) activity.

This chapter includes the following topics:

- Concern Index
- Target Index
- File Sharing Index

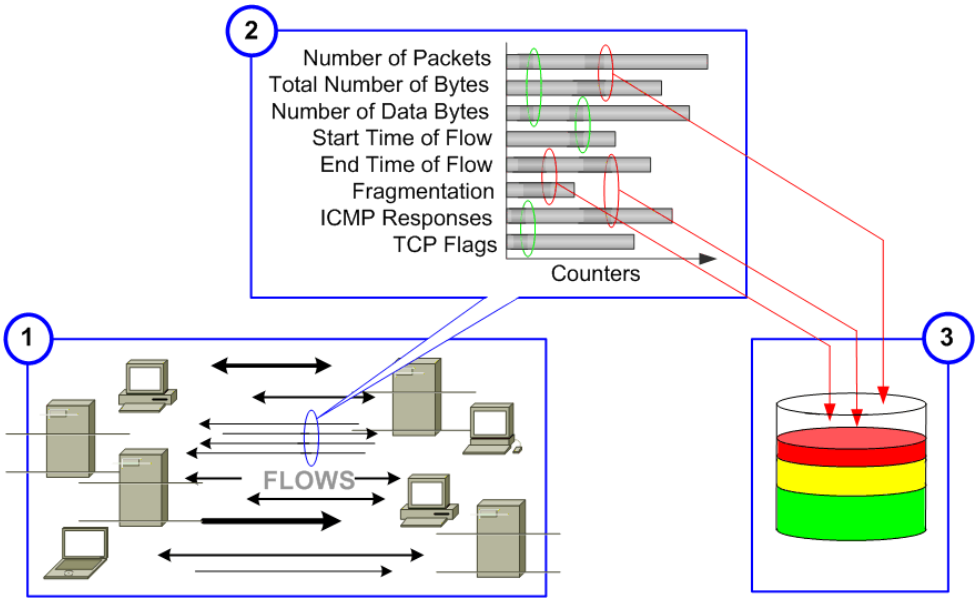
CONCERN INDEX

The Concern Index (CI) is the primary means by which Stealthwatch notifies you of suspicious flow activity, such as a packet being sent intentionally to evoke a response from a network host during denial-of-service (DoS) or scanning activity. Stealthwatch labels these occurrences as Security Events.

A Security Event could indicate a security breach, a misconfigured device, a malfunctioning server, or another source of networking issues. Stealthwatch keeps track of the information associated with these events and increases the number of CI points for that host. The greater the CI, the greater the level of concern over that behavior.

When the number of points exceeds the set threshold, Stealthwatch raises a High CI alarm against the host that is the source of the activity. CI values can range from zero points to hundreds of thousands of points.

The following diagram illustrates the three basic stages involved in incrementing the CI:



1. The Stealthwatch Flow Collector observes the flows in which the host is involved.
2. The Flow Collector compares the activity to what has been configured as acceptable behavior.
3. The Flow Collector finds that some of the host's activities are not acceptable, and then increases the CI.

An inside host with a High Concern Index alarm usually indicates that the host is exhibiting abnormal behavior and should be examined for possible compromise, misuse, or policy violations.

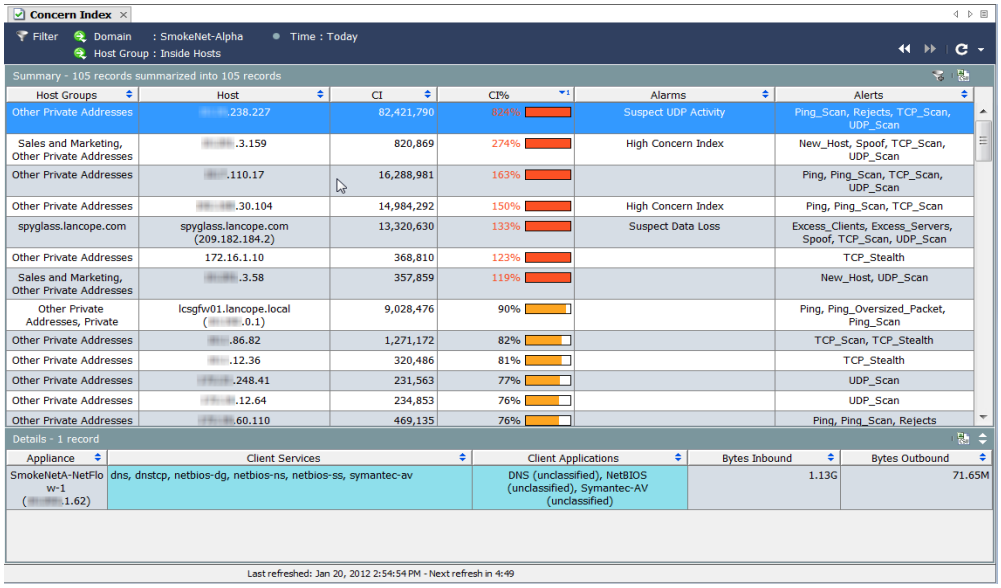
An outside host with a High Concern Index alarm is often doing “bad things” in an attempt to violate your network integrity. In either case, the Concern Index document can help you identify which hosts are attacking your network, as well as which hosts are being attacked.

Note:

If a host’s activity surpasses its CI threshold, and the High Concern Index alarm for the associated host group is suppressed, then the Flow Collector will not raise a High Concern Index alarm against that host.

The Stealthwatch Flow Collector clears all index counts every 24 hours at the user-defined *archive hour*. At that time, the Flow Collector saves the log files and Web files it has gathered during the preceding 24 hours, and then begins another day of data collection.

The Concern Index document displays information for hosts that have had the highest number of CI points since the last archive hour.



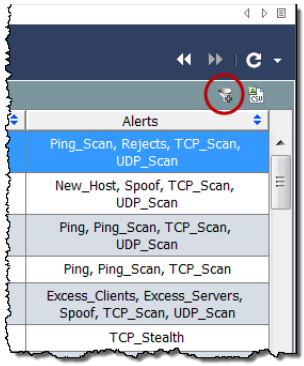
To display the Concern Index document, right-click a domain or host group and select **Security > Concern Index**.

The Concern Index document helps you prioritize threats and focus on the events that really matter. Instead of seeing thousands of daily alerts, Stealthwatch provides you with a handful of actionable items in order of severity from highest to lowest.

Note:

An alert is an informational summary of unusual network activity; however, unlike alarms, alerts are not sent as notifications.

By default, the Concern Index Filter button (located in the upper right corner of the document) is activated, and the Concern Index shows only those hosts that have active Concern Index alarms (i.e., that have a CI percent above 100). To see hosts that have a CI percent greater than 50, click the **Concern Index Filter** button. The plus sign on the Concern Index Filter button turns gray , and hosts that have a CI percent greater than 50 are displayed, regardless if there is an active High Concern Index alarm or not.



Note:
The accumulated CI for a host is cleared at the archive hour.

Notice that the Concern Index has a Summary section at the top and a Details section at the bottom. Select a row in the Summary section to see further information about that row in the Details section.

In the preceding example, the host with the highest threat level is xxx.xxx.238.227. For purposes of this example, we will assume that this is an inside host. We can easily see the following information about this host:

- Since the last archive hour, this host has accumulated a CI percent of approximately 824 percent.
- This host has also caused two alerts: Ping_Scan, Rejects, TCP_Scan, and UDP_Scan**.**
- It has received 1.13G of data.
- It has sent 71.65M of data.

With the combination of CI percent, alarm, alert, and data transfer, this looks like a possible security breach. This host should be examined for possible compromise, misuse, or policy violations.

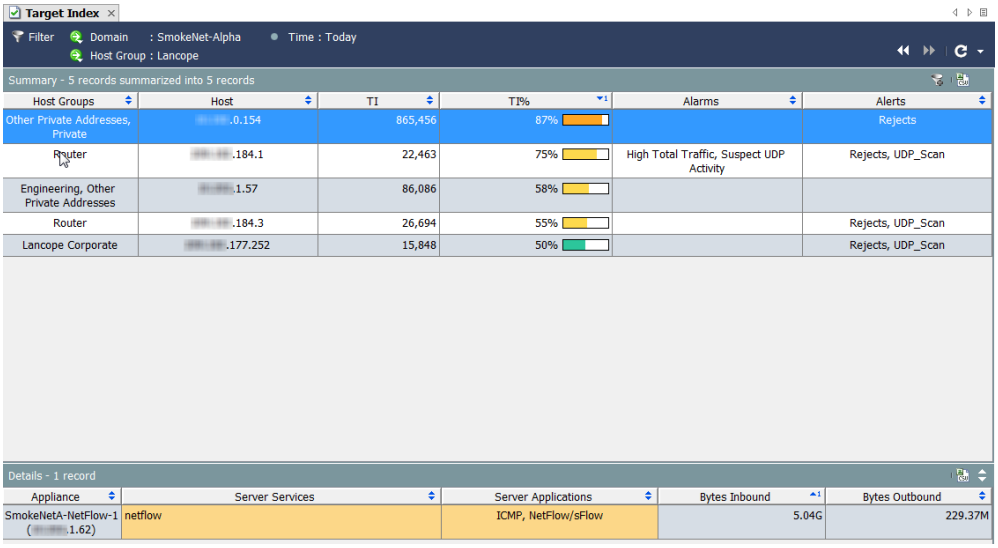
Double-click the host IP address to open the Host Snapshot for the host that is the source of the Security Event.

Note:
For descriptions of the various columns that can be viewed in the Concern Index document, refer to the *Stealthwatch Desktop Client Online Help*.

TARGET INDEX

The Target Index (TI) displays hosts (within the requested data set) that have had the highest target index since the last Stealthwatch Flow Collector archive hour. The Stealthwatch Flow Collector triggers the High Target Index alarm when a target IP address has ***received*** a number of Security Events or other malicious attacks and has exceeded the threshold. The purpose of the target index is to alert you to possible distributed attacks by many hosts directed at a single inside host.

Once you have identified compromised hosts and the associated services and ports, you can block banned ports at your firewall and perhaps at the host itself, depending on your equipment and software. You can also disconnect the host from the network and scrub it.

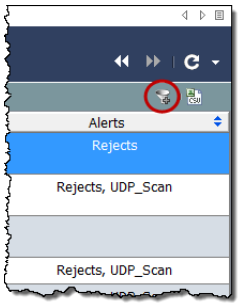


To display the Target Index, right-click a domain or host group and select **Security > Target Index**.

Target index values can range from zero points to hundreds of thousands of points. As target index points accumulate for each host, a TI alarm can result. By default, the data is sorted by TI percent in descending order. The data represents the greatest data values that have been observed in the domain since the last archive hour. For example, a host with a TI percent of 158 has exceeded its TI threshold by 58 percent and may deserve more investigation. The percentage is followed by a graphic that changes color when the TI threshold is approached, as described in the following table.

Percentage of Configured Threshold	Text Color
0% of configured threshold	Empty graphic
0% to 50% of configured threshold	Green
51% to 75% of configured threshold	Yellow
76% to 99% of configured threshold	Orange
100% of configured threshold or greater	Red

By default, the Target Index Filter button (located in the upper right corner of the document) is activated, and the Target Index shows only those hosts that have active Target Index alarms (i.e., that have a TI percent above 100). To see hosts that have a TI percent greater than 50, click the **Target Index Filter** button. The plus sign on the Target Index Filter button turns gray, and hosts that have a TI percent greater than 50 are displayed.

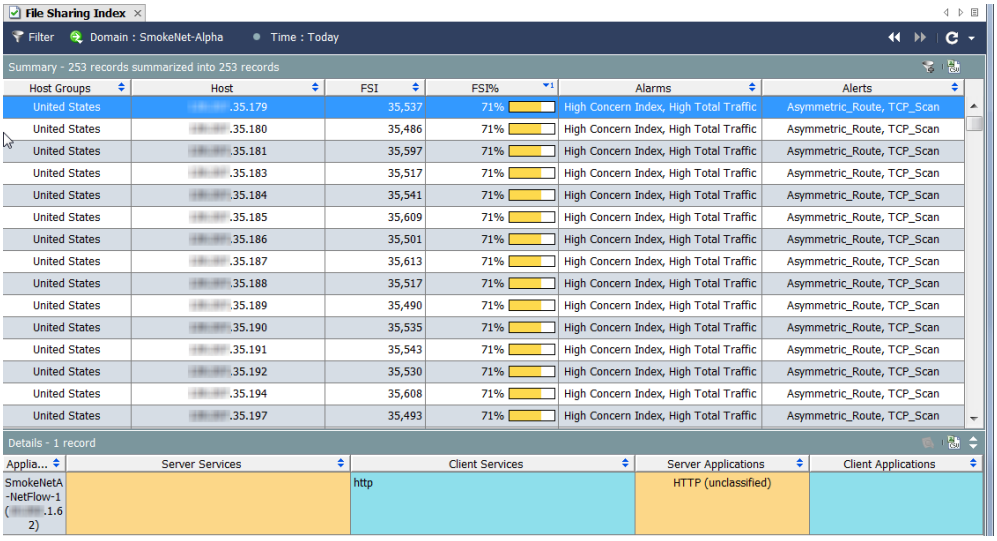


FILE SHARING INDEX

The goal of the File Sharing Index (FSI) is to detect suspected file-sharing applications, and specifically Peer-to-Peer (P2P) communications, that place organizations at risk. This could occur via possible transmission of sensitive information or abuse of the organization's network by sharing copyrighted material with others inside or outside of the network.

The Stealthwatch Flow Collector collects a variety of information on connections made by all hosts on the network. By correlating certain statistics, a File Sharing Index is derived that identifies the hosts that appear to be involved with file transfers that may be indicative of P2P activity.

Using correlation techniques, the index displays the hosts that are most active and/or have tripped the sensor combinations that are most commonly associated with file sharing activity by adding points. This technique is similar to the one that determines the Concern Index value that the Stealthwatch Flow Collector uses to indicate scanning activity. The File Sharing Index document provides you with a prioritized list of hosts for investigation and an optional host-level alarm.



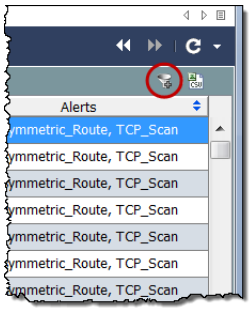
To display the File Sharing Index, right-click a domain or host group, and then select **Security > File Sharing Index**.

File sharing index values can range from zero points to hundreds of thousands of points. As file sharing index points accumulate for each host, an File Sharing Index alarm can result. By default, the data is sorted by FSI percent in descending order. The data represents the greatest data values that have been observed in the domain since the last archive hour. For example, a host with an FSI percent of 158 has exceeded its FSI threshold by 58 percent and may deserve more investigation.

The percentage is followed by a graphic that changes color when the FSI threshold is approached, as described in the following table.

Percentage of Configured Threshold	Text Color
0% of configured threshold	Empty graphic
0% to 50% of configured threshold	Green
51% to 75% of configured threshold	Yellow
76% to 99% of configured threshold	Orange
100% of configured threshold or greater	Red

By default, the File Sharing Index Filter button (located in the upper right corner of the document) is activated, and the File Sharing Index shows only those hosts that have active File Sharing Index alarms (i.e., that have a FSI percent above 100). To see hosts that have a FSI percent greater than 50, click the **File Sharing Index Filter** button. The plus sign on the File Sharing Index Filter button turns gray , and hosts that have a FSI percent greater than 50 are displayed.



6

MONITORING TRAFFIC AND NETWORK PERFORMANCE

OVERVIEW

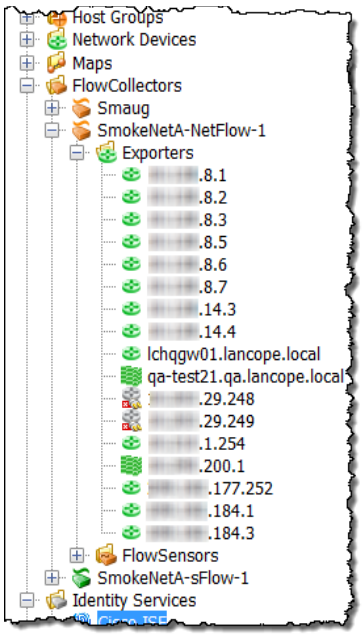
Stealthwatch uses network behavior analysis to monitor your network and let you know when changes occur that could indicate potential problems. The system continually observes every host on your network, recording behavior such as when the host is more or less active, how much data is being transmitted between hosts, and the kind of traffic involved.

This chapter describes how to access graphical and tabular data that represents traffic on your network so that you can see changes in host and network behavior. So, if any potential threats do exist, you can resolve them before they can inflict harm to your network.

This chapter includes the following topics:

- Monitoring Traffic
- Exporters/Network devices
- Network Performance

MONITORING TRAFFIC

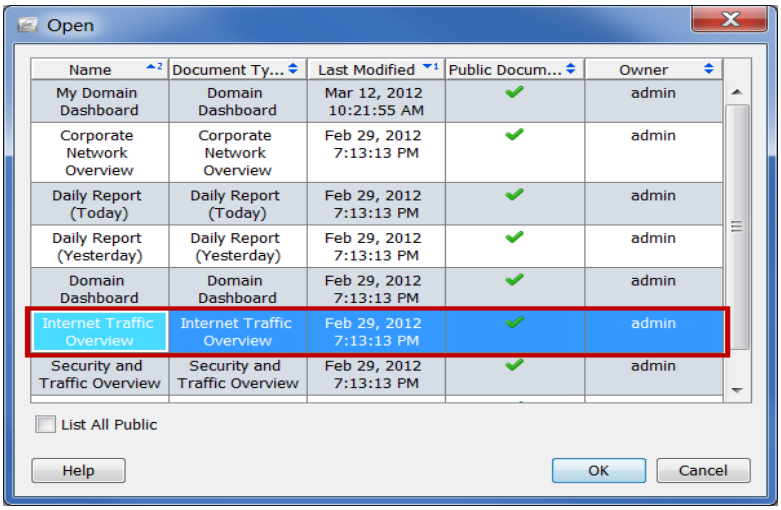


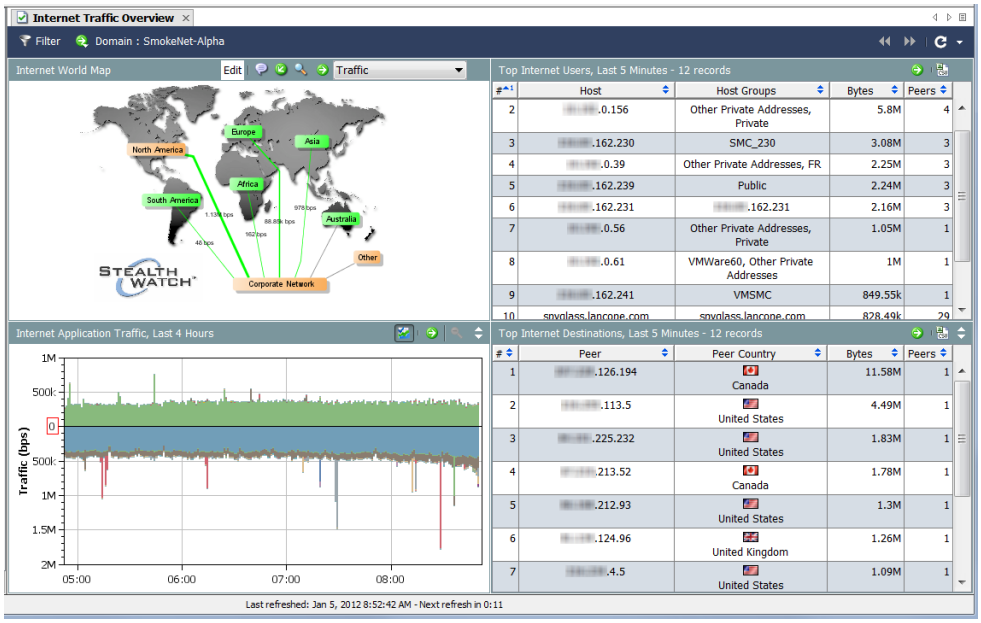
The Enterprise tree is in the frame located on the left side of the SMC graphical user interface. This frame uses a tree menu to provide you with a fast and easy way to see the status of your system and to request documents.

The main area of interest for monitoring traffic is exporters, which are routers or switches that are configured to send data to a Stealthwatch Flow Collectors.

Internet Traffic Overview

The Internet Traffic Overview provides graphical and tabular data of domain traffic associated with the Internet. To display this document, select **File > Open** from the Main Menu. The following dialog opens. Select the Internet Traffic Overview document and click **OK**.





As you look at the Internet World Map, ask yourself the following questions:

- Do any of the host groups or host group relationships show critical or major alarms? The colors and callouts help you to make this determination.

  If so, get more information by right-clicking the alarming host group or host group relationship, and then selecting **Alarm Table**.

- Click the arrow in the drop-down list in the document header to change the data type that appears. Do any of the host group relationships show unusual amounts of data? The thickness of the lines and the status text for the lines help you to make this determination.

  If so, get more information by right-clicking the host group relationship, and then selecting **Host Group Relationship Dashboard**.

As you look at the Internet Application Traffic, ask yourself the following questions:

- Does the graph show unusual spikes for applications being used in your organization?

Tip:

You can click the **Hide Others** button to hide traffic for applications that are not among the top number used. This button toggles to hide or show the data.

- Does the graph show a significant amount of traffic for applications that are not normally used in your organization?
- Does the graph show a significant amount of traffic for the Undefined or Others applications?

If so, you should configure more application definitions.

As you look at the Top Internet Users, ask yourself the following questions:

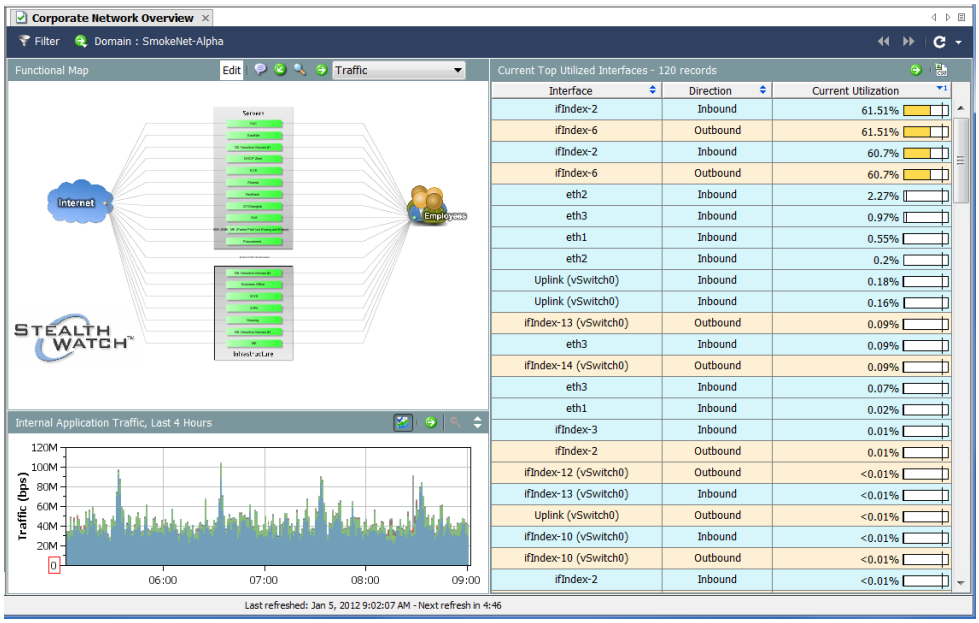
- Does the table show a significant amount of traffic for hosts that should not be among the top internet users in your organization?
- Does the table show hosts in your organization that are acting as servers and are sending a significant amount of traffic?
- Does the table show the hosts in your organization that are sending/ receiving traffic to or from a large number of peers?

As you look at the Top Internet Destinations, ask yourself the following questions:

- Does the table show a significant amount of traffic for peers that should not be communicating with your organization?
- Does the table show peers that are acting as clients and are receiving a significant amount of traffic from hosts in your organization?
- Does the table show peers that are sending/receiving traffic to or from a large number of hosts in your organization?

Corporate Network Overview

The Corporate Network Overview provides graphical and tabular data of domain traffic associated with your overall corporate network. To display this document, select **File > Open** from the Main Menu. The Open dialog opens. Select the Corporate Network Overview document and click **OK**.



As you look at the Functional Map, ask yourself the following questions:

- Do any of the host groups or host group relationships show critical or major alarms? The colors and callouts help you to make this determination.

  If so, get more information by right-clicking the alarming host group or host group relationship, and then selecting **Alarm Table**.

- Click the arrow in the drop-down list in the document header to change the data type that appears. Do any of the host group relationships show unusual amounts of data? The thickness of the lines and the status text for the lines help you to make this determination.

  If so, get more information by right-clicking the host group relationship, and then selecting **Host Group Dashboard**.

As you look at the Internal Application Traffic, ask yourself the following questions:

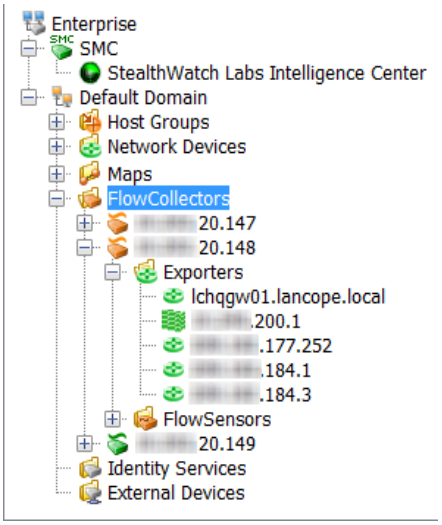
- Does the graph show unusual spikes for applications being used in your organization?
- Does the graph show a significant amount of traffic for applications that are not normally used in your organization?
- Does the graph show a significant amount of traffic for the Undefined or Others applications? If so, you should configure more application definitions.

As you look at the Current Top Utilized Interfaces, ask yourself the following questions:

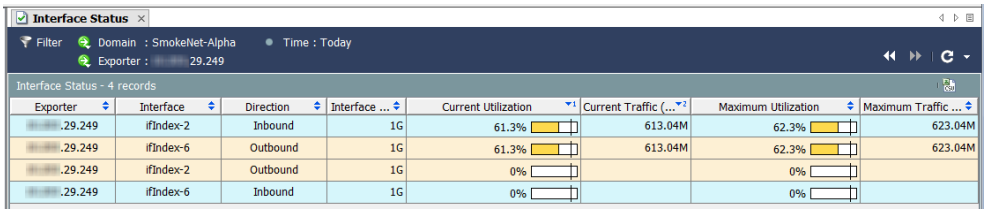
- Does the table show any interfaces that are saturated (i.e., are indicating unusually high percentages of utilization)?
- Does the table show any interfaces that should not be included among the top users?

EXPORTERS/NETWORK DEVICES

Exporters exist in the tree below the Stealthwatch Flow Collectors that receive their data, as shown in the example to the right.



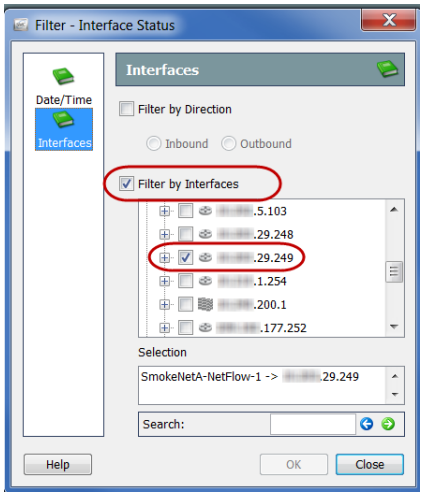
To navigate directly to a document for an exporter, expand the Network Devices option under the appropriate host in the Enterprise tree, and then double-click the exporter. The Interface Status document opens. This document displays statistics for the interfaces on routers or switches (i.e., exporters) that are sending data to a Stealthwatch Flow Collector for sFlow or a Stealthwatch Flow Collector for NetFlow.



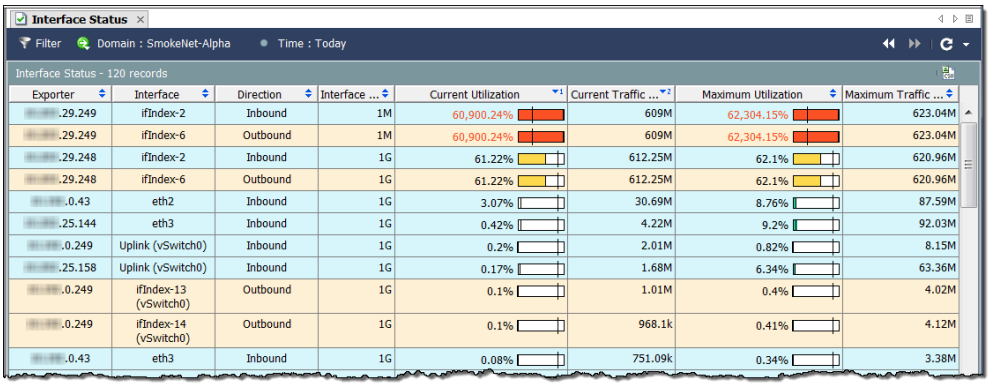
Note:

The Interface Status document is not available for the Cisco ASA exporter type.

Click the **Filter** button in the upper left corner of the Interface Status document. In the Filter - Interface Status dialog that opens, click the **Interfaces** button if it is not already highlighted.

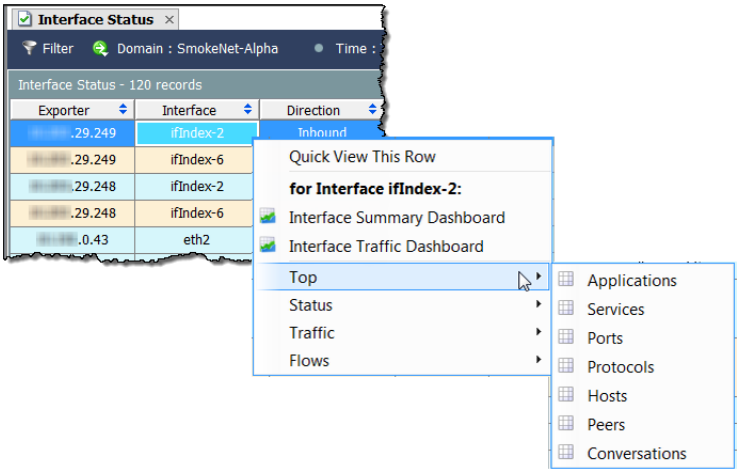


Click the **Filter by Interfaces** check box to remove the checkmark. Next, find the exporter by which the document is currently filtered (it will be the only one with a check). Click this exporter's check box to remove the checkmark, and then click **OK**. The Interface Status document now shows traffic statistics for the entire domain, as shown in the following example.

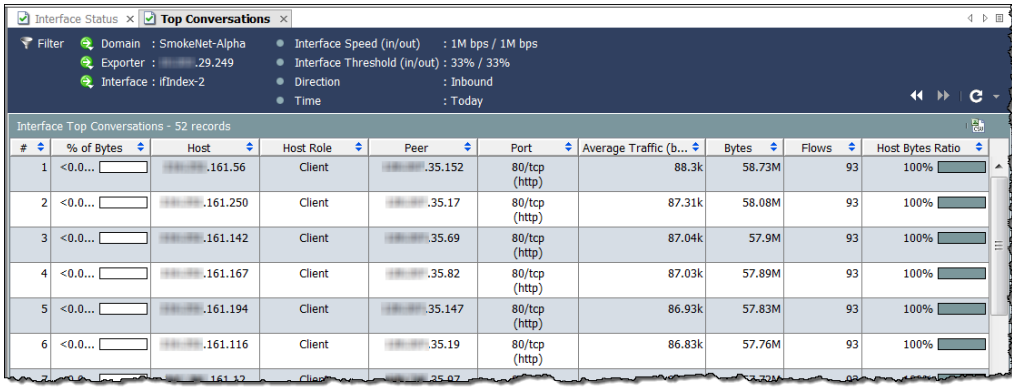


Exporter	Interface	Direction	Interface ...	Current Utilization	Current Traffic ...	Maximum Utilization	Maximum Traffic ...
.29.249	ifIndex-2	Inbound	1M	60,900.24%	609M	62,304.15%	623.04M
.29.249	ifIndex-6	Outbound	1M	60,900.24%	609M	62,304.15%	623.04M
.29.248	ifIndex-2	Inbound	1G	61.22%	612.25M	62.1%	620.96M
.29.248	ifIndex-6	Outbound	1G	61.22%	612.25M	62.1%	620.96M
.0.43	eth2	Inbound	1G	3.07%	30.69M	8.76%	87.59M
.25.144	eth3	Inbound	1G	0.42%	4.22M	9.2%	92.03M
.0.249	Uplink (vSwitch0)	Inbound	1G	0.2%	2.01M	0.82%	8.15M
.25.158	Uplink (vSwitch0)	Inbound	1G	0.17%	1.68M	6.34%	63.36M
.0.249	ifIndex-13 (vSwitch0)	Outbound	1G	0.1%	1.01M	0.4%	4.02M
.0.249	ifIndex-14 (vSwitch0)	Outbound	1G	0.1%	968.1k	0.41%	4.12M
.0.43	eth3	Inbound	1G	0.08%	751.09k	0.34%	3.38M

Right-click an interface in the Interface column and select **Top**. A pop-up menu appears, from which you can choose several options.



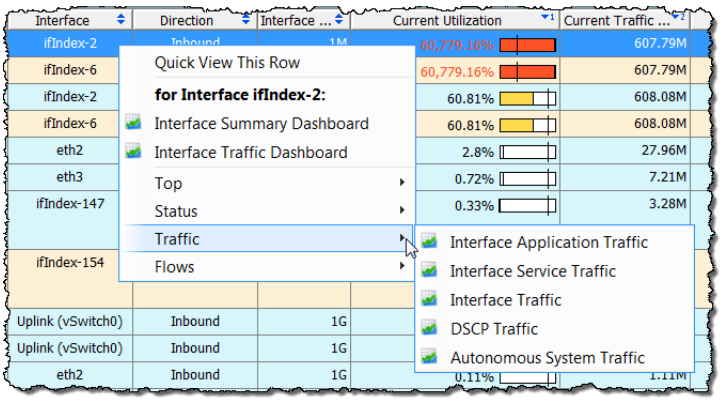
For example, if you select **Top > Conversations**, the Top Conversations document will be displayed, as shown in the following example. The Top Conversations document lists flow data according to the top conversations. The direction (which you can change in the filter) indicates whether the data includes all traffic (i.e., Total); traffic inbound to the selected item; traffic outbound from the selected item; or traffic within the selected item.



Tip:

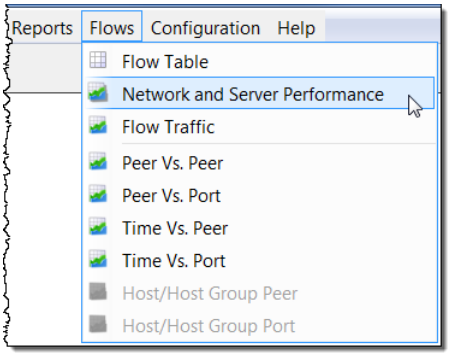
You can double-click an interface to open a Summary Report.

You can find many other useful documents for monitoring traffic by right-clicking within a column, and then selecting **Traffic** from the first pop-up menu.



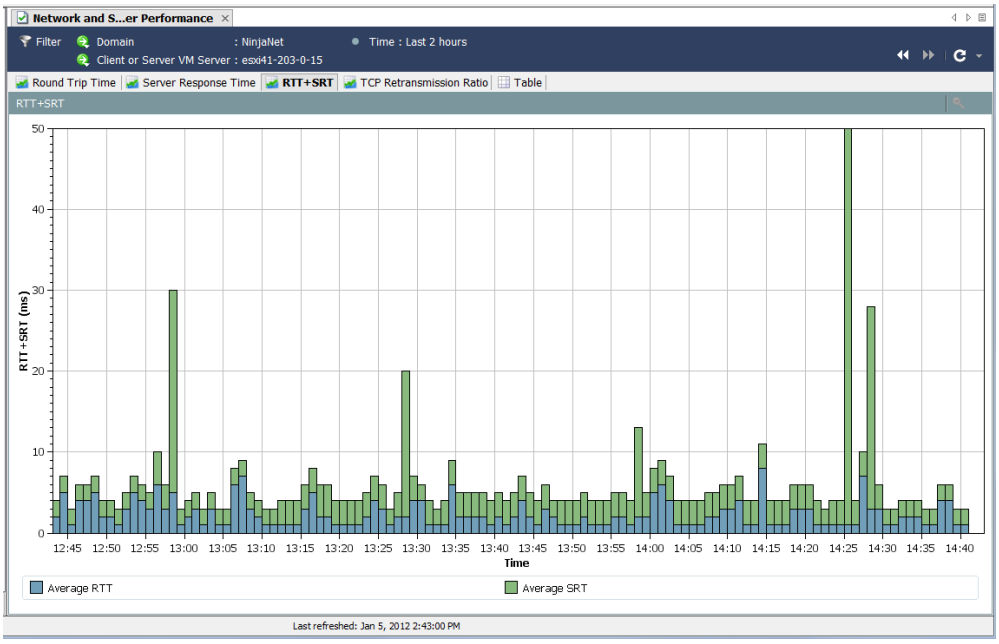
NETWORK PERFORMANCE

Suppose you have an employee who is complaining about the “slow Internet.” You can use the Network and Server Performance document to investigate these types of issues. To access this document, from the Main Menu select **Flows > Network and Server Performance**.



Note:

This report requires a Stealthwatch FlowSensor to gather the specific values that populate this report.

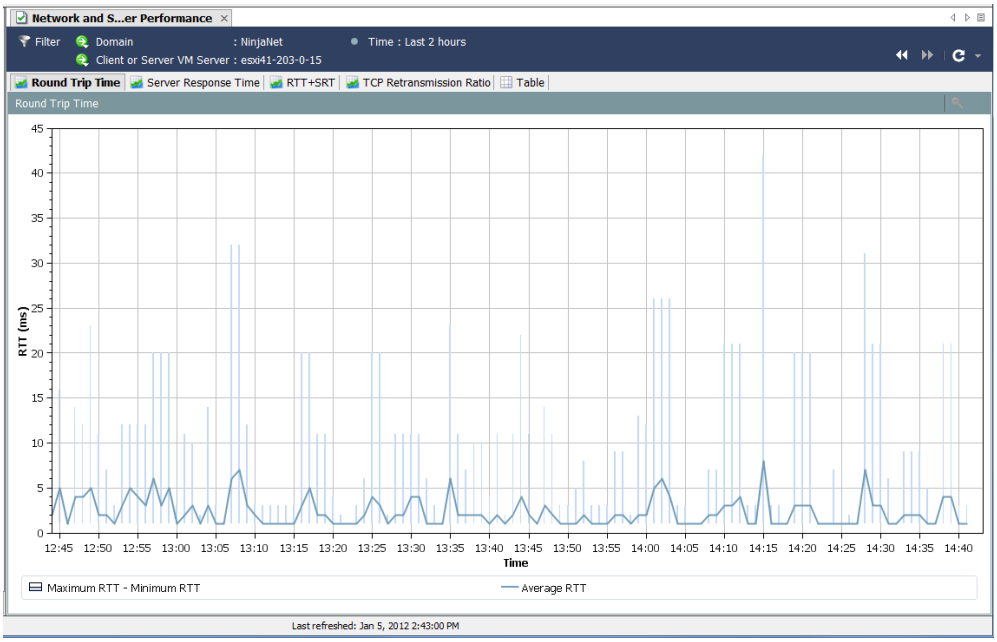


The Network and Server Performance document displays various performance data for flows stored in the database. Access the following tabs located at the top of the document to view this data:

- Round-Trip Time
- Server Response Time
- RTT+SRT
- TCP Retransmission Ratio
- Table

Round-Trip Time

The Round Trip Time tab graphically displays statistics for round trip time for flows.

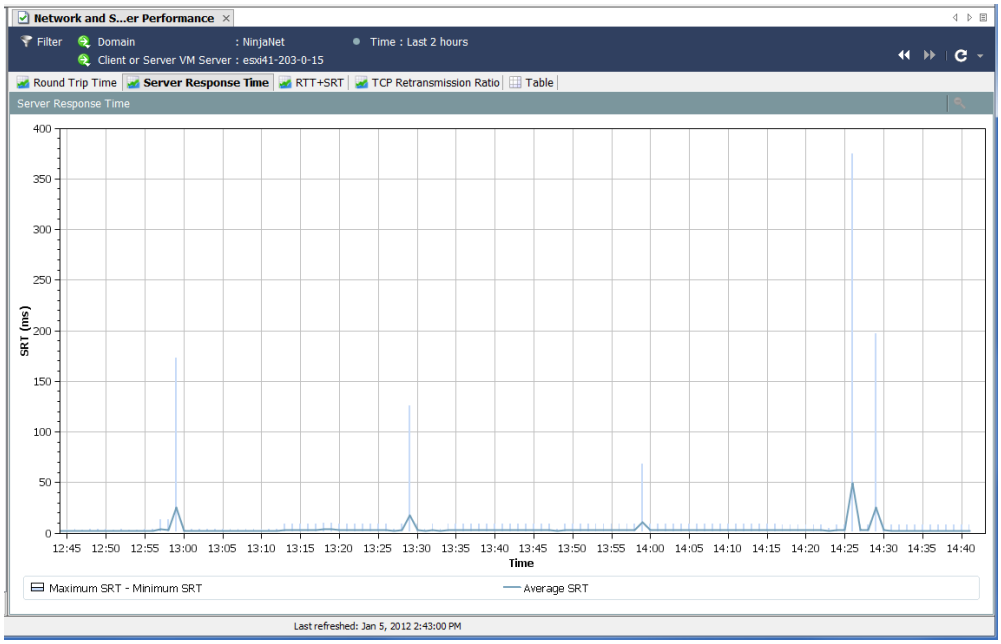


This feature is useful for measuring the amount of time required for flows to complete between host groups that are far apart. You can set this up using the Hosts page on the Filter.

The dark line that is at the bottom of the graph represents the calculated average RTT, while the tall, thin lines represent the spread between the calculated minimum and maximum RTT each minute.

Server Response Time

The Server Response Time tab graphically displays statistics for server response time (SRT) for flows.

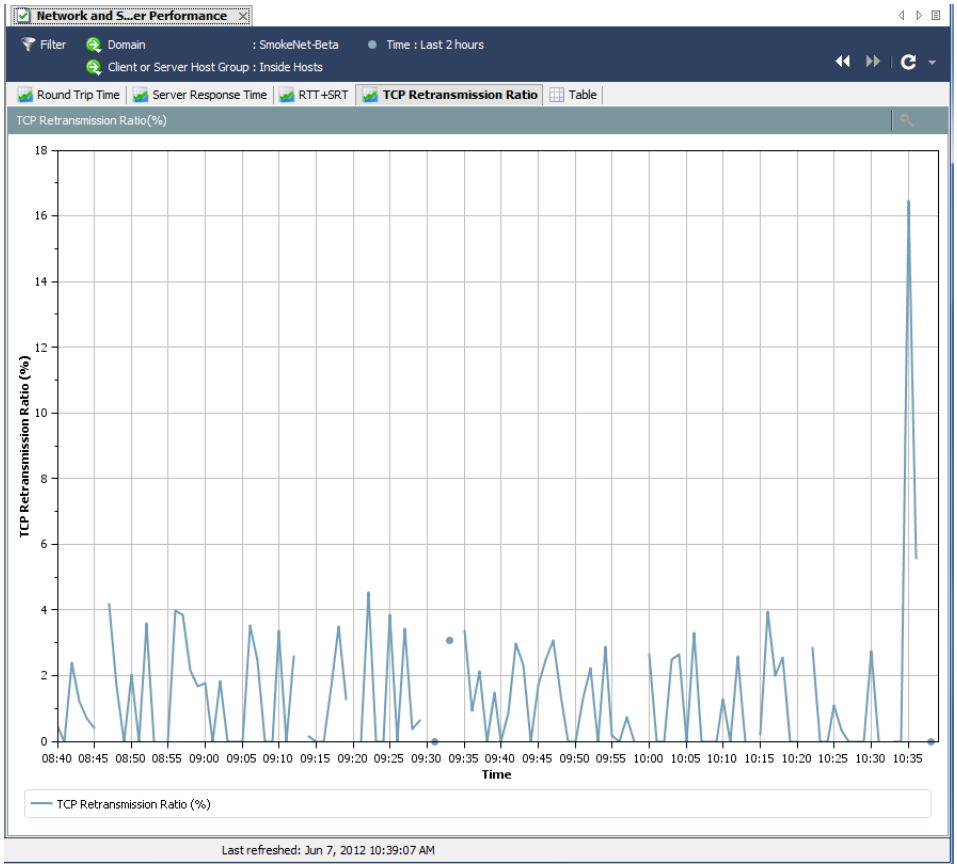


This feature is useful for measuring the amount of time required for a server to respond to a request. For example, a user complains that their Web-based application is performing poorly because screens are “taking forever to populate.” With this document, you can observe the server’s SRT and compare the average SRT with the user’s own SRT from the server.

TCP Retransmission Ratio

The TCP Retransmission Ratio tab of the Network and Server Performance document graphically displays the percentages of packets that have been retransmitted. The data covers a 2-hour period by default, with a 1-min. interval between data

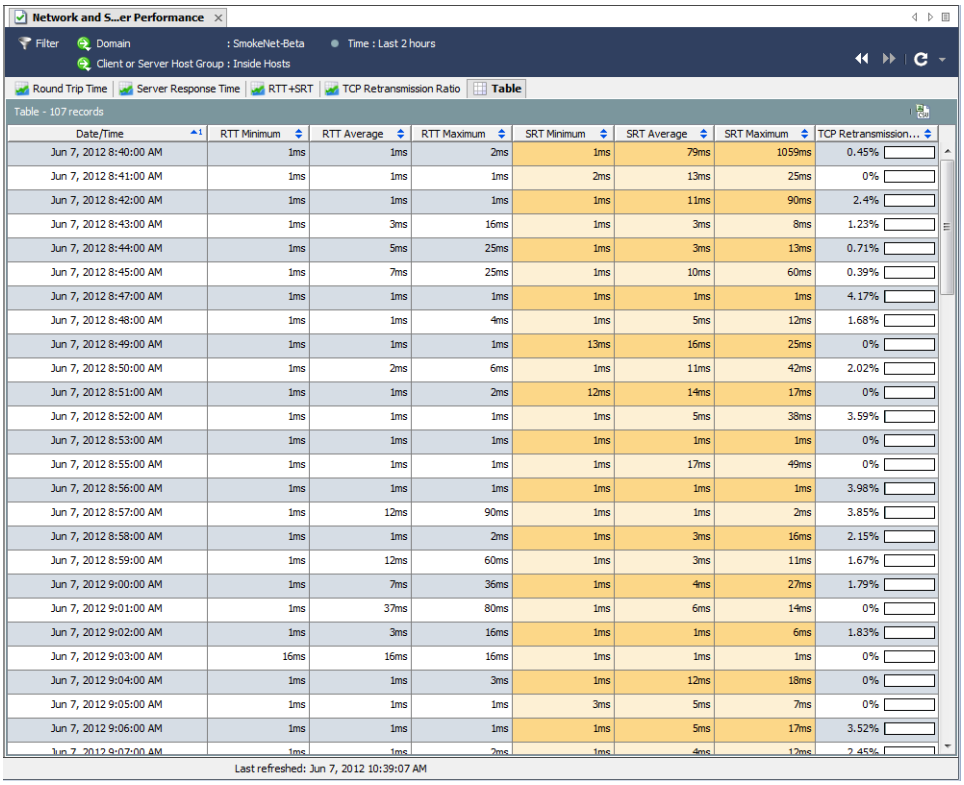
records.Retransmission usually occurs because packets are either damaged or lost..



Note:
This document is available only for domains that have a Stealthwatch Flow Collector for NetFlow that is receiving data from a Stealthwatch FlowSensor.

Table

The Table tab of the Network and Server Performance document lists performance data for flows. The data covers a 2-hour period by default, with a 1-min. interval between data records.



Date/Time	RTT Minimum	RTT Average	RTT Maximum	SRT Minimum	SRT Average	SRT Maximum	TCP Retransmission...
Jun 7, 2012 8:40:00 AM	1ms	1ms	2ms	1ms	79ms	1059ms	0.45%
Jun 7, 2012 8:41:00 AM	1ms	1ms	1ms	2ms	13ms	25ms	0%
Jun 7, 2012 8:42:00 AM	1ms	1ms	1ms	1ms	11ms	90ms	2.4%
Jun 7, 2012 8:43:00 AM	1ms	3ms	16ms	1ms	3ms	8ms	1.23%
Jun 7, 2012 8:44:00 AM	1ms	5ms	25ms	1ms	3ms	13ms	0.71%
Jun 7, 2012 8:45:00 AM	1ms	7ms	25ms	1ms	10ms	60ms	0.39%
Jun 7, 2012 8:47:00 AM	1ms	1ms	1ms	1ms	1ms	1ms	4.17%
Jun 7, 2012 8:48:00 AM	1ms	1ms	4ms	1ms	5ms	12ms	1.68%
Jun 7, 2012 8:49:00 AM	1ms	1ms	1ms	13ms	16ms	25ms	0%
Jun 7, 2012 8:50:00 AM	1ms	2ms	6ms	1ms	11ms	42ms	2.02%
Jun 7, 2012 8:51:00 AM	1ms	1ms	2ms	12ms	14ms	17ms	0%
Jun 7, 2012 8:52:00 AM	1ms	1ms	1ms	1ms	5ms	38ms	3.59%
Jun 7, 2012 8:53:00 AM	1ms	1ms	1ms	1ms	1ms	1ms	0%
Jun 7, 2012 8:55:00 AM	1ms	1ms	1ms	1ms	17ms	49ms	0%
Jun 7, 2012 8:56:00 AM	1ms	1ms	1ms	1ms	1ms	1ms	3.98%
Jun 7, 2012 8:57:00 AM	1ms	12ms	90ms	1ms	1ms	2ms	3.85%
Jun 7, 2012 8:58:00 AM	1ms	1ms	2ms	1ms	3ms	16ms	2.15%
Jun 7, 2012 8:59:00 AM	1ms	12ms	60ms	1ms	3ms	11ms	1.67%
Jun 7, 2012 9:00:00 AM	1ms	7ms	36ms	1ms	4ms	27ms	1.79%
Jun 7, 2012 9:01:00 AM	1ms	37ms	80ms	1ms	6ms	14ms	0%
Jun 7, 2012 9:02:00 AM	1ms	3ms	16ms	1ms	1ms	6ms	1.83%
Jun 7, 2012 9:03:00 AM	16ms	16ms	16ms	1ms	1ms	1ms	0%
Jun 7, 2012 9:04:00 AM	1ms	1ms	3ms	1ms	12ms	18ms	0%
Jun 7, 2012 9:05:00 AM	1ms	1ms	1ms	3ms	5ms	7ms	0%
Jun 7, 2012 9:06:00 AM	1ms	1ms	1ms	1ms	5ms	17ms	3.52%
Jun 7, 2012 9:07:00 AM	1ms	1ms	2ms	1ms	4ms	17ms	2.45%

Note:

This document is available only for domains that have a Stealthwatch Flow Collector for NetFlow that is receiving data from a Stealthwatch FlowSensor.

7

ANALYZING FLOWS

OVERVIEW

You have determined that a specific host has been compromised. You want to "pull back" conversations to and from that host in order to identify the host suspected of causing the compromise. Or, you see a high spike in traffic and want to analyze the data and determine the cause of the spike. Or, an alarm has been triggered and you need to determine if it is a threat to your network.

The flow analysis process allows you to make these determinations in order to secure your network. This chapter gives an overview of the flow analysis process and then walks you through several scenarios of the most common uses.

This chapter includes the following topics:

- Flow Filter
- Flow Table Tabs
- Quick View
- Flow Analysis Scenarios
- External Lookup

FLOW FILTER

The Flow Filter dialog allows you to choose the flow data you wish to review and to set different levels of filtering to receive the desired results.

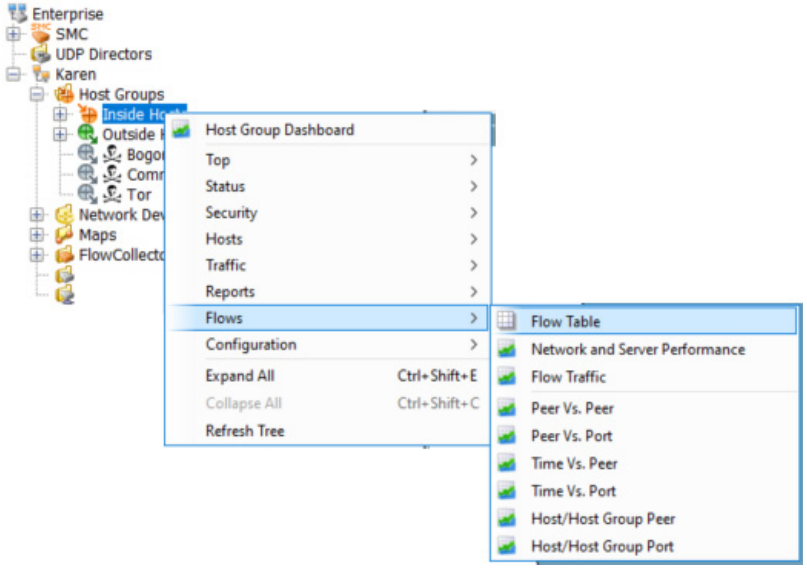
Entering Flow Queries

To query for flow data, complete the following steps:

Note:

It is not necessary to use all the settings described in the following steps.

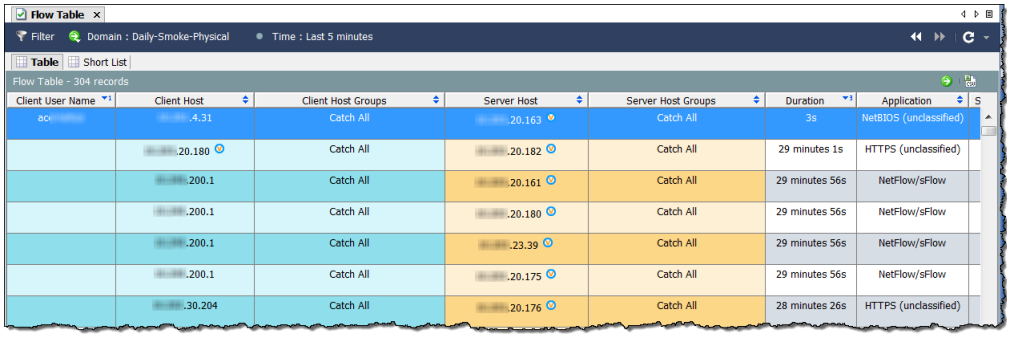
1. Right-click a domain, appliance, host group, or host IP address, and then select **Flows > Flow Table**.



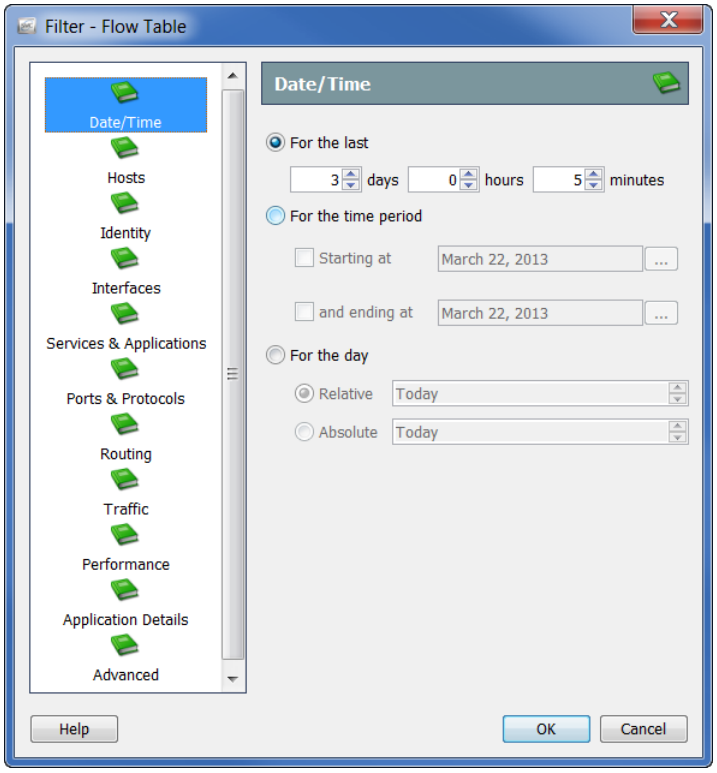
Tip:

If you press **Ctrl** on the keyboard as you click **Flow Table** from the pop-up menu, the filter will display first to enable you to refine the search criteria. After you click **OK**, the Flow Table will display using the search criteria you entered.

The Flow Table opens.



2. Click the **Filter** button in the upper left corner of the Flow Table to open the Filter dialog, and then click the **Date/Time** icon if it is not already highlighted. The Date/Time page opens.

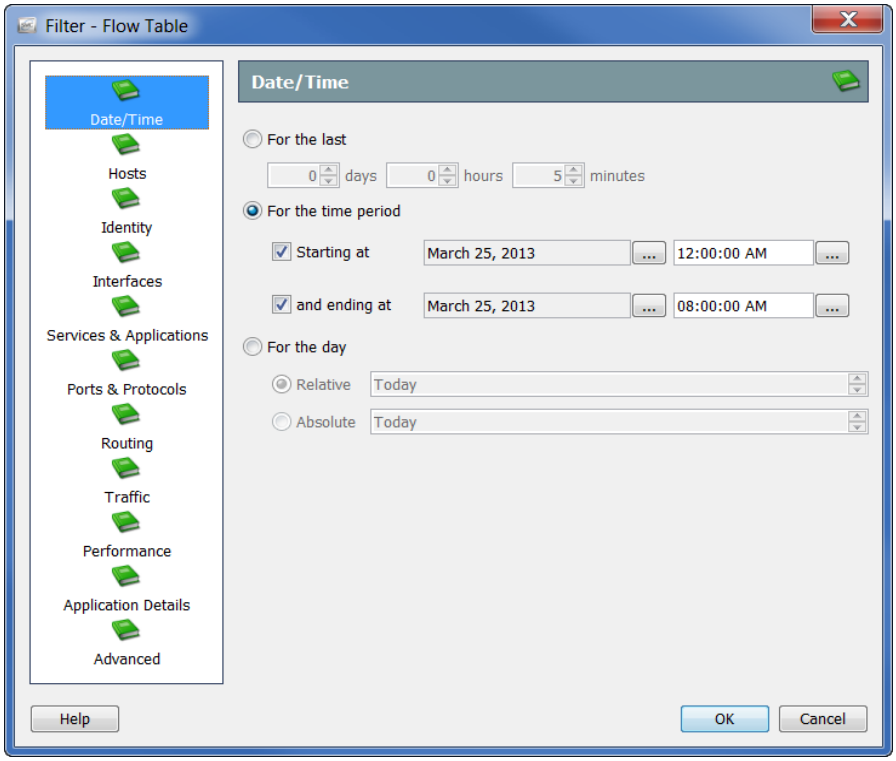


3. Specify an exact date/time, range, or relative setting by which to filter the flow data. For example, if you wanted to show all the flows between midnight and 8:00 AM on a particular day, you would complete the following steps:

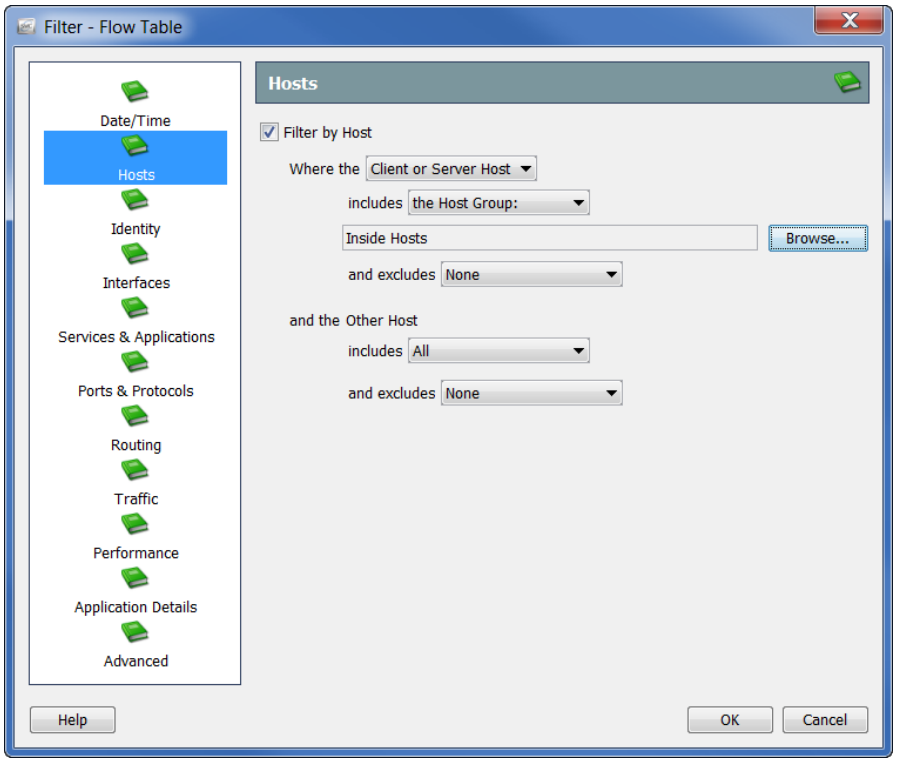
   a. Click the **For the time period** option.

   b. Click the **Starting at** option, enter the date you want to filter on, and enter ***12:00:00*** in the time field.

c. Click the **and ending at** option, enter the date you want to filter on, and enter ***08:00:00*** in the time field for that option.

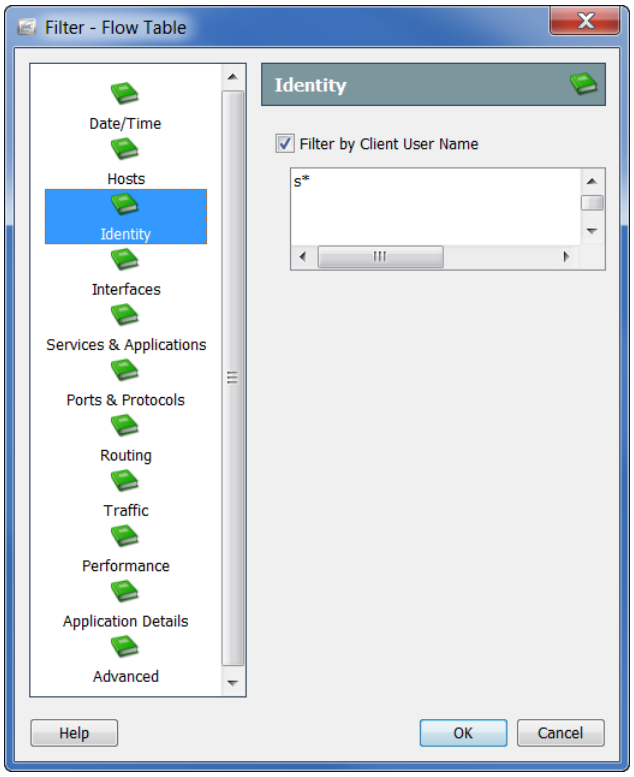


4. Click the **Hosts** icon. The Hosts page opens.



Specify the hosts by which you want to filter the flow data. You can include/exclude a host group, a range of IP addresses (using CIDR format), or a list of IP addresses (in comma-separated format).

5. Click the Identity icon. The Identity page opens.



Specify the user names by which you want to filter the flow data by completing the following steps:

1. Click the Client User Name check box to insert a check mark.
2. Type any of the following content in the text field:
   - A single user name, such as jdoe.
   - Multiple user names, such as jdoe, jalpha, jbeta. You can type the names, separating each name with a comma or pressing **Enter** after each name (to enter one name per line). You can also copy and paste from a comma-separated value (CSV) list of names.
   - Partial name(s) with wild cards. The wild card can be in any position, such as srh*, *doe. You can use more than one wild card in each name.

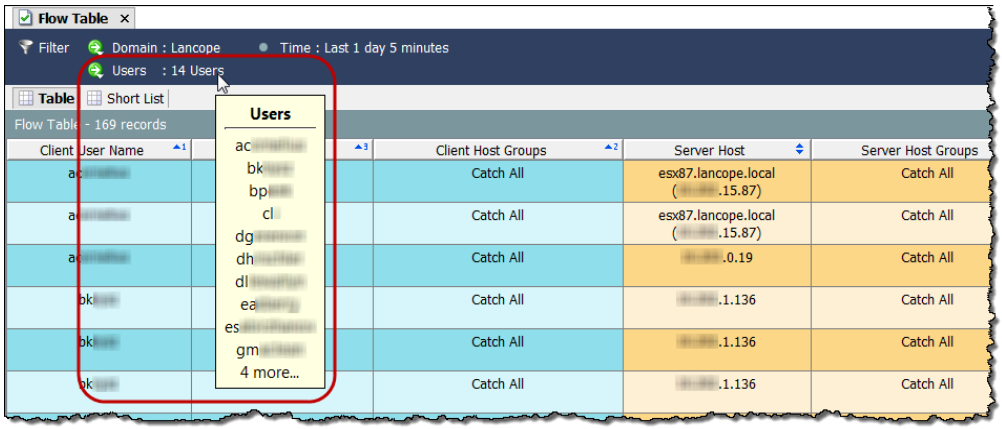
Notes:

- This field is not case sensitive.
- A user name cannot contain any of these characters: | + = ? “ < > ( ) : ;

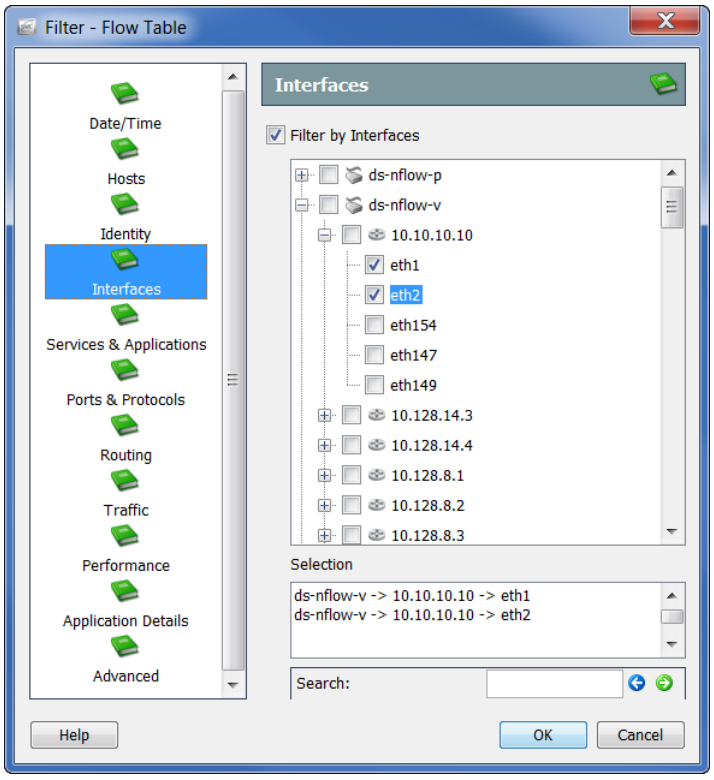
3. Click **OK**.

The results are displayed in the Client User Name column. If you have filtered on only one user, that user's name will display in the header. If you have filtered on more than one user, the header displays the number of user names you have filtered on. If you hover your cursor over this entry, the names of the first ten users you have queried are listed in a pop-up window (refer to the screen below).

The number of user names filtered on in addition to the first ten is displayed at the bottom of the pop-up window. In the example below, 14 user names have been filtered on, so at the bottom of the pop-up window the entry *4 more...* appears.

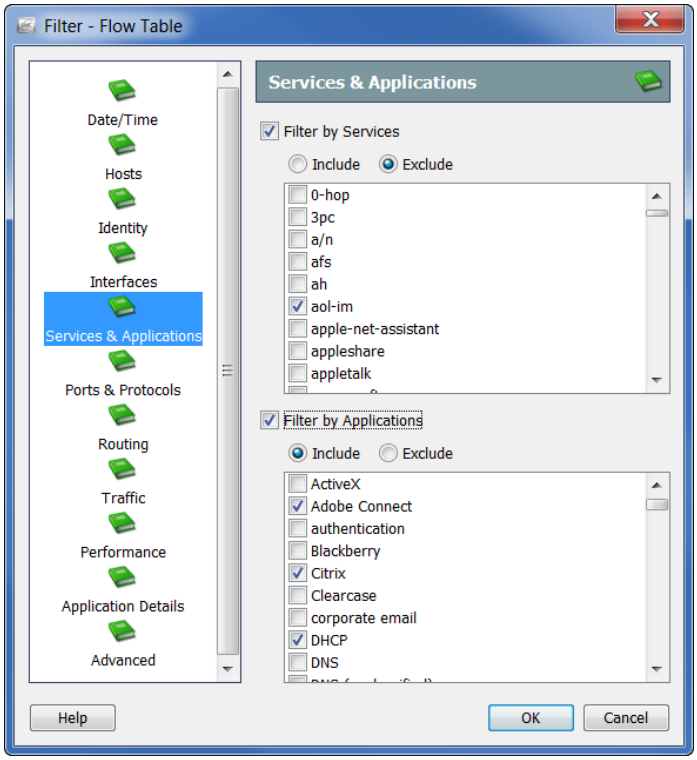


4. Click the **Interfaces** icon. The Interfaces page opens.



Specify the interfaces by which you want to filter the flow data. You can click individual interfaces, an entire exporter, or a Stealthwatch appliance.

5. Click the **Services & Applications** icon. The Services & Applications page opens.

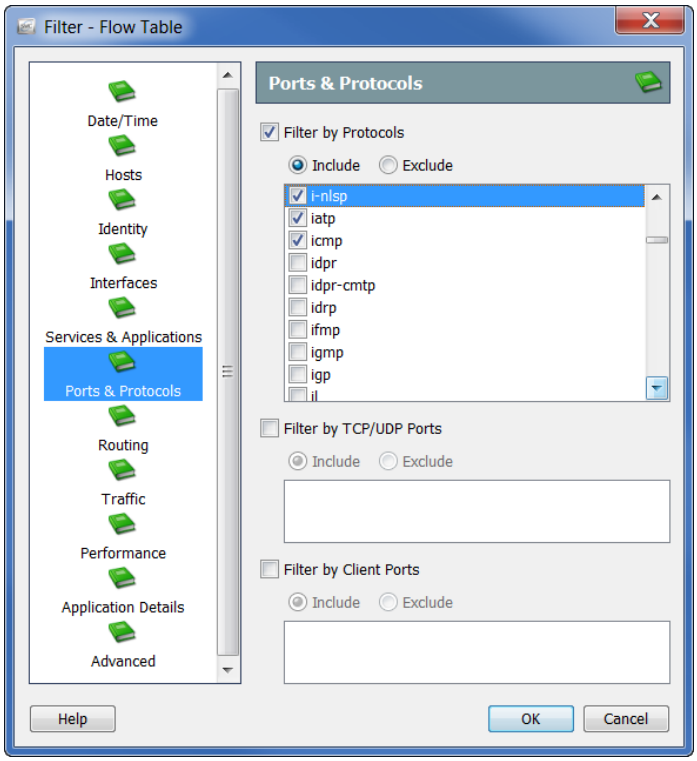


Specify the services or applications by which you want to filter the flow data by clicking one or both of the following check boxes to add a check mark(s):

- Filter by Services
- Filter by Applications

Click either the **Include** or **Exclude** option. For example, you may wish to limit your query to everything except Facebook. In that case, you would click the **Filter by Applications** check box to add a check mark, click the **Exclude** option, and then click the **Facebook** check box to add a check mark.

6. Click the **Ports & Protocols** icon. The Ports & Protocols page opens.

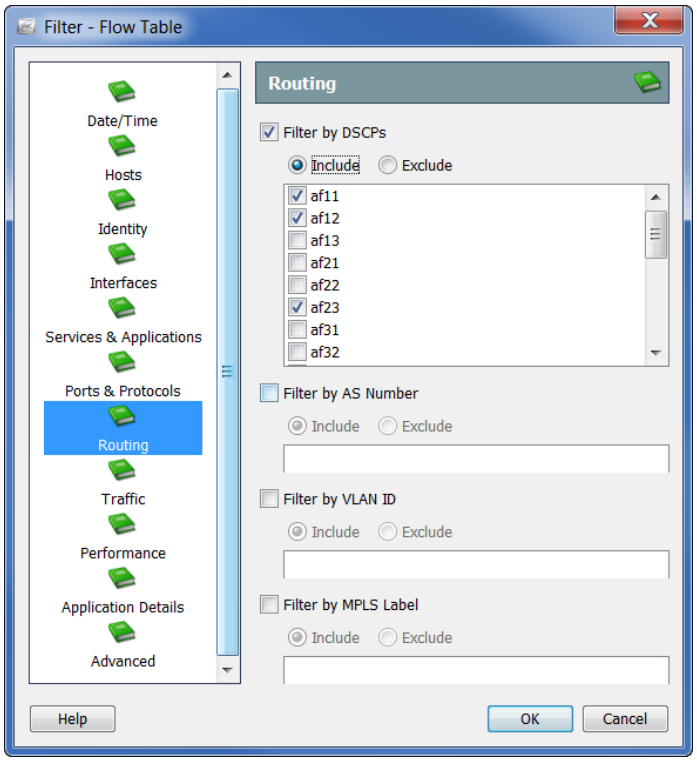


Specify the ports and protocols by which you want to filter the flow data by clicking any or all of the following check boxes to add a check mark(s):

- Filter by Protocols
- Filter by TCP/UDP Ports
- Filter by Client Ports

Click either the **Include** or **Exclude** option to further customize your query.

7. Click the **Routing** icon. The Routing page opens.

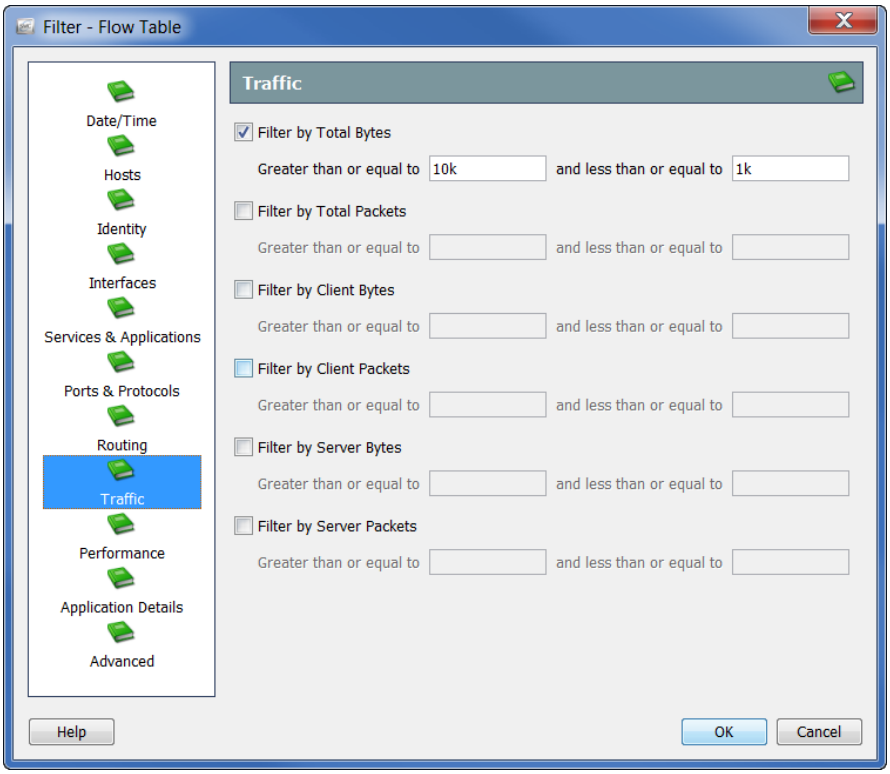


Specify the parameters by which you want to filter the flow data by clicking any or all of the following check boxes to add a check mark(s):

- Filter by DSCPs
- Filter by AS Number
- Filter by VLAN ID
- Filter by MPLS Label

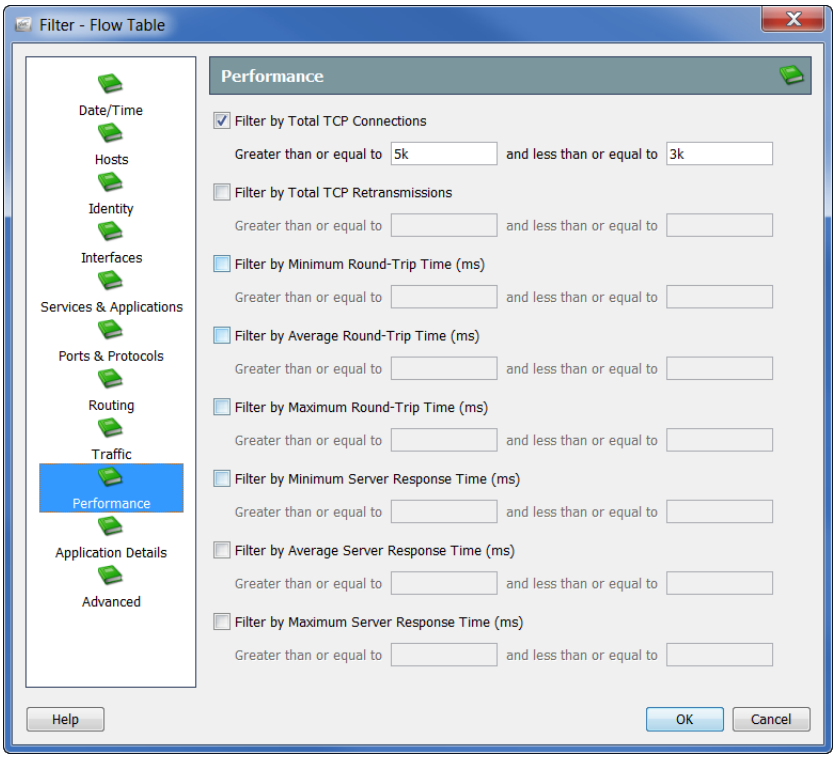
Click either the **Include** or **Exclude** option to further customize your query.

8. Click the **Traffic** icon. The Traffic page opens.



Specify the type and size of traffic data by which you want to filter the flow data.

9. Click the **Performance** icon. The Performance page opens.

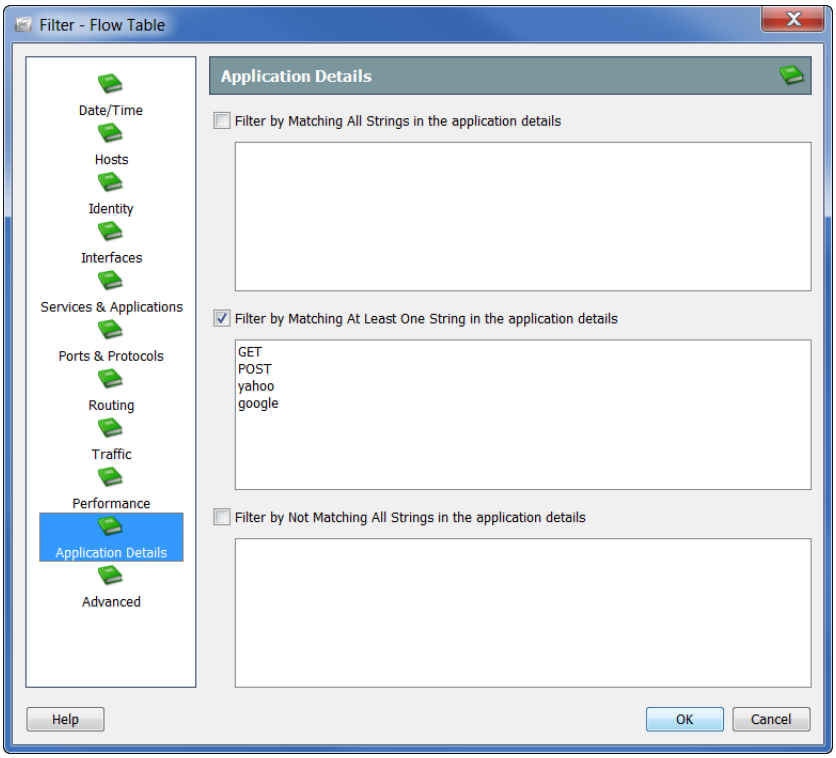


Specify the type and size of performance data by which you want to filter the flow data.

Note:

All values on the Performance page require a Stealthwatch FlowSensor to collect and store this information.

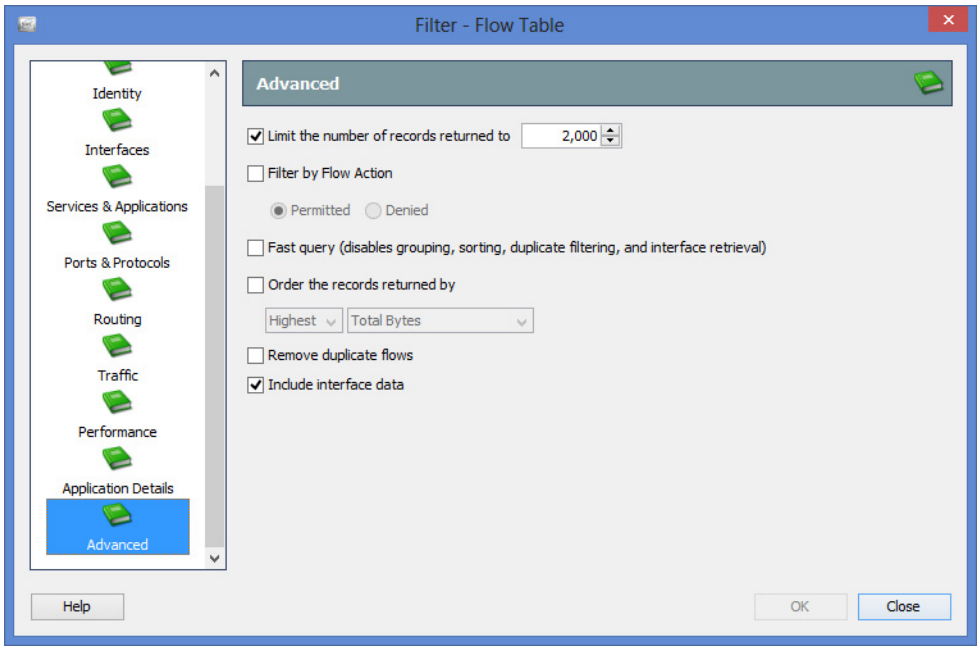
10. Click the **Application Details** icon. The Application Details page opens.



Specify the payload information by which you want to filter the flow data.

All values on the Application Details page requires a FlowSensor or exporting payload within Flexible NetFlow to collect and store this information.

11. Click the **Advanced** icon. The Advanced page opens.



You can limit the query to a maximum number of flow records. You can also specify how the data will be sorted (e.g., on the server, before the data is pulled) and whether or not duplicate flows will be removed from the results.

Notes:

- The **Remove duplicate flows** option is only relevant if there are multiple Flow Collectors. A single Flow Collector automatically de-duplicates.
- If you do not need to view interface data, click the **Include interface data** check box to remove the check mark. This allows for quicker data retrieval.

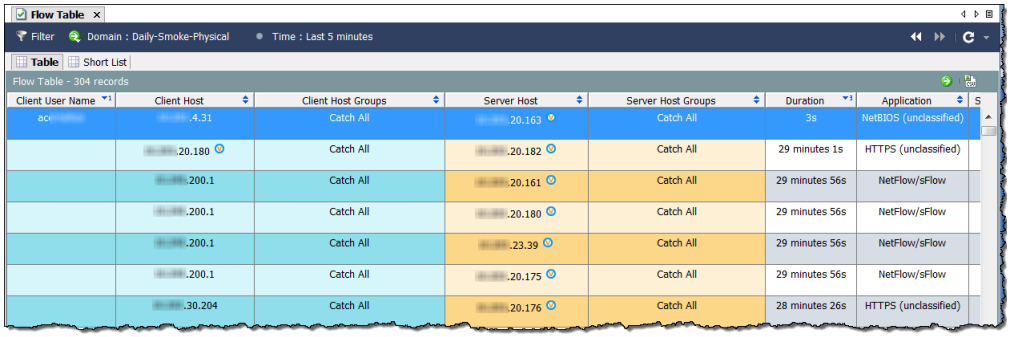
12. Click **OK** when you are ready to perform the filtering. The flow query is sent, and the retrieved data appears in the Flow Table document.

The next time you access the Flow Table, only the filter settings you have specified on the Advanced page will still be in effect. No filter settings on any other pages in the Flow Table filter will be retained.

FLOW TABLE TABS

Table Tab

The Table tab on the Flow Table document displays data for flows based on the options you specified on the Flow Table Filter.



Note:

You can click the **Go to Document** button in the upper right corner of the document to display other documents using the same flow data.

Because imported flow files do not include the original appliance/domain information, pop-up menu options that require this information are not available (they are grayed out) for imported flow files.

Note:

For more information about importing flow files, refer to the “How to Import a Flow File” topic in the *Stealthwatch Desktop Client Online Help*.

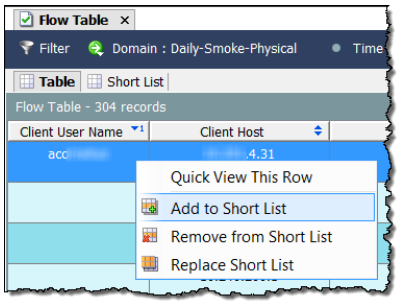
To change the columns displayed in the table, right-click a heading and select the desired columns from the pop-up menu. A heading with a check mark next to its name indicates that it will be displayed in the document.

Short List Tab

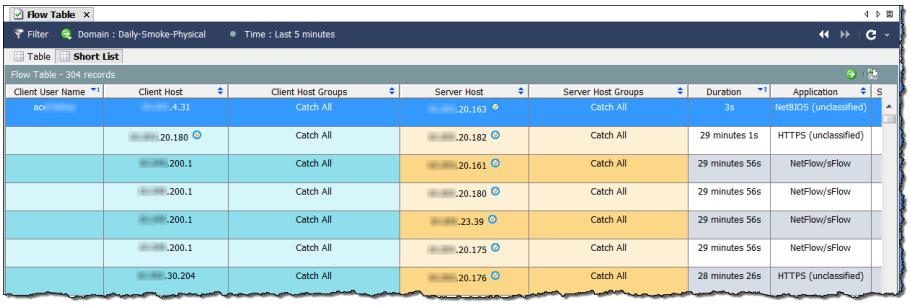
The Short List tab shares the same configuration as the Table tab. Changes made on one are automatically reflected on the other.

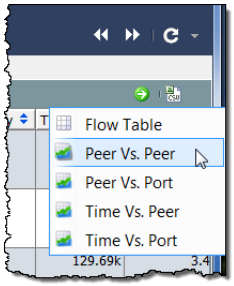
The Short List tab on the Flow Table document allows you to display a subset of the flow data that appears on the Flow Table: Table page. For example, the Table tab may show thousands of records of flows, but you may want to view only a small number of those rows for closer analysis. The Short List feature allows you to select specific rows for easier viewing.

Right-click a row(s) on the Table tab and select **Add to Shortlist**, as shown in the example to the right.



To view the flow, click the **Short List** tab to open the Flow Shortlist. The row(s) you selected will be displayed in this document.





To view the subset of data graphically, click the **Go to Document** button and click the type of analysis (e.g., Peer vs. Peer) you desire from the pop-up menu.

Only the data for the hosts in the Short List appears, rather than all the data that was retrieved by the Flow Table Filter.

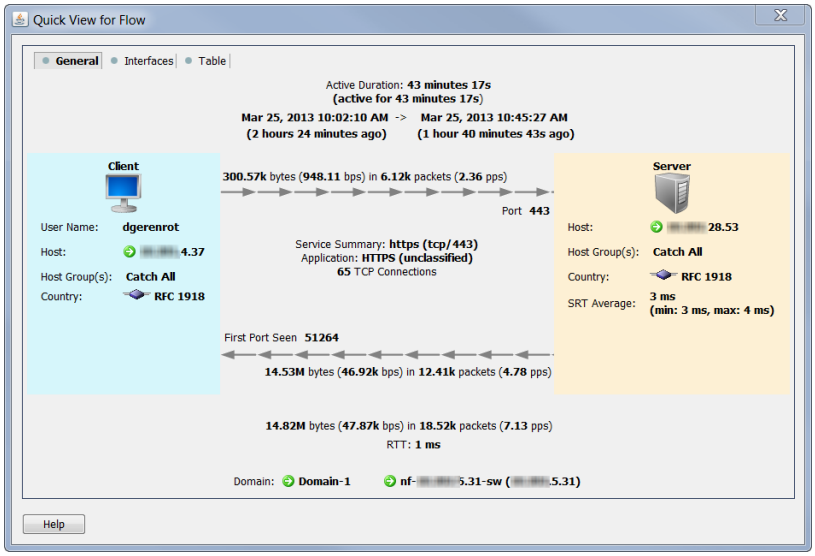
QUICK VIEW

The Quick View dialog provides a quick and easy way to view tabular data graphically. It also provides quick navigation to filtered views of other documents.

To see the Quick View dialog, click a table cell, and then press the Spacebar. To make the dialog disappear, press the Spacebar again or the Esc key.

As shown in the example below, the Quick View dialog shows data on the following tabs:

- General
- Interfaces
- Table



You can navigate from tab to tab by pressing the Alt key together with the ← or → key on your keyboard.

You can navigate from flow to flow (while keeping the Quick View dialog open) by pressing the Alt key together with the ↑ or ↓ key on your keyboard.

Tip:

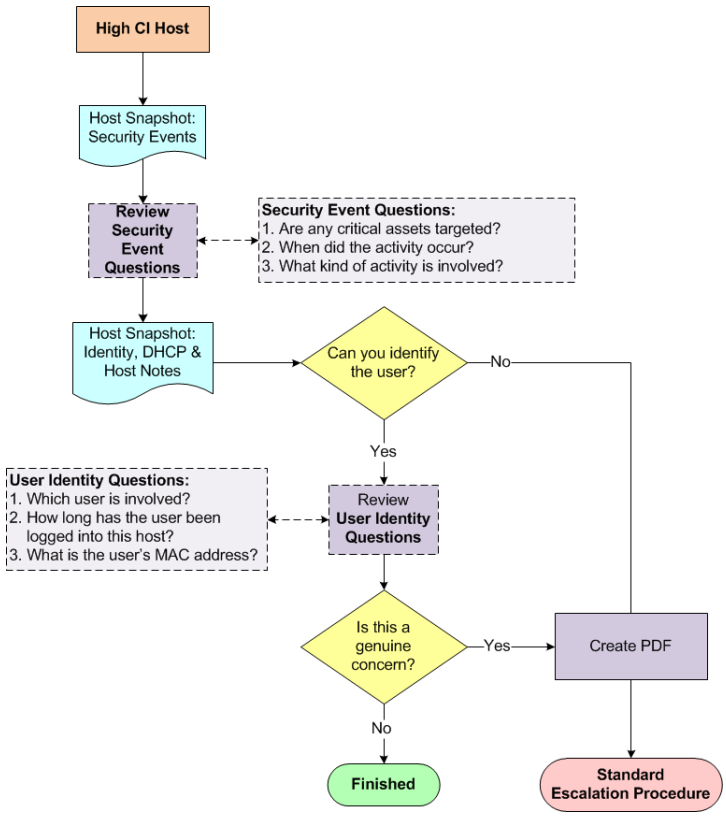
The same navigation features (e.g., drilling down to other documents) that apply to other tables apply here as well.

FLOW ANALYSIS SCENARIOS

Now that you are familiar with the flow analysis process, we will walk you through several common scenarios.

High Concern Index Hosts

A High CI host is a host that is the source of suspicious flow activity (Security Events). The following diagram illustrates a workflow you can use to determine if the threat is genuine.



Workflow Overview

The following steps provide an overview of the procedures illustrated in the preceding workflow diagram.

1. Open the Host Snapshot: Security Events page for the source host and review the details. Refer to the following section, "Examining Security Event Activity (Host Snapshot)."
2. Click the **Identity, DHCP & Host Notes** tab.
3. Can you identify the user?
   - If yes, go to step 4.

- If no, go to step 6.

4. Review the information of any users logged in to the source host. Refer to "Examining User Identity Information (Host Snapshot)" on page 158.
5. Based on the information you have gathered, does this activity appear to be a genuine concern?
   - If yes or if you are unsure, go to step 6.
   - If no, stop here.
6. Create a PDF of the Host Snapshot and escalate according to your organization's standard escalation procedure.

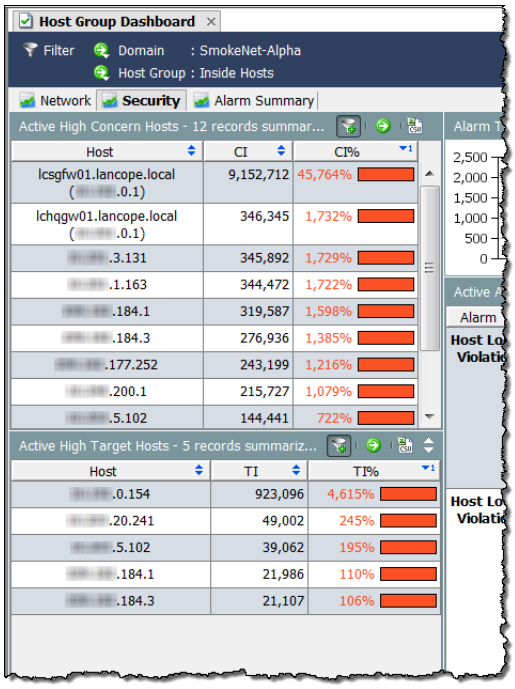
Examining Security Event Activity (Host Snapshot)

A High CI host could be infected with malware or compromised in some other way. The SMC provides several places, including the following, where you can easily identify High CI hosts:

- Concern Index
- Alarm Table (if an alarm was triggered)
- Host Group Dashboard: Security page

This workflow starts the investigation from the Host Group Dashboard: Security page. Complete the following steps to examine the Security Event activity of a High CI host.

1. On the Host Group Dashboard, click the **Security** tab. In the **Active High Concern Hosts** and the **Active High Target Hosts** sections, the High CI hosts and High TI hosts are listed for the host group associated with that particular Host Group Dashboard.

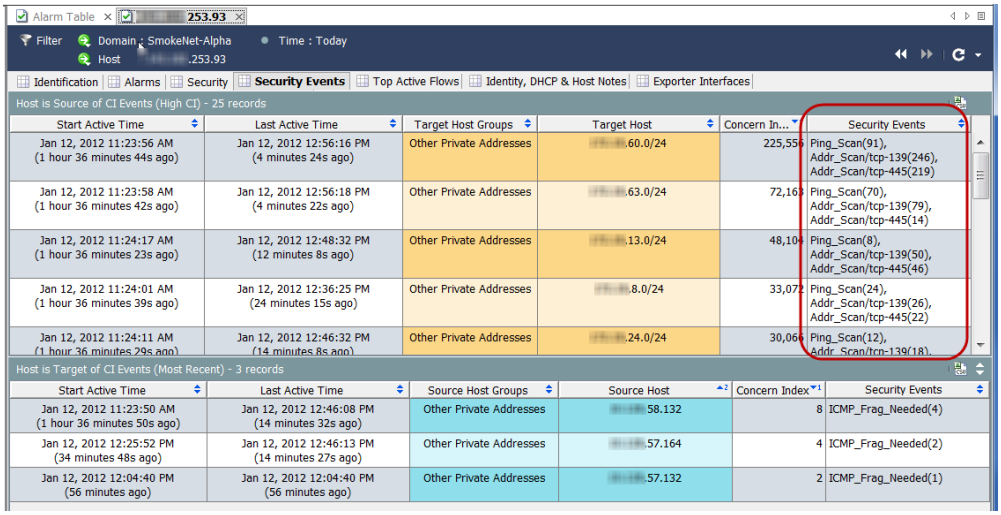


2. Double-click the appropriate host IP address to open its Host Snapshot.

Tip:

If you know the IP address, you also can find the Host Snapshot by using the global Search function.

3. Click the **Security Events** tab.
4. In the **Host is Source of Security Events (High CI)** section, review the entries in the Security Events column (refer to the following example). Ask yourself the following questions:
   - Are any critical assets being targeted?
   - When did the activity occur?
   - What kind of activity is involved?



Note:

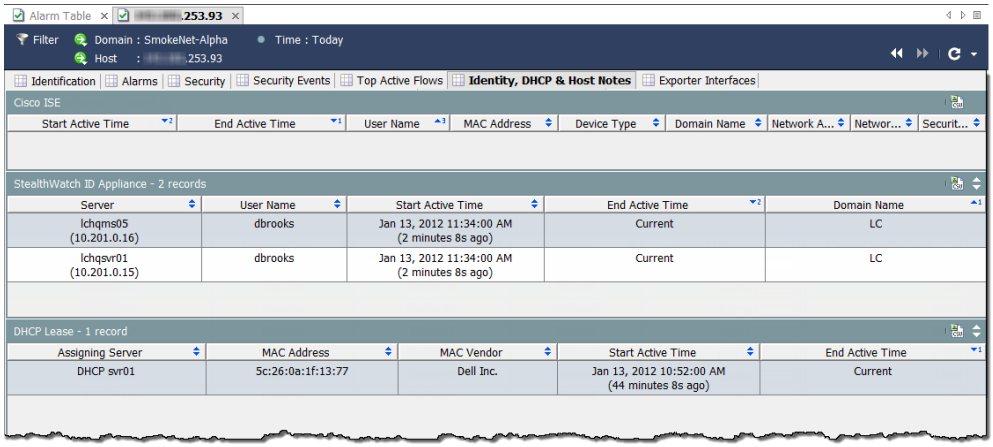
Refer to the "Security Events" topic in the *Stealthwatch Desktop Client Online Help* for detailed descriptions of specific Security Events.

5. Examine the user identity information as described in the following section.

Examining User Identity Information (Host Snapshot)

Once you understand the Security Event activity of a High CI host, complete the following steps to examine the identity of the user(s) that have logged in to that host.

1. On the Host Snapshot, click the **Identity, DHCP & Host Notes** tab.



2. Do you see any user information?
   - If yes, go to step 3.
   - If no, go to step 5.

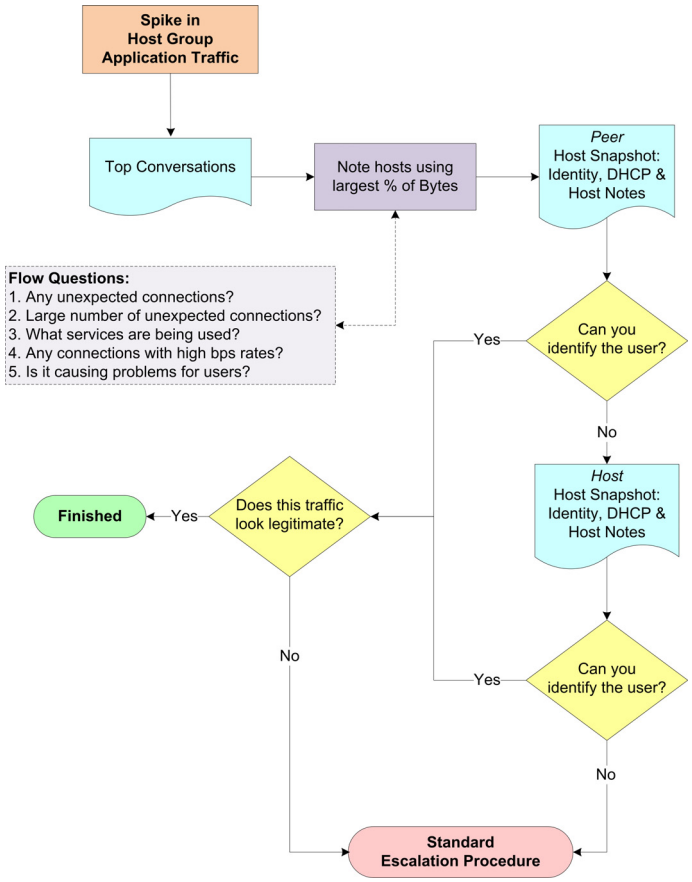
3. Review the user information with the following questions in mind:

- Which user(s) have logged in to this host?
- How long have they been logged in?
- What is the user's MAC address?

4. Based on the information you have gathered about this host, does this activity appear to be a genuine concern?
   - If yes, or if you are unsure, go to step 5.
   - If no, stop here.
5. Create a PDF of the Host Snapshot and escalate according to your organization's standard escalation procedure.

Spike in Application Traffic

If you see a sudden increase in traffic in one area of your network, use the workflow illustrated in the following diagram to help you determine the cause of this sudden increase, and to determine whether or not you should be concerned.



Workflow Overview

The SMC provides several places where you can see traffic spikes, such as the following:

- Any traffic graph that you can access via the Traffic menu.
- Host Group Dashboard: Network page

This workflow starts the investigation from the Network page. The following steps provide an overview of the procedures illustrated in the preceding workflow diagram.

1. On the Network page, determine in which direction the traffic spike is going. Refer to "Identifying the Hosts Involved" on page 162.
2. Double-click that traffic spike to open the Top Conversations document, and then identify which host pair is using the most bandwidth in the noted direction. Refer to "Identifying the Hosts Involved" on page 162.
3. Review the following questions regarding the host pair identified above:
   - Are there any unexpected connections (e.g., unauthorized host groups or servers)?
   - Are there a large number of unexpected connections?
   - What ports are being used?
   - Are there large amounts of traffic being sent and/or received?
   - Are there any connections with high bps rates?
   - Does this spike correlate with user complaints about the network?
4. Open the Host Snapshot: Identity, DHCP & Host Notes page for the peer. Refer to "Identifying the Users Involved" on page 162.
5. Can you identify the user involved?
   - If yes, go to step 8.
   - If no, go to step 6.
6. Open the Host Snapshot: Identity, DHCP & Host Notes page for the host. Refer to "Identifying the Users Involved" on page 162.
7. Can you identify the user involved?
   - If yes, go to step 8.
   - If no, go to step 9.
8. Does this traffic look like legitimate activity?
   - If yes, or if you are not sure, go to step 9.
   - If no, you can disregard the traffic spike.
9. Gather the information you have collected thus far and escalate according to your organization's standard escalation procedure.

Identifying the Direction of Traffic

The Host Group Dashboard provides the most comprehensive view of host group application traffic on its Network tab.

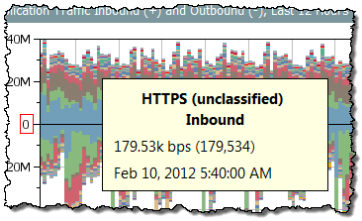
Look at the **Application Traffic Inbound (+) and Outbound (-)** and the **Application Traffic Within** charts to immediately see if you have a spike in traffic, and to determine in which direction that traffic is traveling.

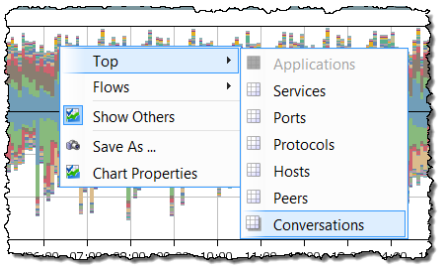
The **Application Traffic Inbound (+) and Outbound (-)** chart shows traffic traveling into the Inside Host Groups from the Outside Host Groups and vice versa. Inbound traffic appears above the zero (0) line. Outbound traffic appears below the zero line.

The **Application Traffic Within** chart shows traffic that is traveling only between the subhost groups within the network (Inside Host Groups).

Each chart displays the top 15 applications used over the time period set in the filter. A different color represents each application. The legend for each chart lists the services in order from the most used to the least used. Hover the cursor over an application in the legend to see that application highlighted in the chart.

Hover the cursor over a data point on the chart to display a tool tip that provides details about that traffic, as shown in the example to the right.



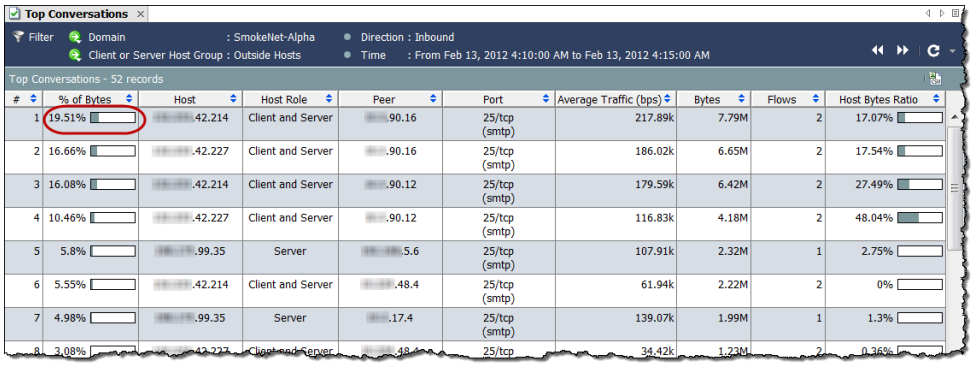


Double-click a data point to display a pop-up menu that allows you to choose from several options to learn more about that traffic, as shown in the example to the left.

Identifying the Hosts Involved

Once you know the direction in which the traffic is traveling, complete the following steps to determine which host pair involved.

1. On the Network tab, double-click the traffic spike to open the Top Conversations document.



#	% of Bytes	Host	Host Role	Peer	Port	Average Traffic (bps)	Bytes	Flows	Host Bytes Ratio
1	19.51%	.42.214	Client and Server	.90.16	25/tcp (smtp)	217.89k	7.79M	2	17.07%
2	16.66%	.42.227	Client and Server	.90.16	25/tcp (smtp)	186.02k	6.65M	2	17.54%
3	16.08%	.42.214	Client and Server	.90.12	25/tcp (smtp)	179.59k	6.42M	2	27.49%
4	10.46%	.42.227	Client and Server	.90.12	25/tcp (smtp)	116.83k	4.18M	2	48.04%
5	5.8%	.99.35	Server	.5.6	25/tcp (smtp)	107.91k	2.32M	1	2.75%
6	5.55%	.42.214	Client and Server	.48.4	25/tcp (smtp)	61.94k	2.22M	2	0%
7	4.98%	.99.35	Server	.17.4	25/tcp (smtp)	139.07k	1.99M	1	1.3%
8	3.08%	.42.227	Client and Server	.48.4	25/tcp	34.42k	1.23M	2	0.36%

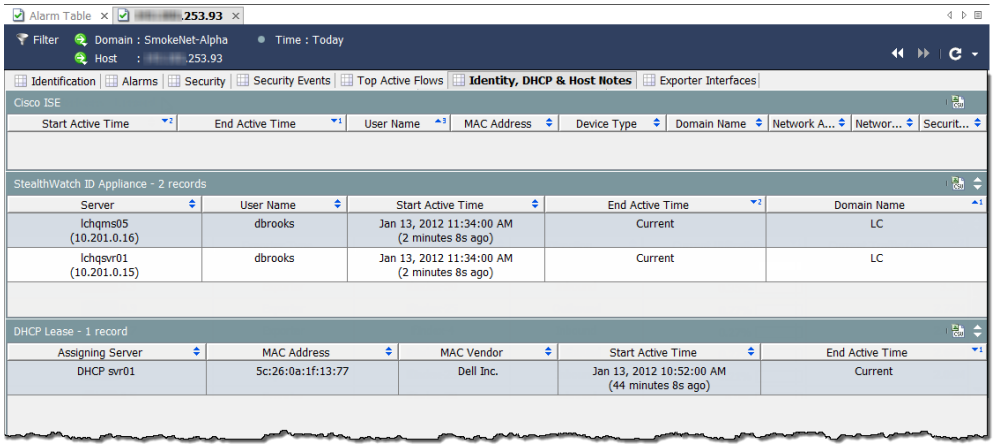
2. Identify the host and the peer that are using the highest percentage of bytes. (By default, this is represented by the number **1** in the **#** column.)
3. Review the following questions regarding the host pair identified above:
   - Are there any unexpected connections (e.g., unauthorized host groups or servers)?
   - Are there a large number of unexpected connections?
   - What ports are being used?
   - Are there large amounts of traffic being sent and/or received?
   - Are there any connections with high bps rates?
   - Does this spike correlate with user complaints about the network?

Identifying the Users Involved

After you know the IP addresses of the host pair(s) involved in the traffic spike, complete the following steps to see if you can identify which users are involved and whether or not this activity is of any concern.

1. Double-click the appropriate host IP address to open its Host Snapshot.

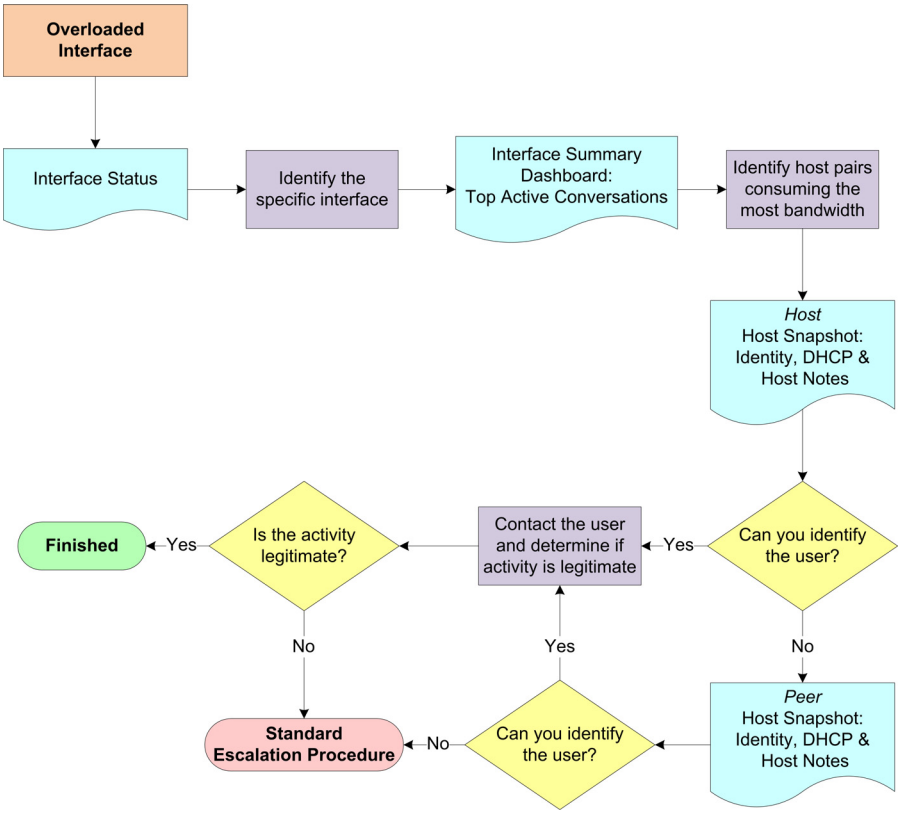
2. Click the I**dentity, DHCP & Host Notes** tab.



3. Do you see any user information?
   - If yes, go to step 6.
   - If no, go to step 4.
4. Double-click the appropriate peer IP address to open its Host Snapshot.
5. Click the **Identity, DHCP & Host Notes** tab.
6. Do you see any user information?
   - If yes, go to step 6.
   - If no, go to step 7.
7. Does this activity appear to be of any concern?
   - If yes, or if you are unsure, go to step 7.
   - If no, stop here.
8. Gather the information you have collected thus far and escalate according to your organization's standard escalation procedure.

Overloaded Interface

If you know or suspect that an interface has become overloaded or is close to capacity, you can use the workflow shown in the following diagram to help pinpoint the source of the problem.



Workflow Overview

The SMC provides several places, including the following, where you can easily see interface utilization:

- Network Devices within the Enterprise tree
- Interface Status
- Alarm Table (if an Interface Utilization Exceeded alarm was triggered)

This workflow starts the investigation from the Interface Status document. The following steps provide an overview of the procedures illustrated in the preceding workflow diagram.

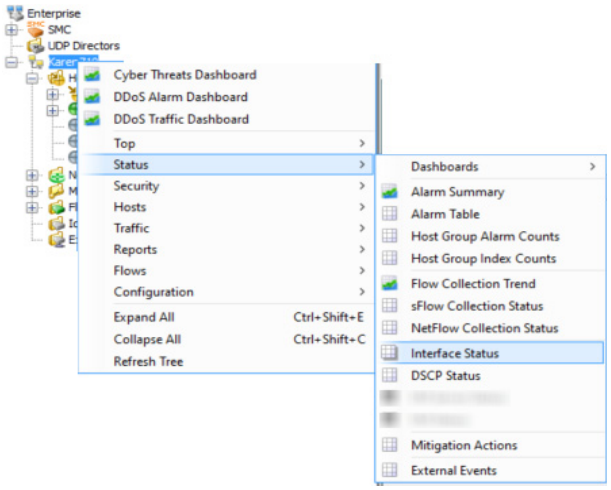
1. Open the Interface Status document for the domain to identify the overloaded interface. Refer to the following section, "Identifying an Overloaded Interface (Interface Status)."
2. Open the Interface Summary Dashboard for the over-utilized interface and look at the Top Active Conversations.

3. Note the IP addresses of the host pair (host and peer) consuming the most bandwidth.
4. Open the Host Snapshot: Identity, DHCP & Host Notes page for the host. Refer to "Identifying Users Logged In to a High Bandwidth Host" on page 172.
5. Can you identify the user?
   - If yes, go to step 8.
   - If no, go to step 6.
6. Open the Host Snapshot: Identity, DHCP & Host Notes page for the peer. Refer to "Identifying Users Logged In to a High Bandwidth Host" on page 172.
7. Can you identify the user?
   - If yes, go to step 8.
   - If no, go to step 10.
8. Contact the user and determine if the activity in which the user is engaged is legitimate.
9. Is the activity legitimate?
   - If yes, stop here.
   - If no, go to step 10.
10. Gather the information you have collected thus far and escalate according to your organization's standard escalation procedure.

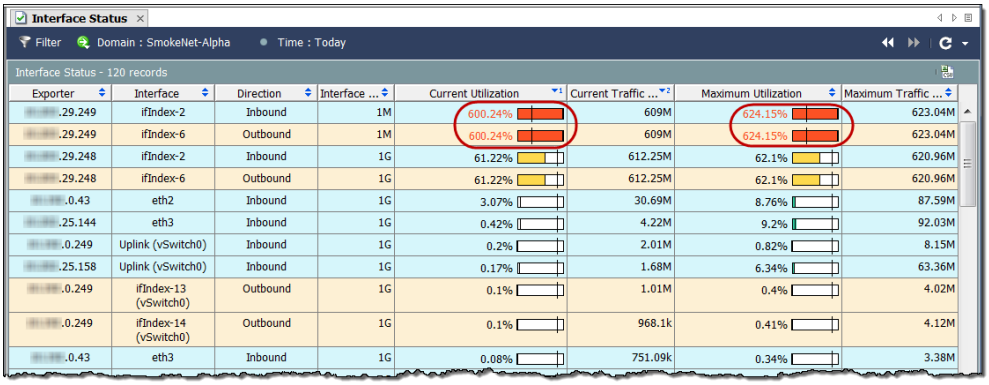
Identifying an Overloaded Interface (Interface Status)

Complete the following steps to open the Interface Status document and identify the specific interface that is either overloaded or close to capacity.

1. Right-click the domain name and select **Status > Interface Status**.
2. When the Interface Status document opens, identify any interfaces that are either overloaded or close to capacity, as



shown in the following example. (**Hint:** Look for red, orange, or yellow bars in the Current Utilization and Maximum Utilization columns.)

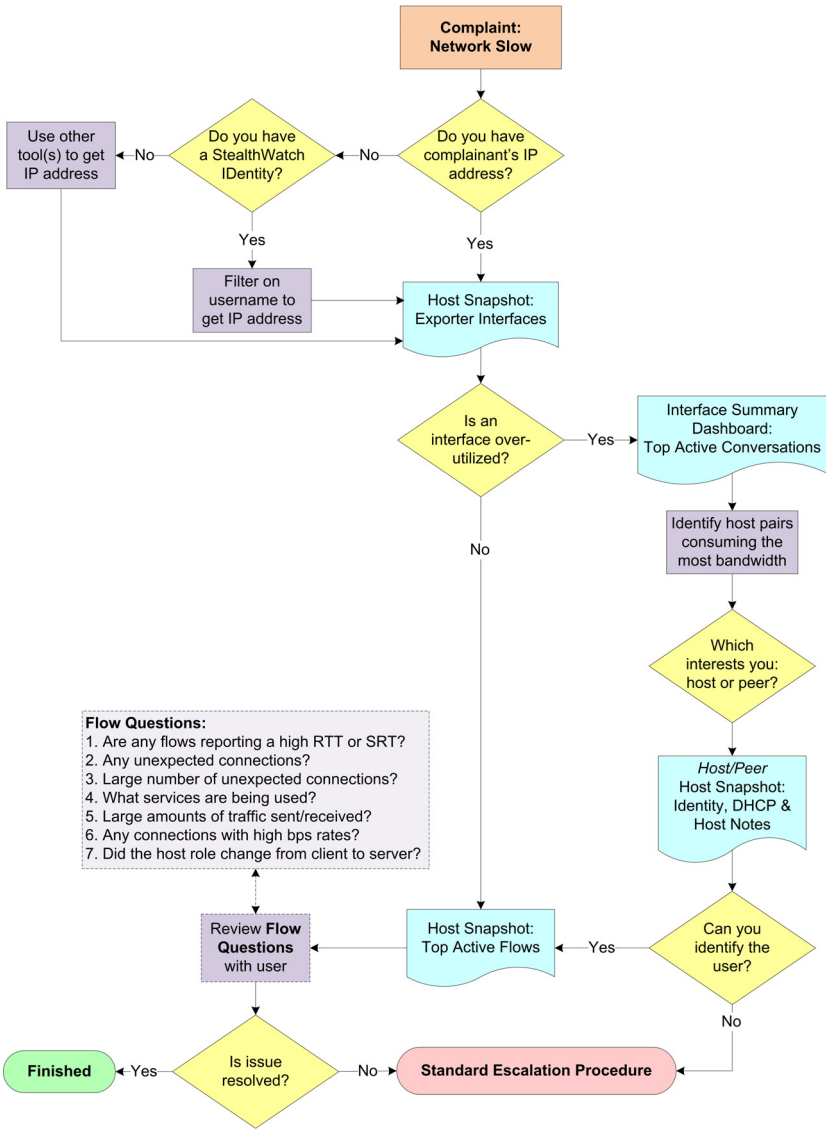


Exporter	Interface	Direction	Interface ...	Current Utilization	Current Traffic ...	Maximum Utilization	Maximum Traffic ...
.29.249	ifIndex-2	Inbound	1M	600.24%	609M	624.15%	623.04M
.29.249	ifIndex-6	Outbound	1M	600.24%	609M	624.15%	623.04M
.29.248	ifIndex-2	Inbound	1G	61.22%	612.25M	62.1%	620.96M
.29.248	ifIndex-6	Outbound	1G	61.22%	612.25M	62.1%	620.96M
.0.43	eth2	Inbound	1G	3.07%	30.69M	8.76%	87.59M
.25.144	eth3	Inbound	1G	0.42%	4.22M	9.2%	92.03M
.0.249	Uplink (vSwitch0)	Inbound	1G	0.2%	2.01M	0.82%	8.15M
.25.158	Uplink (vSwitch0)	Inbound	1G	0.17%	1.68M	6.34%	63.36M
.0.249	ifIndex-13 (vSwitch0)	Outbound	1G	0.1%	1.01M	0.4%	4.02M
.0.249	ifIndex-14 (vSwitch0)	Outbound	1G	0.1%	968.1k	0.41%	4.12M
.0.43	eth3	Inbound	1G	0.08%	751.09k	0.34%	3.38M

3. Double-click the corresponding Interface cell to open the Interface Summary Dashboard for the identified interface to determine why there is so much traffic. Refer to "Finding High Bandwidth Hosts (Interface Summary Dashboard)" on page 172.

Network Slow

One of the most common user complaints is that the network is slow. The following diagram shows a workflow you can use to help pinpoint the source of the problem.



Workflow Overview

The following steps provide an overview of the procedures illustrated in the preceding workflow diagram.

1. Do you have the complaining user's IP address?
   - If yes, go to step 3.
   - If no, go to step 2.
2. Do you have a Stealthwatch IDentity appliance?

- If yes, use the User Identity filter to search for the user's IP address. Refer to the following section, "Using the Stealthwatch IDentity to Locate an IP Address."
- If no, use any tool (e.g., ipconfig) you have available to obtain the user's IP address.

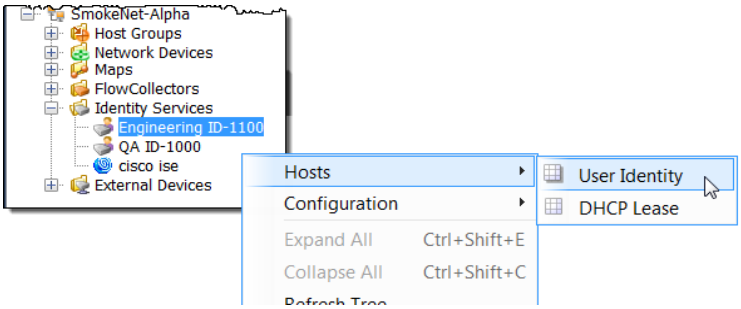
3. Open the Host Snapshot: Exporter Interfaces page for the user's IP address. Refer to "Checking for Over-Utilized Interfaces (Host Snapshot)" on page 170.
4. Are any interfaces over-utilized or close to capacity?
   - If yes, open the Interface Summary Dashboard for the over-utilized interface and look at the Top Active Conversations. Refer to "Finding High Bandwidth Hosts (Interface Summary Dashboard)" on page 172.
   - If no, go to step 8.
5. Note the IP addresses of the host pair (host and peer) consuming the most bandwidth.
6. Based on which host pair interests you the most, open the Host Snapshot: Identity, DHCP & Host Notes page for either the host or the peer to try to identify the user(s) logged in to that IP address. Refer to "Identifying Users Logged In to a High Bandwidth Host" on page 172.
7. Can you identify the user(s)?
   - If yes, obtain the user's IP address and go to step 8.
   - If no, go to step 10.
8. Open the associated Host Snapshot: Top Active Flows page and review the details of the flows associated with the user to potentially determine the cause of the issue. Refer to "Reviewing Top Active Flows" on page 173.
9. Were you able to resolve the issue?
   - If yes, stop here.
   - If no, go to step 10.
10. Gather the information you have collected thus far and escalate according to your organization's standard escalation procedure.

Using the Stealthwatch IDentity to Locate an IP Address

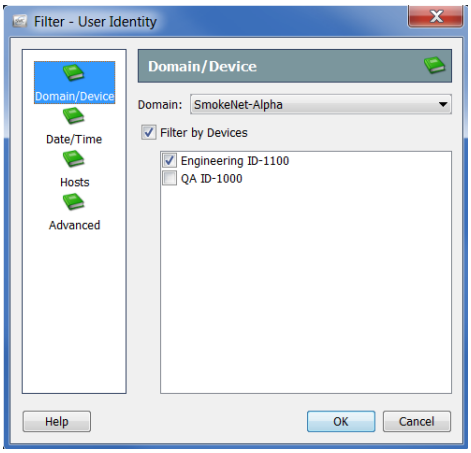
If you have a Stealthwatch IDentity appliance, complete the following steps to quickly locate the IP address(es) that a specific user is using or has used.

1. In the Enterprise tree, expand the Identity Services branch and locate the IDentity appliance you want to use.

2. Right-click the IDentity appliance and select **Hosts > User Identity**.



The Filter dialog: User Identity page opens. The domain and device you chose are automatically selected on the Domain/Device page.

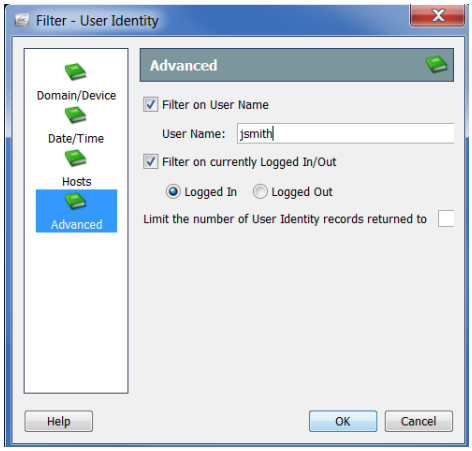


Notes:

- The filter opens to the last page you viewed the last time you closed the filter. If you have never opened the filter, it will open to the Domain/Device page.
- To look through all IDentity appliances for the user's IP address, click the **Filter by Devices** check box on the Domain/Device page to remove the check mark.

3. Click the **Advanced** button. The Advanced page opens.

4. Click the **Filter on User Name** check box to add a check mark, and then type the user's login name in the User Name field.



5. By default, the filter looks only for the IP addresses of users who are logged in at the time of the query, as indicated by the selected **Filter on currently Logged In/Out** options.

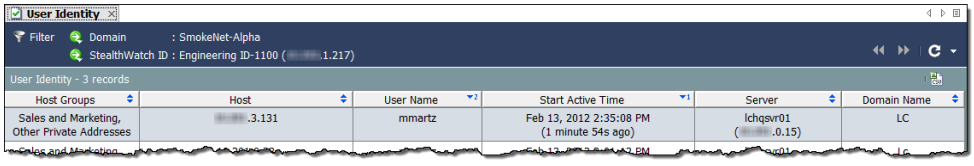
   To search for IP addresses that a user was logged in to at other times, click the **Filter on currently Logged In/Out** check box to remove the check mark, and then go to the Date/Time page of the filter to specify the time frame in question.

6. If desired, change the number of records that display by typing over the value in the **Limit the number of User Identity records returned to** field.

Note:

For troubleshooting the type of issue described in this section, you generally do not need to define any other parameters in the filter. If you need additional assistance, refer to the *Stealthwatch Desktop Client Online Help*.

7. Click **OK**. The User Identity document opens, displaying the IP addresses associated with the specified user name.



Tip:

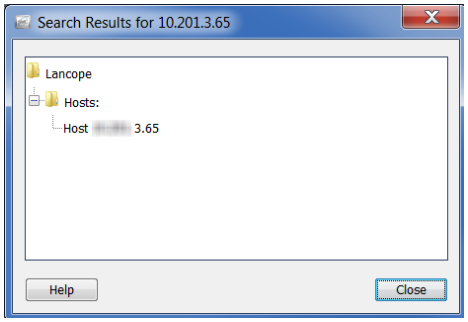
Double-click the IP address to open the associated Host Snapshot.

Checking for Over-Utilized Interfaces (Host Snapshot)

Complete the following steps to open the Host Snapshot: Exporter Interfaces tab for a particular IP address to see if any interfaces are overloaded.

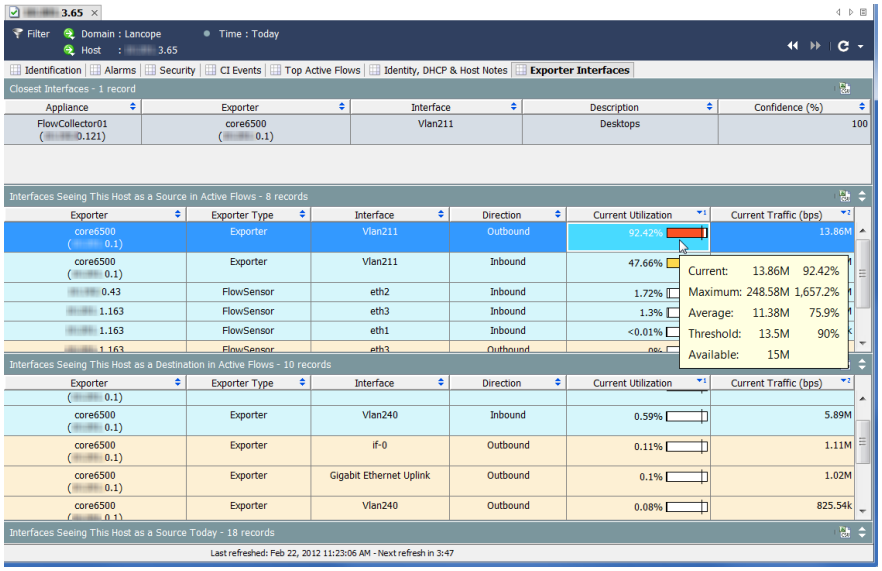
1. Did you use the User Identity document to locate the IP address?
   - If yes, double-click the IP address to open the Host Snapshot, and then go to step 4.
   - If no, go to step 2.

2. In the SMC tool bar, type the IP address in the Global Search field, and then press **Enter**. The Search Results dialog displays a list of each location where that address appears in the SMC, as shown in the example to the right.



3. Double-click the host IP address entry.

4. When the Host Snapshot opens, click the **Exporter Interfaces** tab.



Tip:

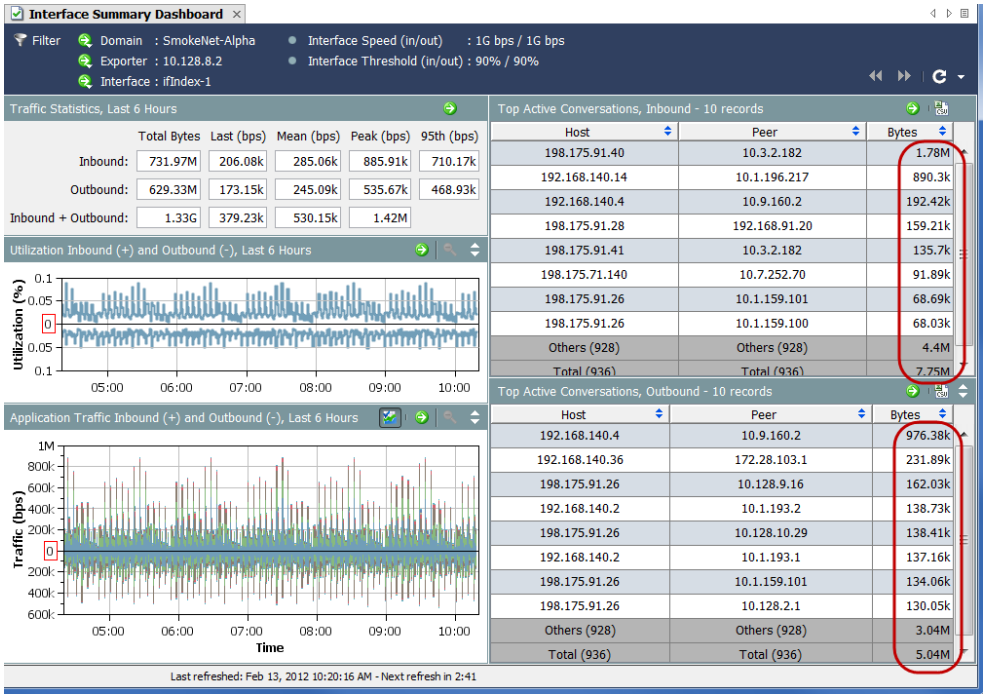
Hover the cursor over a value in the Current Utilization column to see capacity availability and usage details for the associated interface.

5. Are any interfaces overloaded or close to capacity? (**Hint:** Look for red, orange, or yellow bars in the Current Utilization column.)

   - If yes, open the Interface Summary Dashboard for the overloaded interface to determine why there is so much traffic. Refer to the following section, "Finding High Bandwidth Hosts (Interface Summary Dashboard)."
   - If no, click the **Top Active Flows** tab on the Host Snapshot and review the details of the flows associated with the user to potentially determine the cause of the issue. Refer to "Reviewing Top Active Flows" on page 173.

Finding High Bandwidth Hosts (Interface Summary Dashboard)

When you are looking at the Exporter Interfaces tab in the Interface Summary, and you see an interface (in the Interface column) that is overloaded or close to capacity, double-click it to open the associated Interface Summary Dashboard.



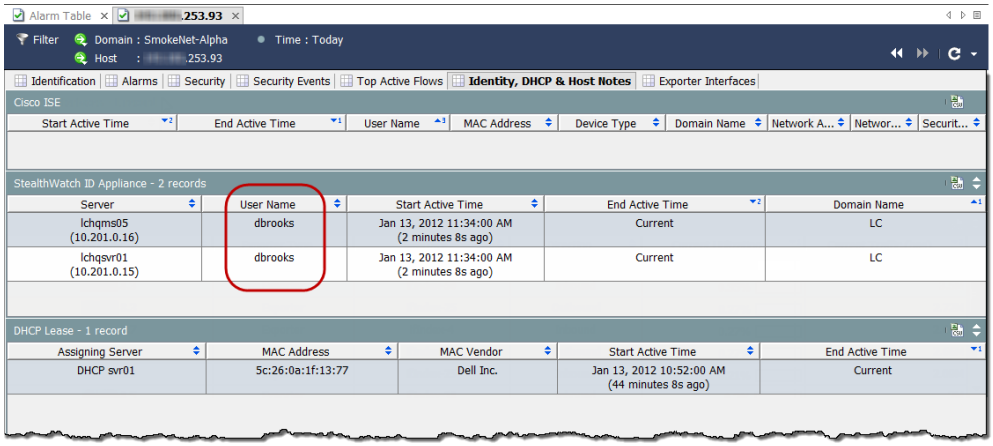
Look at the right side of the dashboard to see the Top Active Conversations Inbound and Outbound. Identify the host pairs (host and peer) that are using the most bandwidth (see the Bytes column) in either direction.

To identify the users logged in to each of those IP addresses, open the Host Snapshot: Identity, DHCP & Host Notes tab for each IP address. Refer to "Identifying Users Logged In to a High Bandwidth Host" on page 172.

Identifying Users Logged In to a High Bandwidth Host

Once you have the IP address for a host and/or peer that is using excessive bandwidth, open the Host Snapshot for that address, and then click the **Identity, DHCP & Host Notes** tab.

If login information is available, you will see the user name for any user logged in to that IP address.



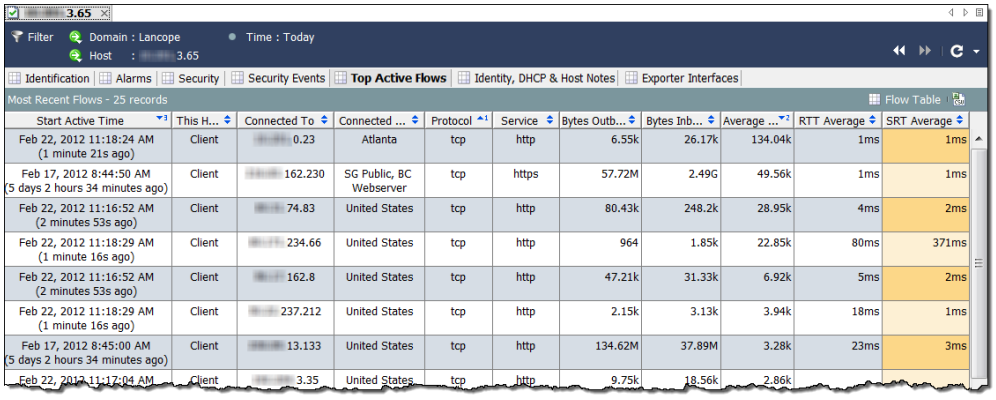
If no user information is available, gather the information you have collected thus far and escalate according to your organization's standard escalation procedure.

Tip:

If you have a Stealthwatch IDentity appliance, you can double-click the user name to open the User Identity document and to see the IP addresses associated with that user.

Reviewing Top Active Flows

The Top Active Flows tab of the Host Snapshot provides details about the 25 most recent flows per Stealthwatch appliance and about the 25 flows with the highest traffic per appliance.



First, look at the RTT and SRT values. If the SRT is unacceptably high, you know that the problem lies with the server, and you can then contact the server team to resolve the problem.

If the SRT value is fine, the issue lies somewhere in the network, most likely with the host itself. Review the following questions as you look at the Top Active Flows tab. The answers may help you determine if the host has been hijacked or infected with malware, or if the user is engaging in unauthorized activity.

1. Are there any unexpected connections (e.g., unauthorized host groups or servers)?
2. Are there a large number of unexpected connections?
3. What services are being used?
4. Are there large amounts of traffic being sent and/or received?
5. Are there any connections with high bps rates?
6. Has the host changed roles from being a client to being a server? If a workstation suddenly starts running as a server, most likely it is infected with malware or has been hijacked.

If you are unable to resolve the issue based on the answers to the previous questions, complete the following steps:

1. Make sure the host's antivirus program or firewall isn't blocking access to the server in question.
2. Because the host's antivirus program may have failed to detect malware and may be compromised, run a virus scan on the host using another antivirus program, such as Malwarebytes' Anti-Malware.
3. Find out if any new applications have been installed or updated on the host. If so, verify that the application has been properly configured. You may need to uninstall the application, and then reinstall it.

If you are unable to resolve the issue using these suggestions, gather the information you have collected thus far and escalate according to your organization's standard escalation procedure.

EXTERNAL LOOKUP

The External Lookup feature allows you to launch a Web application (or internal asset database) to view additional information about an IP address. You can launch this Web application or database directly from the Stealthwatch Desktop Client or the Stealthwatch Web App.

You can also use the External Lookup feature to create shortcuts that enable you to jump quickly from the Stealthwatch Desktop Client to the Stealthwatch Web App.

Stealthwatch includes the following default Web applications (lookup options) for use with the External Lookup feature; you do not have to add them to Stealthwatch:

- Cisco SenderBase
- DShield
- Host Report

Some examples of Web applications that a Stealthwatch administrator can add to view additional information about an IP address include the following:

- BigFix
- CiscoWorks
- Cisco Identity Services Engine (ISE)
- Splunk
- Tripwire
- Ziften

Important:

To add a non-default lookup option, you must use the External Lookup Configuration tool in the Stealthwatch Web App. For information about how to do this, refer to "Configuring External Lookup."

Configuring External Lookup

As mentioned previously, Cisco SenderBase, DShield and Host Name are included by default for use with the External Lookup feature; you do not have to add them to Stealthwatch. To use any other Web application with this feature, you must add it to

Stealthwatch. To do this, use the External Lookup Configuration tool in the Stealthwatch Web App.

Notes:

When upgrading to v6.7, for each external lookup option that you previously added, you will now have two in v6.7.

Stealthwatch no longer uses webLinks.xml files to manage external lookup configuration.

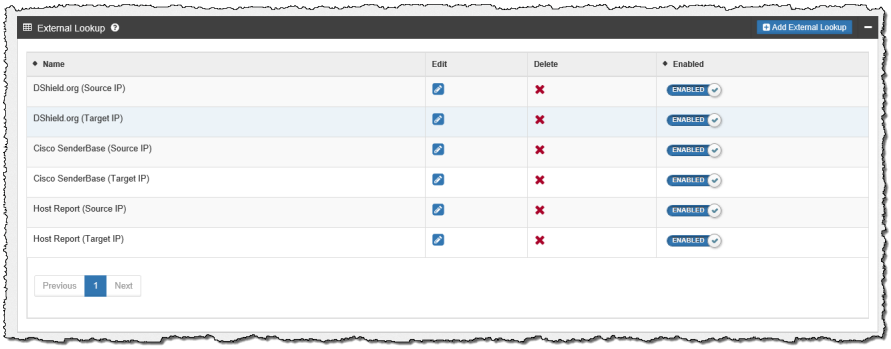
With this tool you can also configure the specific parameters that you want to send to a Web application. The parameters you configure are only sent if they are available for the IP address on which you are performing the lookup.

To add a lookup option and configure the parameters that you want to send to the Web application, complete the following steps:

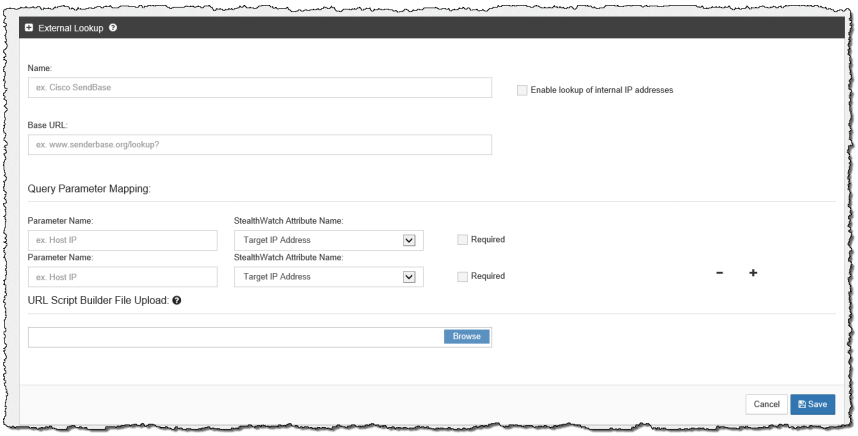
1. In the Stealthwatch Web App, in the left Navigation pane, click **Tools > Settings > External Lookup Configuration**. The External Lookup Configuration page opens.

   To disable a lookup option so that it is not available for use with the External Lookup feature (but to retain its configuration for later use), click **Enabled** in the applicable row. The button toggles to show the status of *Disabled*.

   To enable this lookup option in the future, click **Disabled**. The button toggles to show the status of *Enabled*.



2. Click **Add External Lookup**. The External Lookup section opens.



3. In the top part of this section, type the applicable entries in the following fields:
   - Name
   - Base URL
4. To view information about internal IP addresses in a Web application, ensure you select the “Enable lookup of internal IP addresses” check box.
5. In the Query Parameter Mapping section, in the first Stealthwatch Attribute Name field, select **Source IP Address** or **Target IP Address**.

Important:

You must configure either a source IP address or target IP address for any lookup option that you add.

6. In the corresponding Parameter Name field, enter the Web application’s parameter name used to specify the IP address you selected in the previous step.
7. If desired, configure any of the additional parameters that you want sent to the Web application for the IP address on which you are performing a lookup.
   - Target IP Address
   - Target Port No.
   - Source IP Address
   - Source Port No.
   - Host Name
   - TimeStamp (UTC)
   - Transport Protocol
   - User

   To add additional parameters, click the plus (+) sign located at the end of the first configured row. To delete a configured row, click the minus (-) sign in the applicable row.

Note:

You can map up to 20 query parameters for each lookup option.

8. If you want a parameter to be required when performing a lookup using a specific Web application, select the Required check box. Every parameter you designate to be required for a specific Web application must be available for the IP address on which you are performing a lookup. If one or more of the required parameters are not available for the relevant IP address, that lookup option will not be enabled in the pop-up menu.

9. If your query parameters do not match the standard query parameters, then you must upload your customized script builder configuration into the URL Script Builder File Upload field.

Note:

Ensure you use the variables highlighted in the following script examples.

The script builder file contains the script that configures the query parameters into the URL format that the Web application requires in order to run a query.

If you do not upload a script builder file, Stealthwatch will use the default standard query parameters shown below.

```
BaseURL?[ParameterName1]=[ParameterValue1]&
ParameterName2]=[ParameterValue2]&
ParameterName3]=[ParameterValue3] (and so on for
each parameter you add)
```

URL and script examples

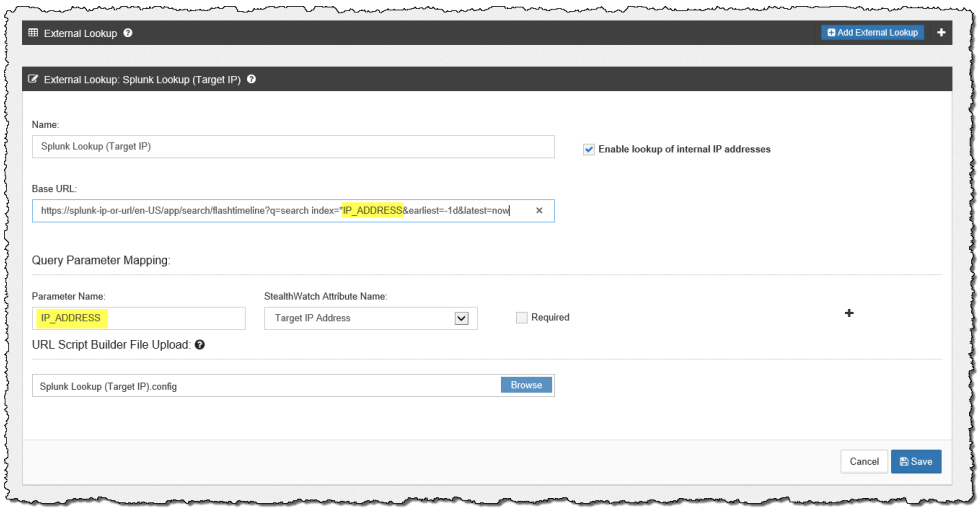
Example 1

The following URL and script example are used for Web applications that use values without parameter names (e.g., Splunk).

```
https://splunk-ip-or-url/en-US/app/search/flash-timeline
?q=search index=* 192.10.20.43 &earliest=-1d&lastest=now
```

```
def String query = baseUrl;
def String url = baseUrl;

vendorValues.each { valueOperand ->

    if (url.indexOf(valueOperand.getName()) != -1) {
        def String convertedStr = "";
        if (valueOperand.getFromValue() instanceof String || valueOperand.getFromValue() instanceof Integer) {
            convertedStr = valueOperand.getFromValue().toString();
        } else if (valueOperand.getFromValue() instanceof Date) {
            convertedStr = new SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss").format(valueOperand.getFromValue().time);
        }
        if (query.indexOf(valueOperand.getName()) != -1) {
            String[] parts = query.split(valueOperand.getName());
            query = "";
            def int i = 0;

            parts.each { part ->
                if (i + 1 < parts.length) {
                    query = query + part + URLEncoder.encode(convertedStr,"UTF-8");
                } else {
                    query = query + part;
                }

                i += 1;
            }

            if (url.endsWith(valueOperand.getName())) {
                query += URLEncoder.encode(convertedStr,"UTF-8");
            }
            url = query;
        }
    }
};

return query;
```

To build the script that configures the query parameters into the URL format shown previously in this example, use the Parameter Name field entry highlighted in the image below.



Note:

You can configure as many attributes as you need; however, ensure that you configure the same number of parameters.

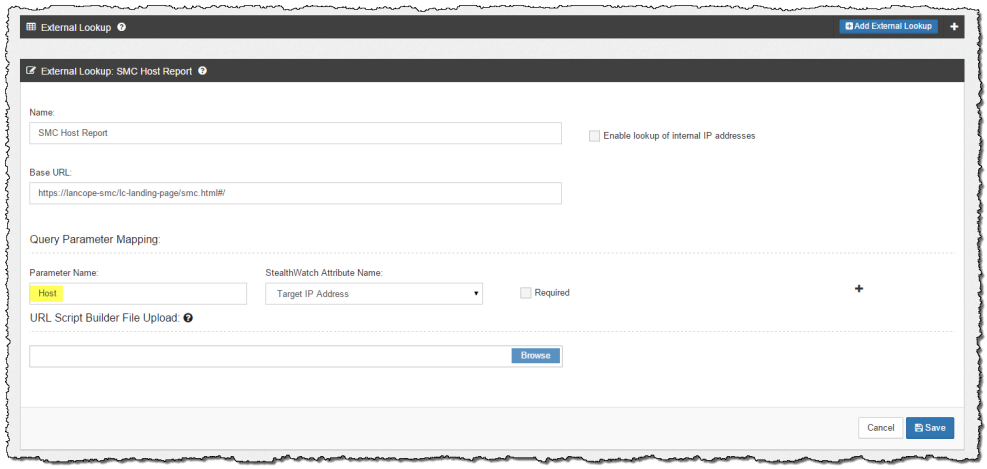
Example 2

The following URL and script example are used for Web applications that use rest-like path parameters (e.g., Stealthwatch Host Report).

```
https://lancope-smc/lc-landing-page/smc.html#/host
/172.21.114.17
```

```
def String query = "";

vendorValues.each { valueOperand ->


    query += valueOperand.getName() + "/";
    def String convertedStr = "";
    if (valueOperand.getFromValue() instanceof String || valueOperand.getFromValue() instanceof Integer) {
        convertedStr = valueOperand.getFromValue().toString();
    } else if (valueOperand.getFromValue() instanceof Date) {
        convertedStr = new SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss").format(valueOperand.getFromValue().time);
    }
    String.valueOf('java.lang.Integer');
    query += URLEncoder.encode(convertedStr,"UTF-8");
};

def char lastChar = baseUrl.charAt(baseUrl.length() - 1);
if (lastChar != '?' && lastChar != '/' && lastChar != '&') {
    baseUrl = baseUrl + "?";
};

query = baseUrl + query;
return query;
```

To build the script that configures the query parameters into the URL format shown previously in this example, use the Parameter Name field entry highlighted in the image below.

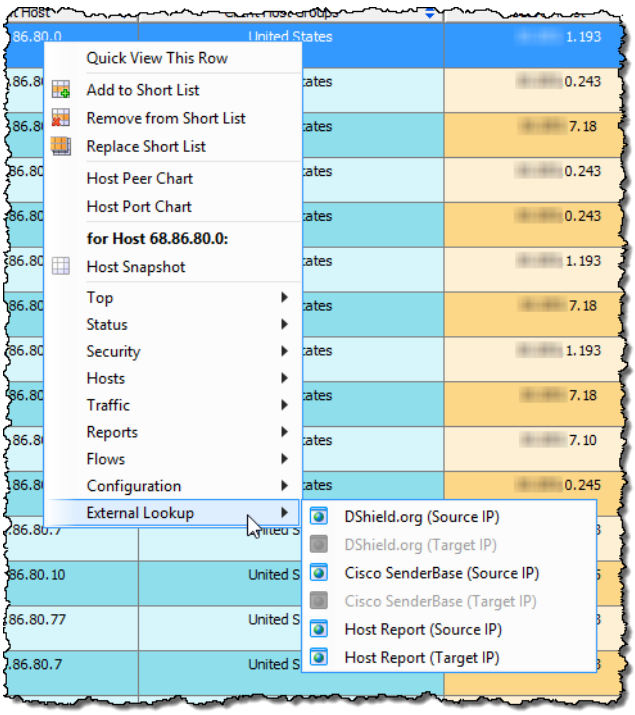


10. When you finish, click **Save**. You are returned to the External Lookup section. The lookup option you just added is now displayed on the list and is enabled by default (it is available for use with the External Lookup feature).

Performing an External Lookup

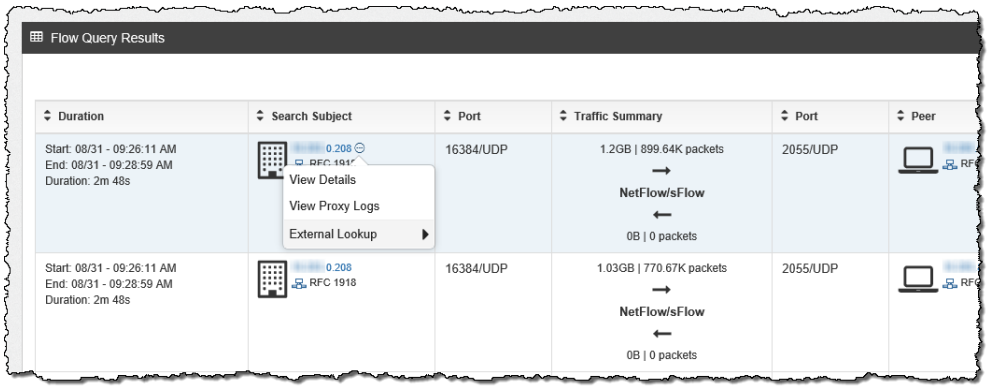
To query a Web application to view additional information about an IP address, complete the following steps:

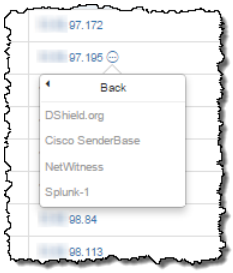
1. Do one of the following:
   - If you are in the Stealthwatch Desktop Client, go to step 2.
   - If you are in the Stealthwatch Web App, go to step 3.
2. Complete the following steps:
   a. In the Stealthwatch Desktop Client, open any document that contains the relevant IP address.
   b. Right-click the IP address.
   c. In the pop-up menu that appears, click **External Lookup**. A secondary pop-up menu appears.



3. Complete the following steps:
   a. In the Stealthwatch Web App, open either the Standard Flow Query Results page or the Advanced Flow Query Results page.
   b. In either the Search Subject column or Peer column, hover over the IP address and click the ellipsis.

c. In the pop-up menu that appears, click **External Lookup**. A secondary pop-up menu appears.

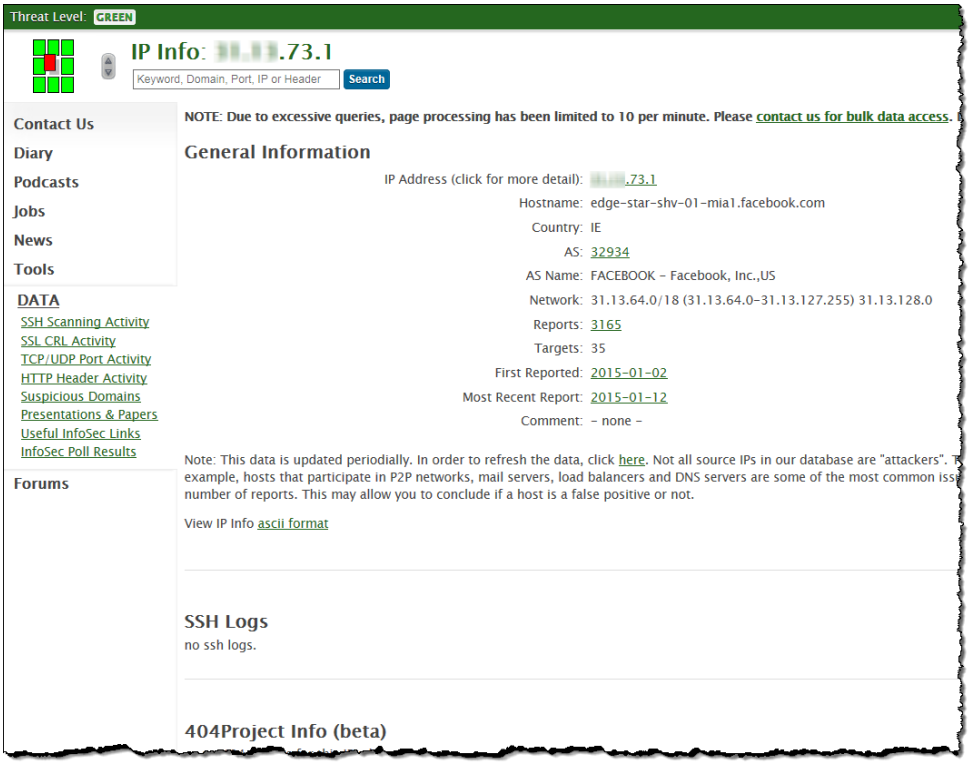




4. Click the desired lookup option from the secondary pop-up menu shown in step 3. The Web application for the lookup option you selected opens (you may be prompted to log in to the Web application) and displays the query results for the IP address on which you are performing the lookup.

   Every parameter you designate to be required for a specific Web application must be available for the IP address on which you are performing a lookup. If one or more of the required parameters are not available for the relevant IP address, that lookup option will not be enabled in the pop-up menu. For more information, refer to “Configuring Vendors” on page 194.

Following is an example of the information returned for a query using the DShield Web application.



8

STEALTHWATCH THREAT INTELLIGENCE FEED

OVERVIEW

Stealthwatch Threat Intelligence Feed (formally Stealthwatch Labs Intelligence Center, or SLIC) is a service from Cicso that delivers frequently updated information from the global threat intelligence feed about threats to your network. Stealthwatch Threat Intelligence Feed provides data about malware Command and Control (C&C) servers and other hosts of interest (e.g., bogons, Tor) that Stealthwatch uses to rapidly and accurately identify harmful network activity.

This chapter includes the following topics:

- About Threat Intelligence Feed
- How Threat Intelligence Feed Functions
- Enabling Threat Intelligence Feed
- Threat Intelligence Security Events

© 2017 Cisco Systems, Inc. All Rights Reserved.

About Threat Intelligence Feed

The icon in the Enterprise tree (which still contains the former name of Stealthwatch Labs Intelligence Center, or SLIC) changes color depending on if Threat Intelligence Feed is enabled and if there are any active alarms. Refer to the following list for guidelines:

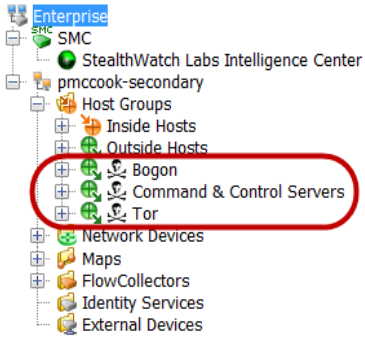
- If Threat Intelligence Feed is disabled, the SLIC icon is gray. (In the image on the right, the icon is shown in the disabled mode.)
- If Threat Intelligence Feed is enabled and there are no active alarms, the SLIC icon is green.
- If Threat Intelligence Feed is enabled and there is a SLIC Channel Down alarm, the SLIC icon is gray, and displayed at the bottom of this icon is a white X against a red background.
- If any alarms other than the SLIC Channel Down alarm exist, the icon's color corresponds to the highest alarm severity.

© 2017 Cisco Systems, Inc. All Rights Reserved.

How Threat Intelligence Feed Functions

Following is the order of events that occur when you enable Threat Intelligence Feed:

1. Threat Intelligence Feed downloads to the SMC the list of identified threats. These are displayed within their respective host group branches in the Enterprise tree, as shown in the image on the right.



2. The SMC distributes this list to each Flow Collector in your system.
3. The Flow Collectors use this information as they monitor the hosts in your network.
4. If the Flow Collectors detect a host in your network communicating with a threat host in Threat Intelligence Feed, a security event is triggered.

Note:

For information about the alarms these security events can trigger (if configured to do so) and the conditions that must exist before each one is raised, refer to "Threat Intelligence Security Events" on page 190.

5. If Threat Intelligence Feed has been enabled in the SMC, but the SMC server is not able to retrieve data from Threat Intelligence Feed, the SLIC Channel Down alarm is triggered. The SLIC icon in the Enterprise tree turns gray and an X appears at the bottom of the icon.

   This alarm clears when either of the following two conditions is true:

   - The SMC server begins retrieving data from Threat Intelligence Feed again.
   - You disable Threat Intelligence Feed.

Threat Intelligence Feed Host Groups

Note:

Host group branches within the Stealthwatch Labs Intelligence Center branch cannot be renamed, changed, moved, or deleted.

These host groups IP addresses, port numbers, protocols, host names, and URLs known to be used for malicious activity. The following host groups are included in Threat Intelligence Feed:

© 2017 Cisco Systems, Inc. All Rights Reserved.

- Bogon - A bogon is an IP address that has not been officially assigned on the public Internet.
- Command & Control Servers - A C&C server is the centralized computer that issues commands to a botnet and receives reports back from the hijacked computers.
- Tor - Tor is an Internet anonymization service.

Note:

To detect URLs in Threat Intelligence Feed that may be contacting your hosts, you must have a FlowSensor or router installed that is configured to export IPFIX (vs. NetFlow). (By default, the FlowSensor is configured to export IPFIX.).

If you want to investigate a host that has communicated with a malicious host in one of the previously mentioned host groups, but the malicious host no longer appears in the relevant host group, go to the Alarm Table and filter on the following components:

- Types - Select the applicable bogon, Command & Control, or Tor alarm(s), depending on which type of malicious host(s) you are wanting to filter on.
- Date/Time - Filter according to the time period for which you want to investigate.

© 2017 Cisco Systems, Inc. All Rights Reserved.

ENABLING THREAT INTELLIGENCE FEED

For information about how to enable Threat Intelligence Feed, refer to the “Threat Intelligence Feed Configuration” topic in the Stealthwatch Desktop Client online help.

© 2017 Cisco Systems, Inc. All Rights Reserved.

THREAT INTELLIGENCE SECURITY EVENTS

This section describes the security events that can be triggered by threat hosts that are in the Threat Intelligence Feed. Each of these security events will trigger an alarm in the SMC client interface if configured to do so. (They can be configured in the Host Policy Manager in the Stealthwatch Desktop Client.) Once triggered, they are displayed in the Alarm Table in the Stealthwatch Desktop Client.

Depending on what the Flow Collectors detect and the configuration of the SMC, the following security events can trigger alarms:

Security Events	Description
Bot Infected Host – Attempted C&C Activity	This alarm indicates that a host in your network has tried to communicate with a C&C server that appears on the C&C Servers list, and is therefore now a member of a botnet. Communication is one-way only. The inside host, as the initiator, accumulates Concern Index (CI) points. If the C&C server it attempts to contact is also an inside host, then that C&C server accumulates Target Index (TI) points. For more information about these indexes, refer to Chapter 6, “Indexes: Ranking Behavior Changes.”
Bot Infected Host – Successful C&C Activity	This alarm indicates that a host in your network has communicated with a C&C server that appears on the C&C Servers list, has received a response, and is therefore now a member of a botnet. The C&C server may be either inside or outside of your network. Communication is two-way. The inside host, as the initiator, accumulates CI points. If the C&C server it contacts is also an inside host, then that C&C server accumulates TI points.
Bot Command & Control Server	This alarm indicates that a host inside your network is functioning as a C&C server of a botnet. This alarm is triggered when an inside host on your network matches an IP address that the SLIC Threat Feed has identified as a C&C server. This alarm identifies only the source IP address. Targets are not identified.
Connection from Bogon Address Attempted	Looks for instances of an outside Bogon host unsuccessfully attempting to communicate with a host server inside your network. A Bogon prefix is a route that should not appear in the Internet routing table.
Connection From Bogon Address Successful	Looks for instances of an outside Bogon host, acting as a client, that successfully communicates with a host server inside your network. A Bogon prefix is a route that should not appear in the Internet routing table.

© 2017 Cisco Systems, Inc. All Rights Reserved.

Security Events	Description
Connection from Tor Attempted	Someone has unsuccessfully attempted to connect with you from a current Tor network exit node. Tor is an Internet anonymization service.
Connection from Tor Successful	One or more of the hosts on your network are receiving traffic from a current Tor network exit node. Tor is an Internet anonymization service.
Connection To Bogon Address Attempted	Looks for instances of a host inside your network unsuccessfully attempting to communicate with an outside Bogon host. A Bogon prefix is a route that should not appear in the Internet routing table.
Connection To Bogon Address Successful	Looks for instances of bidirectional traffic between a host inside your network and an outside Bogon IP address, which is one that has not been assigned on the public Internet, and alerts you that communication has occurred. A Bogon prefix is a route that should not appear in the Internet routing table.
Connection to Tor Attempted	One of your active inside hosts has unsuccessfully attempted to connect to a current Tor network entry node. Tor is an Internet anonymization service.
Connection to Tor Successful	One or more of the hosts on your network are sending traffic to the Tor network. Tor is an Internet anonymization service.
Inside Tor Entry Detected	One of your active inside hosts is acting as a Tor entry node. Tor is an Internet anonymization service.
Inside Tor Exit Detected	One of your active inside hosts is acting as a Tor exit node. Tor is an Internet anonymization service.

Note:

For additional information about these alarms, refer to the “Security Event List” topic in the *Stealthwatch Web App online help*.

© 2017 Cisco Systems, Inc. All Rights Reserved.

© 2017 Cisco Systems, Inc. All Rights Reserved.

9

FINDING THE CULPRIT

OVERVIEW

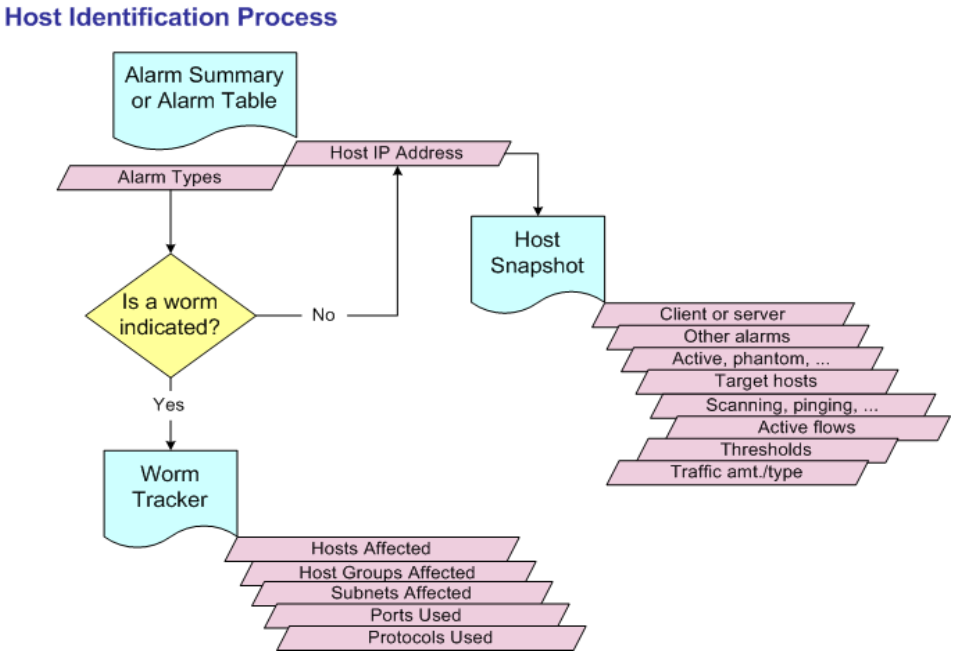
As you have learned, the first step in handling a threat is to find out which host is causing the alarm (i.e., the "source host"). This chapter describes how you can use the SMC to gather information about the source host so that you can make an informed decision as to how to handle the threat.

This chapter includes the following topics:

- Identification Process
- Alarm Summary
- Alarm Table
- Global Search
- Getting Details from the Host Snapshot
- Is the Behavior Normal?
- Which Hosts Share the Same Characteristics?

IDENTIFICATION PROCESS

Sometimes, assessing what to do about an alarm condition is as simple as locating the IP address of the source host. However, at other times you need more information about the host and the alarm as well. Either way, the Alarm Summary and the Alarm Table are instrumental in your assessment. The following diagram illustrates the process to follow when trying to identify a suspicious host:



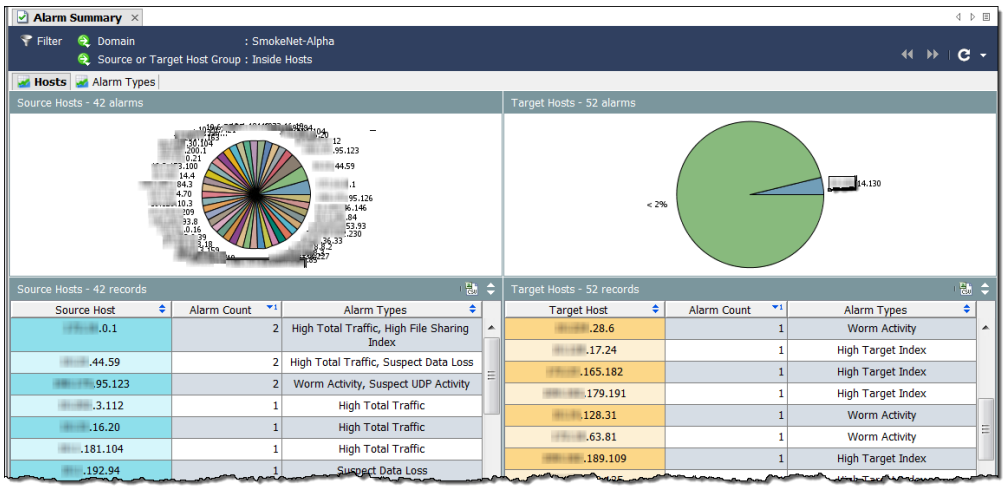
Note:

Keep a record of hosts that have caused trouble on your network so you can easily determine if you have a "repeat offender."

ALARM SUMMARY

Probably the simplest way to identify the host is to use the Alarm Summary. To open this document, right-click a domain, exporter, or FlowSensor, and then select **Status > Alarm Summary** from the pop-up menu.

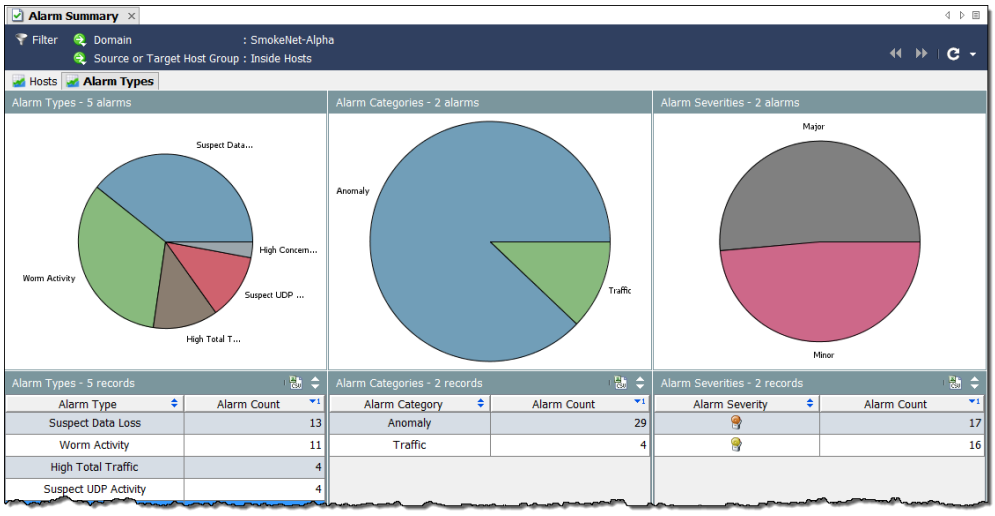
Here, you can see graphical representations of all alarms on the network broken down by types, categories, severity levels, source host IP addresses, and target host IP addresses. In the following example, you can easily see the source host IP address on the Hosts tab.



To navigate from this document, you can perform any of the following actions:

- To see the Host Snapshot, double-click a host IP address on the Hosts tab.
- To get a filtered view of the Alarm Table, double-click the **Alarm Count** or **Alarm Types** column.

Click the **Alarm Types** tab to see a different view.



To navigate from this document, you can perform any of the following actions:

- To get filtered views of the Alarm Table, double-click a chart or a table item on the Alarm Types tab.
- To display the Alarm Table pre-filtered to show only alarms associated with that item, double-click an item in one of the columns or pie charts.

  For example, if you double-click the **High Concern Index** alarm in the Alarm Types column, the Alarm Table will display only High Concern Index alarms.

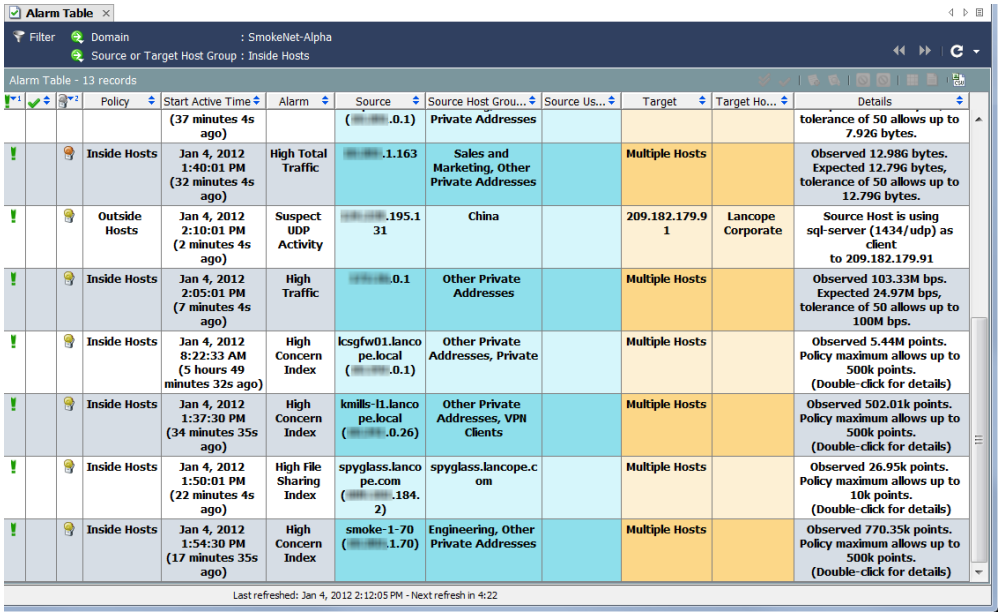
Note:

For a description of each alarm, refer to the *Stealthwatch Desktop Client Online Help*.

ALARM TABLE

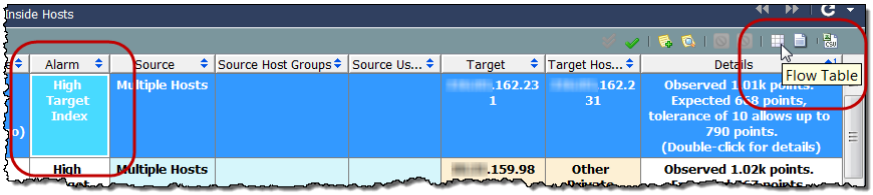
When you want detailed information about alarms, go to the Alarm Table. To open this document, right-click a domain, Stealthwatch Flow Collector, host group, exporter, or FlowSensor, and then select **Status > Alarm Table** from the pop-up menu.

The Alarm Table helps you answer these questions: “What is causing the alarm?” and “How serious is it?” By default, the Alarm Table displays all active alarms that have occurred since the last archive hour of the Stealthwatch Flow Collector(s) that generated them.



Like most SMC documents, the Alarm Table displays data that corresponds to the level at which you open the document. For example, if you open the Alarm Table at the domain level, the alarms it displays will pertain to the domain as a whole. If you open the Alarm Table at the host group level, the alarms it displays will pertain to only the host group and its sub-host groups.

In addition to viewing alarms, the Alarm Table allows you to acknowledge, close, and add notes to alarms (depending on your login privileges). You can click an alarm, and then click the **Flow Table** button to display the Flow Table with all the flows associated with that alarm.



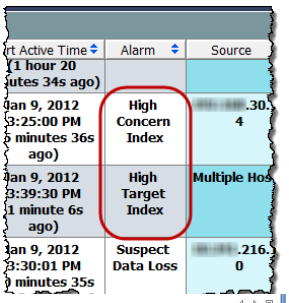
An alarm remains active until the condition that caused the alarm no longer exists. Then, the alarm becomes inactive, at which point you can close it, if desired. You can

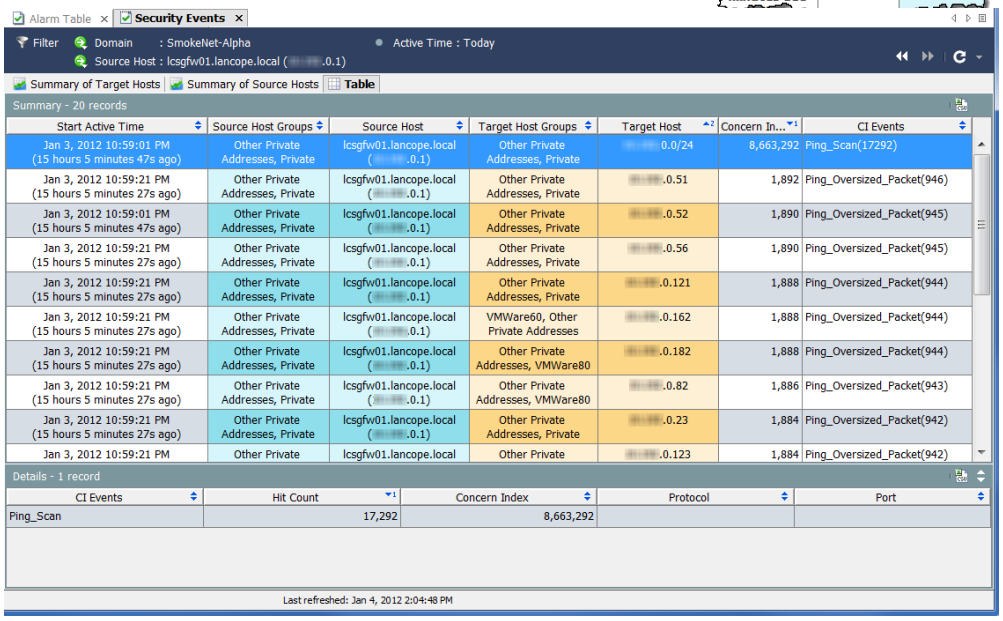
acknowledge an active alarm, but you cannot close it. You can close only inactive alarms.

Another advantage that the Alarm Table provides is that it allows you to perform the following actions:

- Acknowledge/unacknowledge alarms
- Append/view alarm notes
- Block or unblock a host (i.e., alarm mitigation)

If you double-click a High Concern Index alarm or a High Target Index alarm within the Alarm Table, the Security Events document will be displayed, as shown in the following example. This document displays data for Security Events that have caused the alarm.





Note:

For more information about responding to alarms, refer to Chapter 10, "Responding to Alarms."

GLOBAL SEARCH

The Global Search feature allows you to search through all of its documents (across all domains) for certain items. In the Search field in the Main Tool Bar, you can search for the following items using a full string, partial string, or partial string with wild card (*):

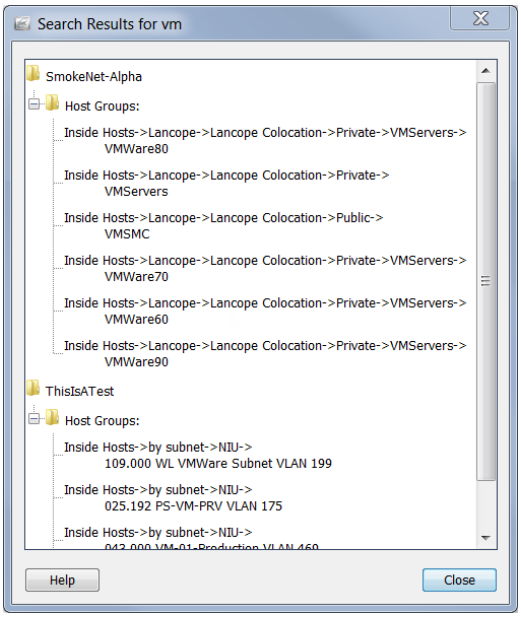
- Alarm ID
- Host or exporter IP address
- The following names:
  - Exporter
  - Host group
  - Server
  - User

Note:
The search results are limited according to the data role and functional role associated with your user name.

Tip:
You can use the Search drop-down list box to select an item that you have previously searched for and then press **Enter** to execute the search.

To perform a search, click inside the Global Search box in the tool bar.

Type a search item and press **Enter**. The Search Results dialog opens.

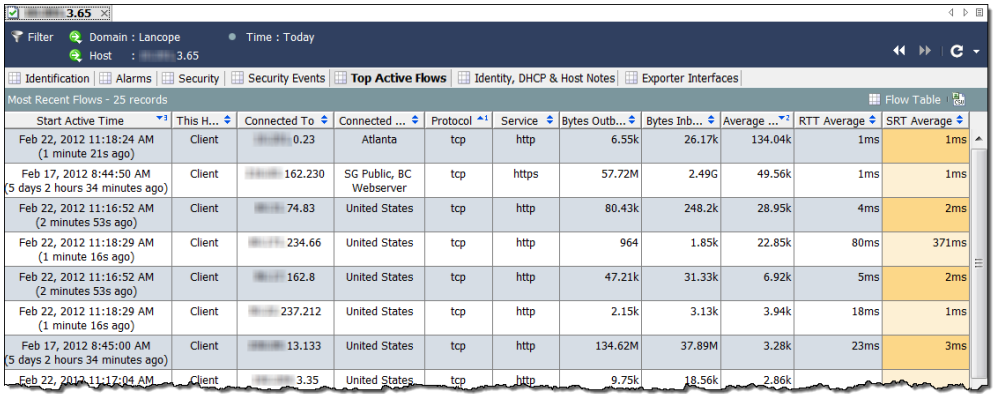


Do one of the following:

- Double-click the search result.
- Right-click the search result and select the desired item from the pop-up menu.

GETTING DETAILS FROM THE HOST SNAPSHOT

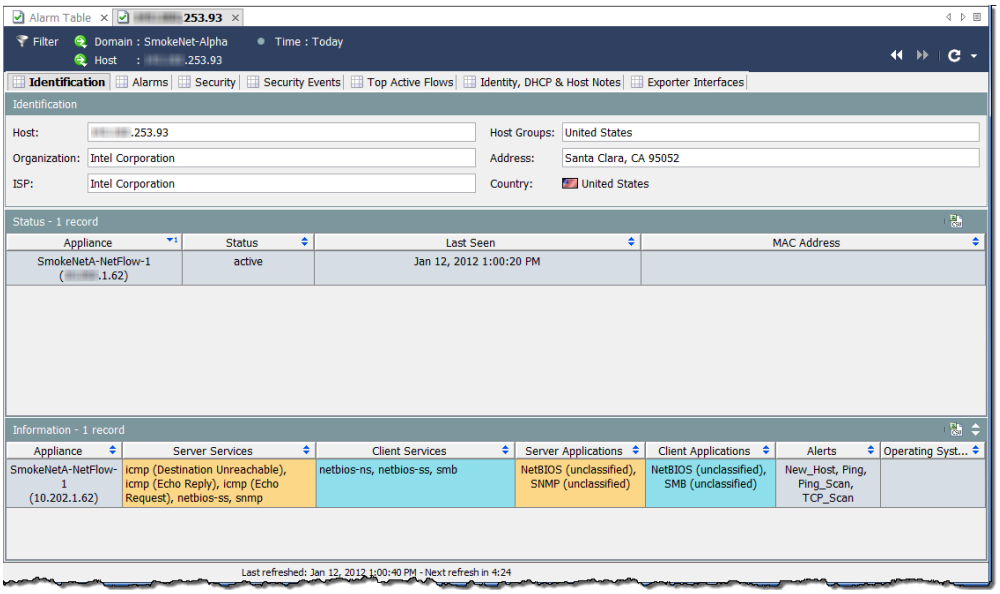
When investigating changes in host behavior, the Host Snapshot document is frequently your first stop. This document provides the most comprehensive information for each host in the network.



Start Active Time	This H...	Connected To	Connected ...	Protocol	Service	Bytes Outb...	Bytes Inb...	Average ...	RTT Average	SRT Average
Feb 22, 2012 11:18:24 AM (1 minute 21s ago)	Client	0.23	Atlanta	tcp	http	6.55k	26.17k	134.04k	1ms	1ms
Feb 17, 2012 8:44:50 AM (5 days 2 hours 34 minutes ago)	Client	162.230	SG Public, BC Webserver	tcp	https	57.72M	2.49G	49.56k	1ms	1ms
Feb 22, 2012 11:16:52 AM (2 minutes 53s ago)	Client	74.83	United States	tcp	http	80.43k	248.2k	28.95k	4ms	2ms
Feb 22, 2012 11:18:29 AM (1 minute 16s ago)	Client	234.66	United States	tcp	http	964	1.85k	22.85k	80ms	371ms
Feb 22, 2012 11:16:52 AM (2 minutes 53s ago)	Client	162.8	United States	tcp	http	47.21k	31.33k	6.92k	5ms	2ms
Feb 22, 2012 11:18:29 AM (1 minute 16s ago)	Client	237.212	United States	tcp	http	2.15k	3.13k	3.94k	18ms	1ms
Feb 17, 2012 8:45:00 AM (5 days 2 hours 34 minutes ago)	Client	13.133	United States	tcp	http	134.62M	37.89M	3.28k	23ms	3ms
Feb 22, 2012 11:17:04 AM	Client	3.35	United States	tcp	http	9.75k	18.56k	2.86k		

In most cases, you can simply double-click a host's IP address anywhere in the Stealthwatch Desktop Client to see the Host Snapshot for that host. The Host Snapshot includes the following information:

- The most recent flows associated with the host.
- The flows with the highest amount of traffic so far today.
- The username(s) of anyone who has logged into the host.
- Any alarms associated with the host.
- Which exporter interfaces are carrying the flow.
- The organization to which the host IP address is assigned, along with the address and Internet Service Provider (ISP), if applicable.
- The host's status and when it was last seen communicating on the network.
- The host's server/client profile(s) and operating system (OS), as well as any alerts associated with the host.

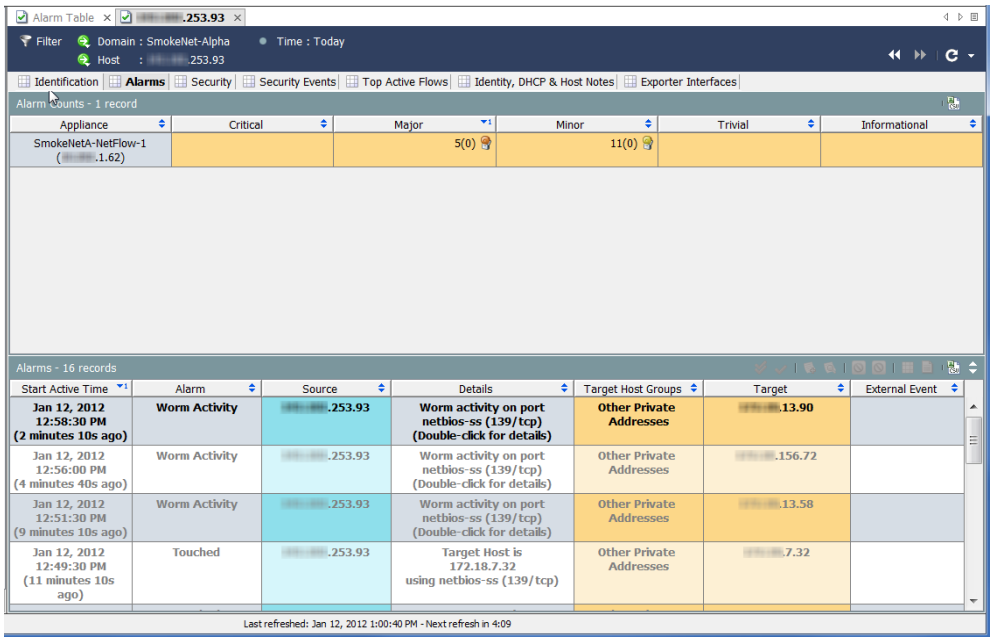


In the preceding example, we can see the following information about the selected host on the Identification tab:

- The host has a private IP address.
- The system last saw activity for this host on January 12, 2012.
- The system reported that, among many other services, netbios traffic occurred for the host as both a server and a client.

Has the Host Caused Other Alarms?

The Alarms tab on the Host Snapshot indicates if the host in question has generated other alarms, and if so, how many and what types.



The more alarms a host causes, the more concerned you should be. Remember, the level of severity is configurable so that it can adjust to your particular situation.

In the preceding example, we see the following information about the selected host:

- The Alarm Counts table displays the number of alarms caused by the selected host as reported by the corresponding Stealthwatch appliances, based on the alarm type and category. In this example, the Stealthwatch appliances reported 11 minor alarm conditions and 5 major alarm conditions.

Note:

You can right-click the column headings and select the columns for the specific alarm types you want to show in the table.

- The Alarms table displays detailed data about the individual alarms generated by the selected host since the last archive hour. In this case, we see that this host has generated several Worm Activity alarms.

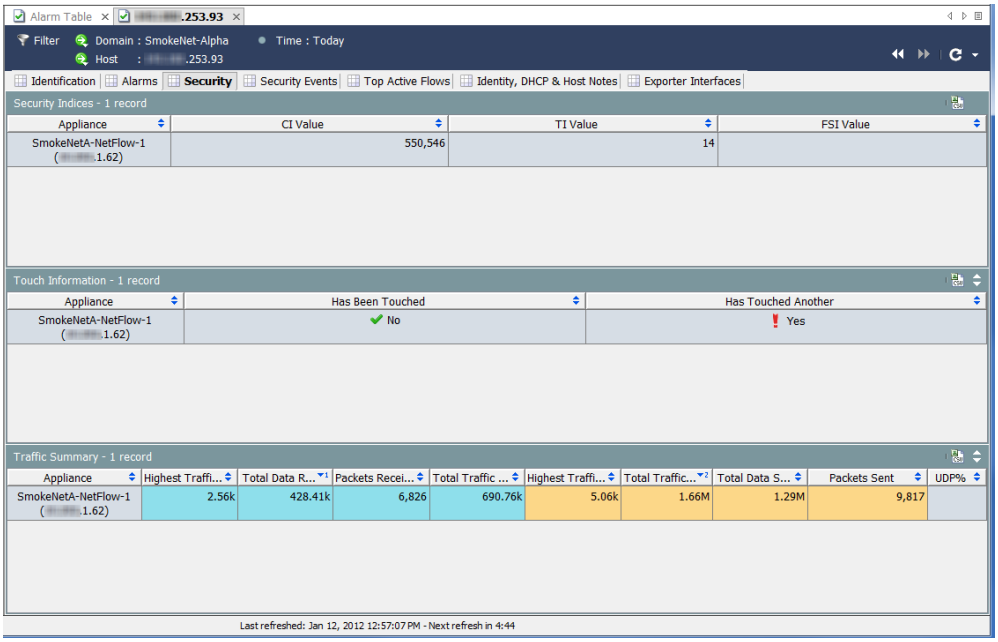
Note:

You can open the Host Policy Manager to see and/or adjust the policy settings established for these values.

Since we suspect that this host may be infected, our next step is to identify the source of the infection and to identify how many hosts are affected.

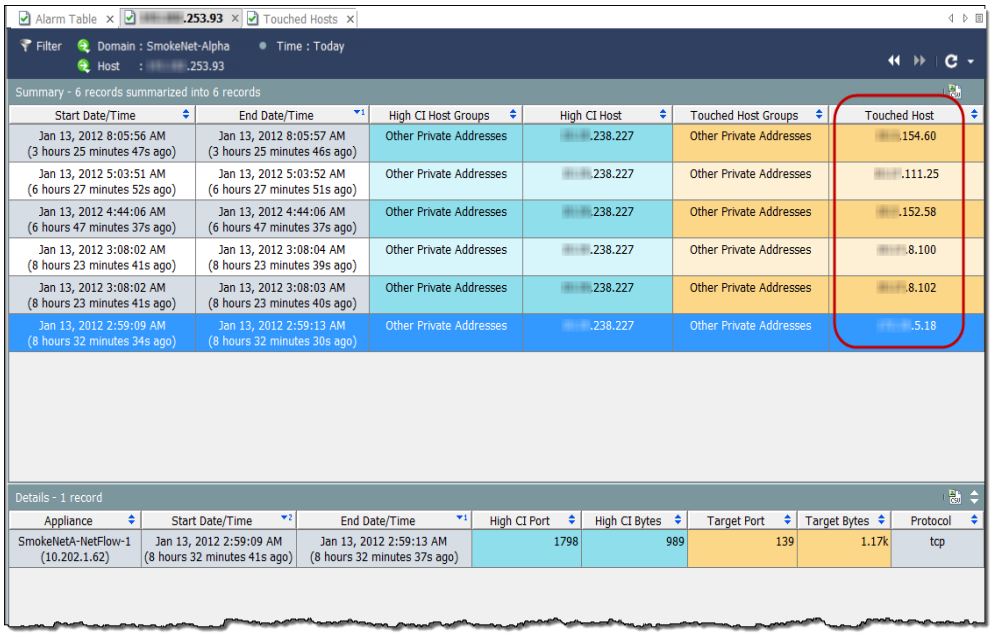
How Widespread is the Threat?

Whether or not a worm is indicated, you can go to the Security tab on the Host Snapshot, shown in the following example, to see if the host in question has touched, or has been touched by, other hosts. The Touch Information table helps you determine if the threat for this host originated somewhere else, as well as whether or not this host has spread the threat to other hosts.



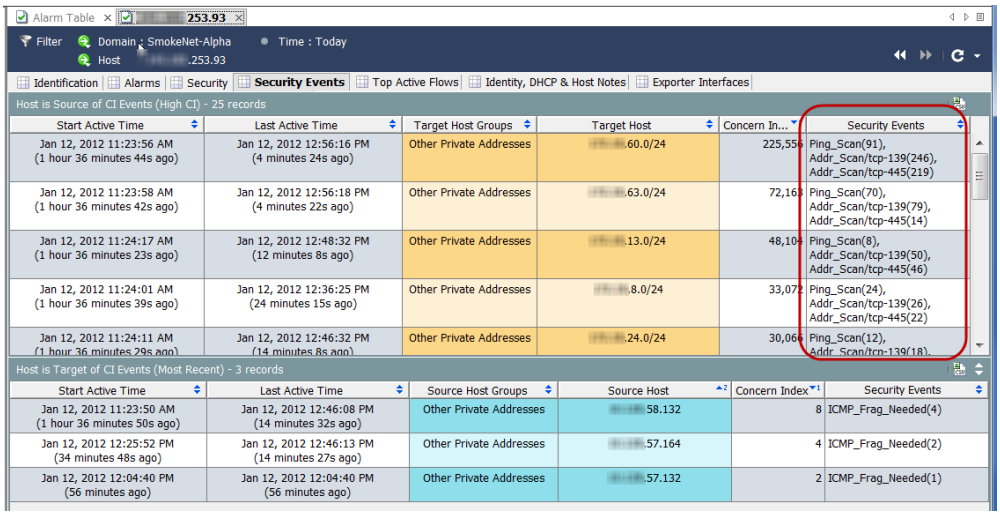
In addition, the Security Indices table shows how far beyond the limits this host has exceeded the various indices per Stealthwatch appliance. The Traffic Summary table shows you how much traffic this host is sending and/or receiving, which is helpful in determining file sharing activity.

In the preceding example, we need to see how many other hosts this host has touched. To do this, we go to the **Has Touched Another** column and double-click **Yes**. The Touched Hosts document opens. We can see in the Touched Host column that the High CI Host has touched a target host at least six times.

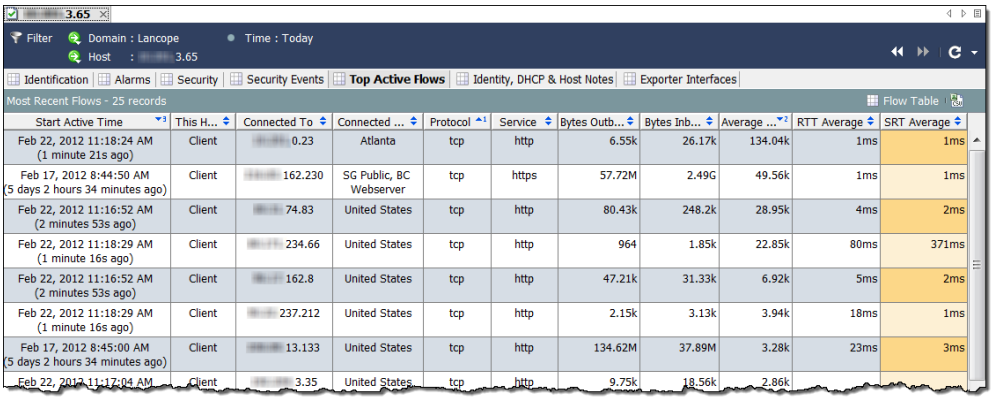


By selecting one of the rows in the previous table, you can see more detailed information in the Details section at the bottom, such as High CI port and bytes, the target port and bytes, and the protocol used for the affected host.

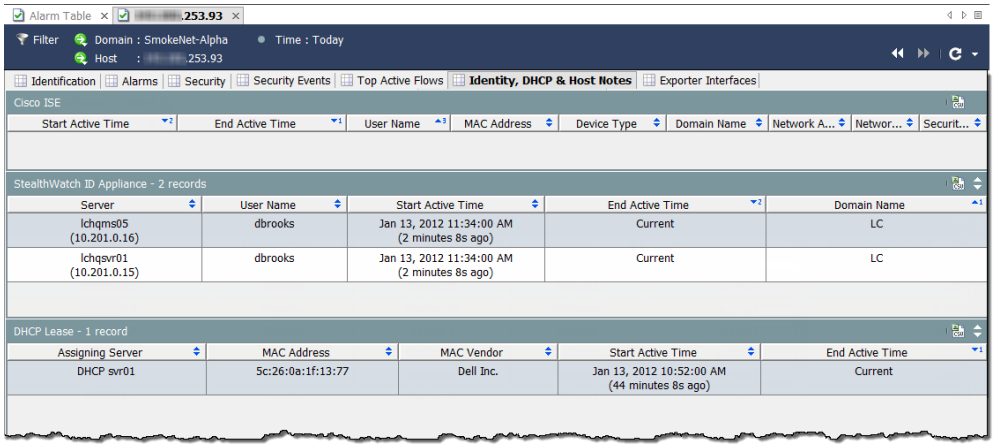
To see the type of Security Event, click the **Security Events** tab on the Host Snapshot. In our example, the types of Security Events are Address Scan and Ping Scan.



If you wish to view the top active flows for this host, click the **Top Active Flows** tab.



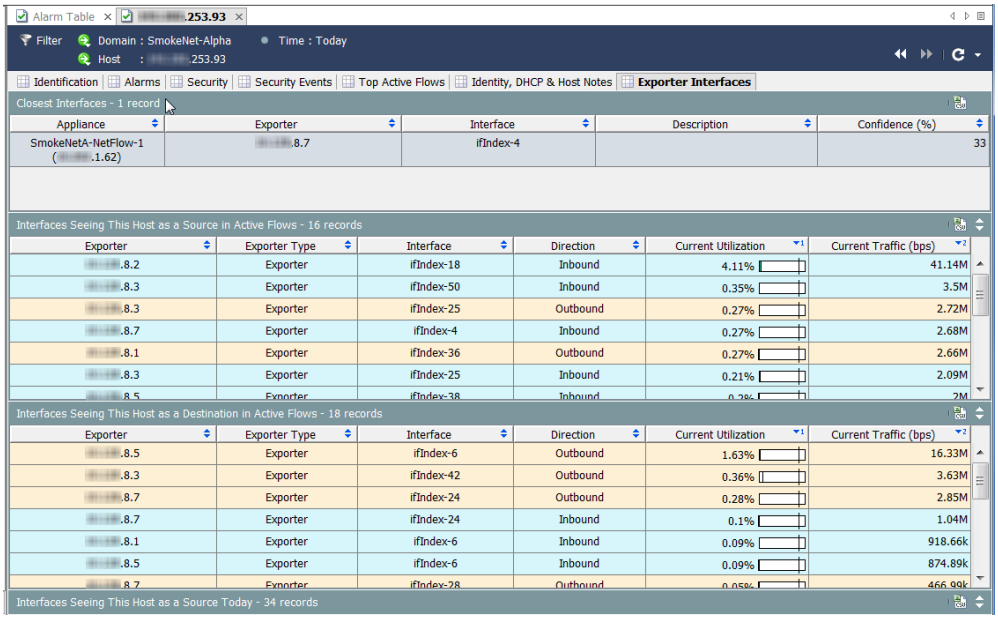
If you want to find out which user in your domain is associated with an IP address, click the **Identity, DHCP & Host Notes** tab.



Note:

You must have a Stealthwatch IDentity appliance or Cisco ISE appliance to get user identity data.

If you want to view additional information about the closest exporter and determine whether the host is seen as a source or a destination of active flows, click the **Exporter Interfaces** tab.



At this point, you have enough information to isolate both the source host and the target hosts. You can now begin the cleanup process per your organization's policies. For instance, you can perform any of the following actions:

- Run anti-virus software on each host.
- If all the hosts are in the same host group, you can block or isolate the whole host group.
- Block the ports on which the data is being exchanged.

IS THE BEHAVIOR NORMAL?

Up to this point, we've made the assumption that an alarm condition is the result of a threat. But, what if the behavior that caused the alarm is perfectly normal for the host in question?

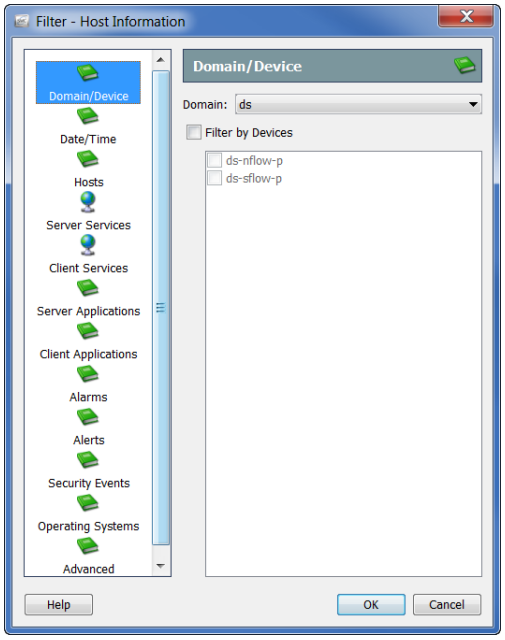
For example, an email server sees a lot of traffic, especially email traffic. However, if the parameters are set too low for that server, you will see multiple mail and/or traffic alarms against that server. The solution in this case is simply to set the parameters higher to a more realistic limit, thereby decreasing the number of unnecessary alarms you see. In other cases, you may have to edit the policy.

Note:

For information about adjusting parameters and editing policies, refer to Chapter 10, "Responding to Alarms."

WHICH HOSTS SHARE THE SAME CHARACTERISTICS?

If you want to see all of the hosts that are causing a particular alarm, using a particular service, or sharing other common characteristics, you can use the Host Information filter. To access this filter, from the Main Menu select **Hosts > Host Information**.

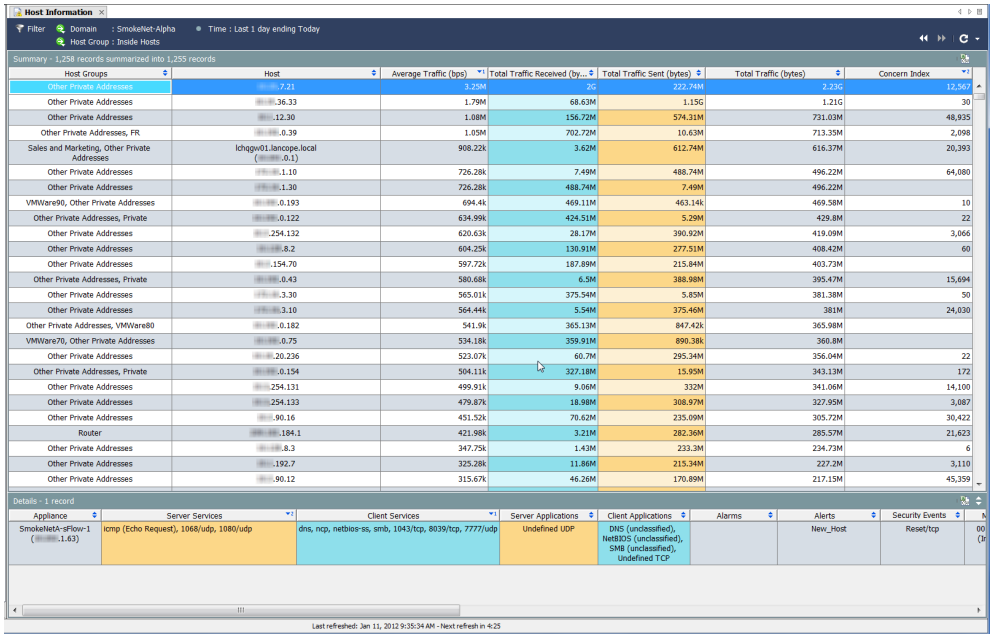


The Filter - Host Information dialog allows you to choose specific parameters to query against for all hosts that fit within those parameters. For example, you can filter for all hosts in a particular host group that are using a disallowed service or application, or that are causing Worm Activity alarms.

Note:

Because you are performing an information query (IQ), this process is sometimes called “performing a host IQ.”

After you specified the desired parameters, click **OK** to display the Host Information document (i.e., the Host IQ) with the requested data.



Note:

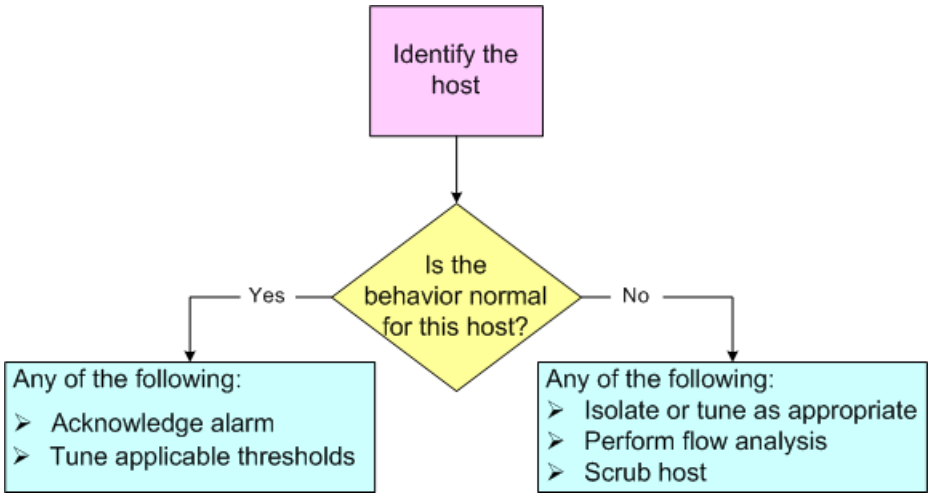
If you filter for all hosts causing High Concern Index alarms as well as TCP_Scan alerts, the result will contain a list of hosts that are most likely infected in some way.

10

RESPONDING TO ALARMS

OVERVIEW

The following diagram illustrates the basic steps to follow when addressing a threat to your network.



As you can see, you must answer the following three questions before you can do anything about an alarm:

- Which host originally caused the alarm?
- Is the behavior that caused the alarm normal for this host?
- What other hosts, if any, were affected?

Note:

You may also find that you are seeing a large number of unnecessary alarms for activity that you know to be okay. For more information about reducing the number of unnecessary alarms you see, refer to Chapter 11, "Reducing Unnecessary Alarms."

Once you have answered the preceding questions, you can then decide how to use the SMC software to respond to the alarm. This chapter includes the most common actions taken when responding to alarms.

Note:

Refer to the *Stealthwatch Desktop Client Online Help* to read about other procedures that you may also want to perform when responding to alarms.

This chapter includes the following topics:

- How to Respond to an Alarm
- Stealthwatch Mitigation Feature

How to Respond to an Alarm

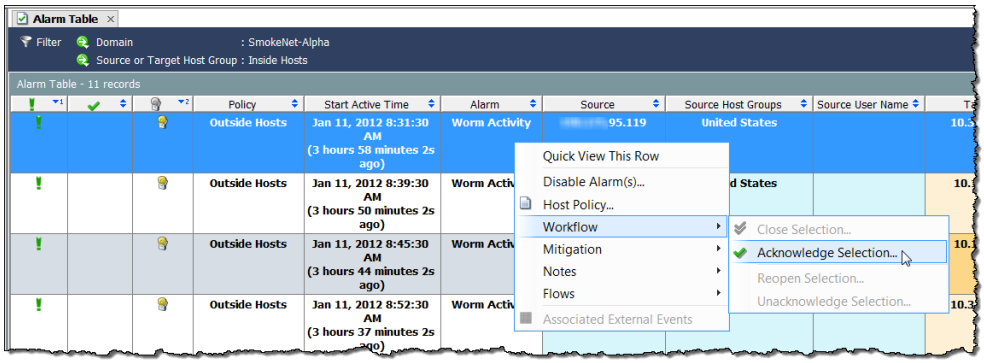
There are several ways to respond to an alarm. You can acknowledge an alarm, unacknowledge an alarm, close an alarm, and reopen a closed alarm. Refer to the following sections to read about these particular procedures.

Acknowledging Alarms

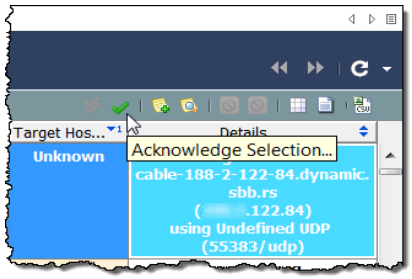
When you acknowledge an alarm, you are indicating that it is being investigated. This is beneficial to workflow and to make other team members aware that the alarm is being investigated. Before you acknowledge an alarm, keep in mind that acknowledging an alarm can be undone if necessary.

An alarm can be acknowledged or unacknowledged regardless of whether the alarm is active or inactive. To use the SMC to acknowledge an alarm, complete the following steps:

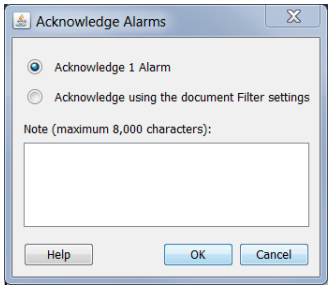
1. On the Alarm Table, right-click the alarm and select **Workflow > Acknowledge Selection**.



You can also click the alarm, and then click the **Acknowledge Selection** button on the Alarm Table toolbar.



The Acknowledge Alarms dialog opens, requesting that you enter a note explaining why the alarm is being closed.



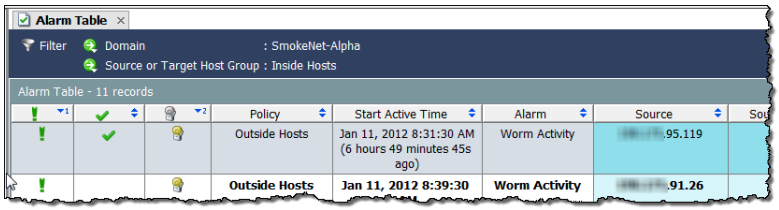
2. Specify either to acknowledge the alarm or to acknowledge using the settings in the document filter. Refer to the following explanations of the available options so you are aware of the implications of acknowledging alarms.

   - **Acknowledge [x] Alarm(s)** – Acknowledges only the alarms currently displayed on the Alarm Table, where [x] equals the total number of alarms selected. If you click this option, the system will acknowledge each alarm one by one. So, if you have a large number of alarms, such as 1000 or more, the system will need a considerable amount of time to finish this process.
   - **Acknowledge using the document Filter settings** – Acknowledges all of the alarms included in the current filter settings in bulk rather than one by one, *including any new alarms that may occur* during the acknowledgement process. For example, suppose the Alarm Table Filter is set to display only Trivial alarm types, and you choose to acknowledge all of the alarms based on this setting. The system will acknowledge not only the Trivial alarms that you see on the Alarm Table now, but also any Trivial alarms that may be generated while the acknowledging process is underway, which you have not seen.

Note:

Because the **Acknowledge using the document Filter settings** option acknowledges alarms in bulk, it is much faster than the other option, especially if you have 1000 or more alarms. However, you must realize that by choosing this option, you may acknowledge alarms that you have never seen.

3. Click in the text entry field, type an explanation as to why the alarm is being acknowledged, and then click **OK**. A check mark appears in the Acknowledged column and the note appears in the Last Note column if you have chosen to show these columns. The text in the table row for that alarm becomes unbolded.



Note:

To see the Acknowledged and/or Last Note columns, right-click a column header and select the appropriate option from the pop-up menu.

Unacknowledging Alarms

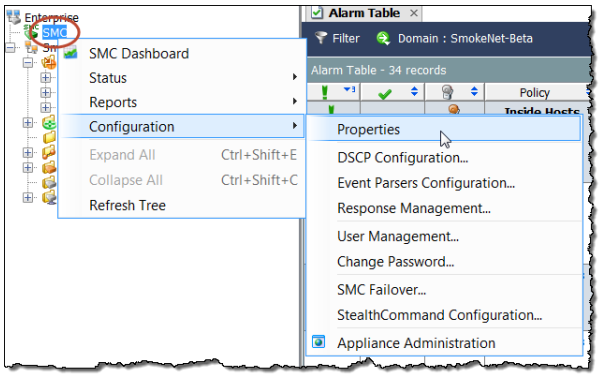
The SMC enables you to unacknowledge one or more acknowledged alarms. You may want to complete the following steps, for example, if you have acknowledged any alarms by mistake.

1. On the Alarm Table, display the acknowledged alarms that you want to unacknowledge. Use the alarm filter if necessary.
2. Right-click an alarm you want to unacknowledge and select **Workflow > Unacknowledge Selection**. The Unacknowledge Alarms dialog opens.
3. Type an alarm note and click **OK**.
4. Repeat steps 2 and 3 for each alarm you want to acknowledge.

Closing Alarms

When you want to indicate that you are satisfied that an alarm has been resolved, you can close the alarm. Note that it is not necessary to manually close alarms.

Once an alarm becomes inactive, it is automatically removed from the database when it is older than the number of days specified for the Alarm Table on the SMC Properties: Data Retention page. To access this page, right-click the SMC icon in the Enterprise tree, and then click **Configuration > Properties**.

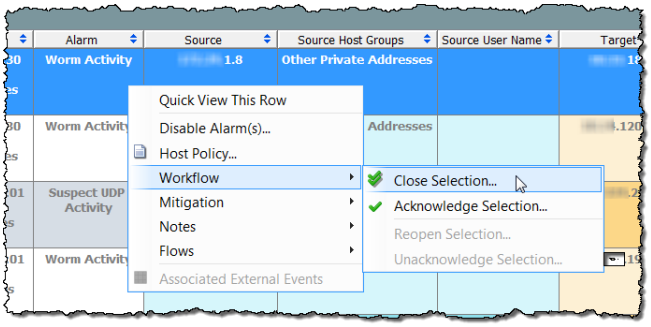


Before you close an alarm, keep the following points in mind:

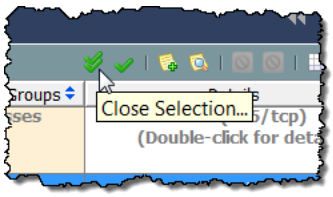
- You cannot close an active alarm.
- When you close an alarm for a particular host, that host may generate that alarm again before the next archive hour.
- Closing an alarm can be undone if necessary.

To use the SMC to close an alarm, complete the following steps:

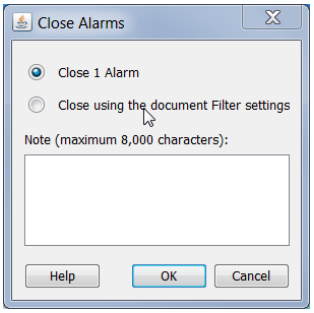
1. Change the Alarm Table filter so that inactive alarms are displayed. To do this, on the States page of the Alarm Table filter dialog, click the **Filter on currently Active** check box to add a checkmark, and then click the **Inactive** option.
2. On the Alarm Table, right-click the alarm and select **Workflow > Close Selection**.



You can also click the alarm, and then click the **Close Selection** button on the Alarm Table toolbar.



The Close Alarms window opens, requesting that you enter a note explaining why the alarm is being closed.



3. Specify either to close the alarm or to close using the settings in the document filter. Refer to the following explanations of the available options so you are aware of the implications of closing alarms.

   - **Close [x] Alarms** – Acknowledges and closes only the alarms currently displayed on the Alarm Table, where [x] equals the total number of alarms displayed on the Alarm Table. If you click this option, the system will acknowledge and close each alarm one by one. So, if you have a large number of alarms, such as 1000 or more, the system will need a considerable amount of time to finish the process with this option.
   - **Close using the document Filter settings** – Acknowledges and closes all of the alarms included in the current filter settings in bulk rather than one by one, *including any new alarms that may occur* during the closing process. For example, suppose the Alarm Table Filter is set to display only Minor alarm types, and you choose to close all of the alarms based on this setting. The system will close not only the Minor alarms that you see on the Alarm Table now, but also any Minor alarms that may be generated while the closing process is underway, which you have not seen.

Note:

Because the "Close using the document Filter settings" option closes alarms in bulk, it is much faster than the other option, especially if you have 1000 or more alarms. However, you must realize that by choosing this option, you may close alarms that you have never seen.

4. Click in the text entry field, type an explanation as to why the alarm is being closed, and then click **OK**. A check mark appears in the Closed column and the note appears in the Last Note column if you have chosen to show these columns.

Note:

To see the Acknowledged and/or Last Note columns, right-click a column header and select the appropriate option from the pop-up menu.

Reopening Closed Alarms

The SMC enables you to reopen one or more closed alarms. You may want to complete the following steps, for example, if you have closed any alarm by mistake:

1. On the Alarm Table, display the closed alarms that you want to reopen. Use the alarm filter if necessary.
2. Right-click an alarm you want to reopen and select **Workflow > Reopen Selection**.
3. Type an alarm note, and then click **OK**.
4. Repeat steps 2 and 3 for each alarm you want to acknowledge.

STEALTHWATCH MITIGATION FEATURE

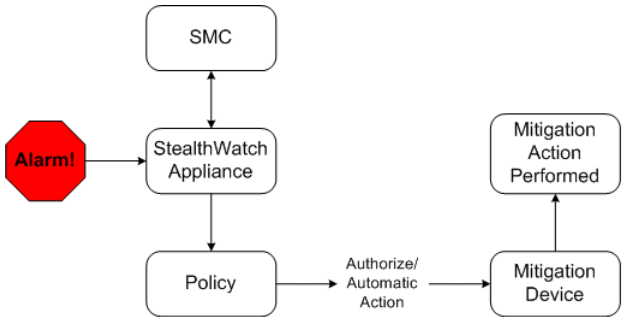
The Stealthwatch software provides a threat mitigation feature that you can use to automate the system's response to various threats. By using this feature, you can reduce the time required to make decisions about how to respond to certain alarms. The system will do it for you as soon as the alarm occurs.

The Stealthwatch mitigation feature can help you go from incident to resolution in seconds. If you prefer, you can set the feature to perform mitigation immediately (Automatic mode) or to ask you for authorization first (Authorize, or manual, mode).

The Stealthwatch mitigation feature is disabled by default. To enable it, you must complete the following steps, which are detailed later in this section:

1. Configure the mitigation devices for each appliance where you want to use mitigation (e.g., define the firewall).
2. Enable the mitigation feature for the policies where you want to use mitigation.
3. Define the desired mitigation actions for individual alarms.

The following illustration provides a general overview of how the Stealthwatch mitigation feature works:



When you enable this feature and a specified alarm then occurs, Stealthwatch sends a signal to the mitigation device requesting the device to perform the configured mitigation action. The device performs the requested action based on the policy settings you have specified for that alarm.

Note:

The system will not perform mitigation against hosts that are on the Broadcast List or on the Mitigation White List. For more information about these lists, please refer to the *Stealthwatch Desktop Client Online Help*.

Configuring the Mitigation Devices

You must configure the SMC to set up communication between Stealthwatch and the mitigation devices. If you want several appliances to use the same mitigation device, you must configure each appliance separately for that device.

Note:

You also may need to configure the mitigation devices themselves to receive information from Stealthwatch devices. For more information, refer to the *Mitigation Device Configuration* guide. You can find this document on the Stealthwatch User Community Web site (https://community.Cisco.com).

You can configure up to five of the following mitigation device types per appliance:

- Brocade INM
- Cisco ASA
- Cisco Guard
- Cisco Router (Internetworking Operating System 11.3 and later)
- Custom
- Radware DefensePro
- Stealthwatch SNMP Mitigation Interface

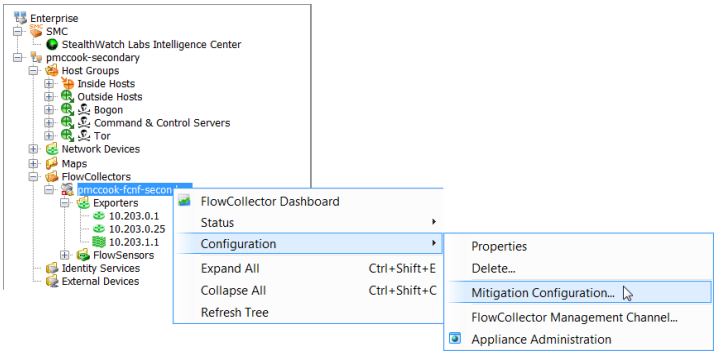
Notes:

- All of these mitigation device types (with the exception of Radware DefensePro) are available only in the Stealthwatch module. Radware DefensePro is available only in the DDoS module.
- Choose the Custom option if you plan to use an expect script to customize mitigation actions. However, we recommend that you contact Cisco Customer Support for assistance before attempting to use expect scripts.

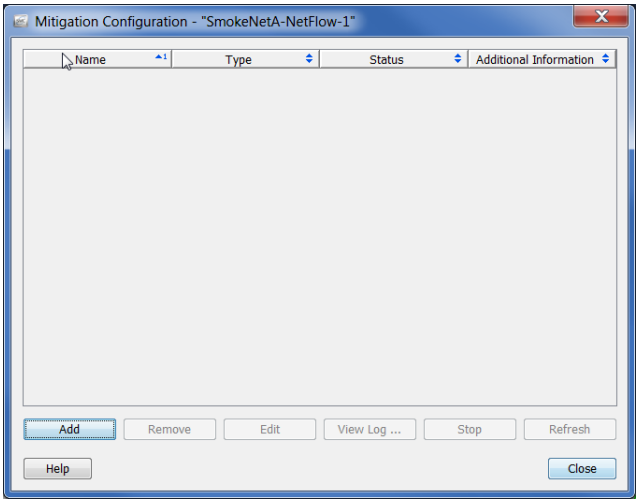
The type of mitigation device you choose determines the type of mitigation actions that the system can perform. For example, a particular device may only support blocking traffic coming from the source IP address.

To configure mitigation devices on the SMC, complete the following steps:

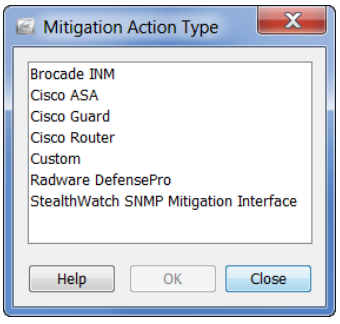
1. Right-click an appliance name and select **Configuration > Mitigation Configuration**.



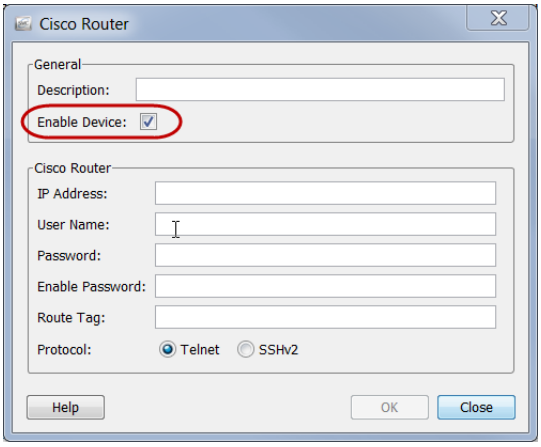
The Mitigation Configuration dialog opens.



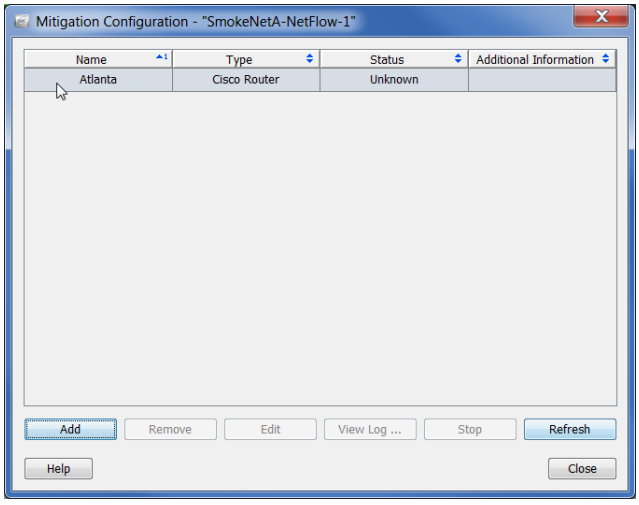
2. Click **Add**. The Mitigation Action Type dialog opens.



3. Click the type of mitigation device you want to use, and then click **OK**. The device information dialog opens for the device type you selected. For example, if you click **Cisco Router**, the Cisco Router information dialog opens.



4. Ensure the **Enable Device** check box contains a check mark, as shown in the preceding example. If you do not make this selection, the device will not receive information from Stealthwatch, and the mitigation feature will not work.
5. Complete all of the specific identifying information for the selected device, and then click **OK**. The device information dialog closes and the device you added is now included on the Mitigation Configuration dialog.



6. Repeat steps 2 through 5 until you have added all of the mitigation devices you need to add for this appliance.
7. When finished, click **Close** to close the Mitigation Configuration dialog.

You are now ready to enable the mitigation feature per host group as described in the next section.

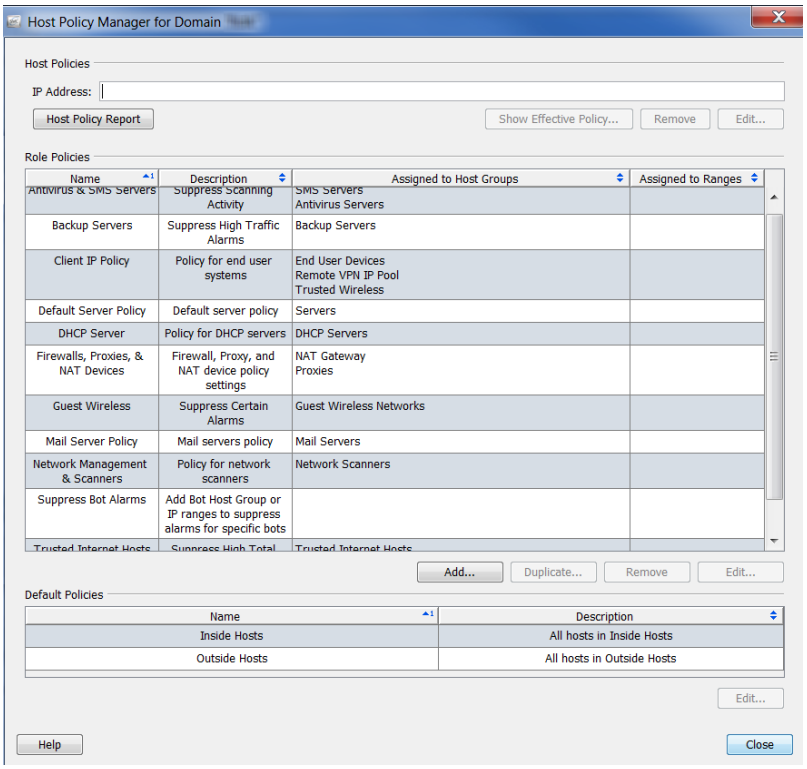
Note:
The mitigation device must be running for the mitigation feature to work.

Enabling the Mitigation Feature for Policies

Once you have configured the mitigation devices, you can enable the Stealthwatch mitigation feature for specific policies, which can be assigned to one or more host groups. For example, you may want to enable the mitigation feature for the Inside Hosts default policy. You can also enable the feature for only a few host groups, or even for specific host IP addresses.

For the following example we will assume that we want to enable the mitigation feature for a specific role policy. To do this, complete the following steps:

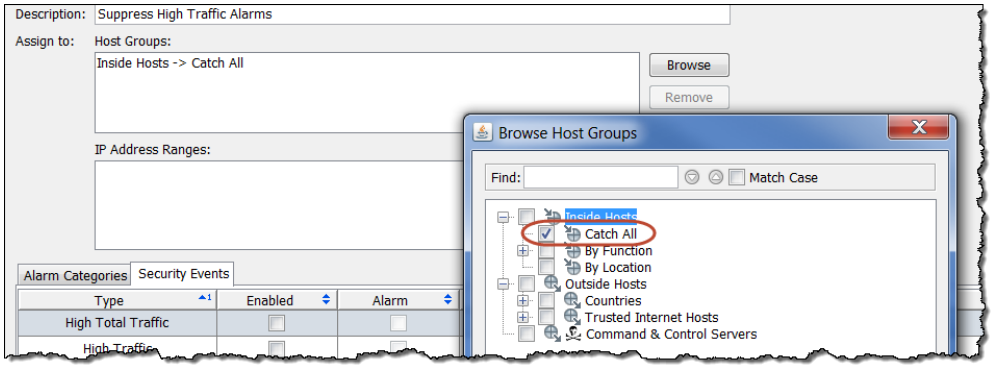
1. From the Main Menu select **Configuration > Host Policy Manager**. The Host Policy Manager dialog opens.



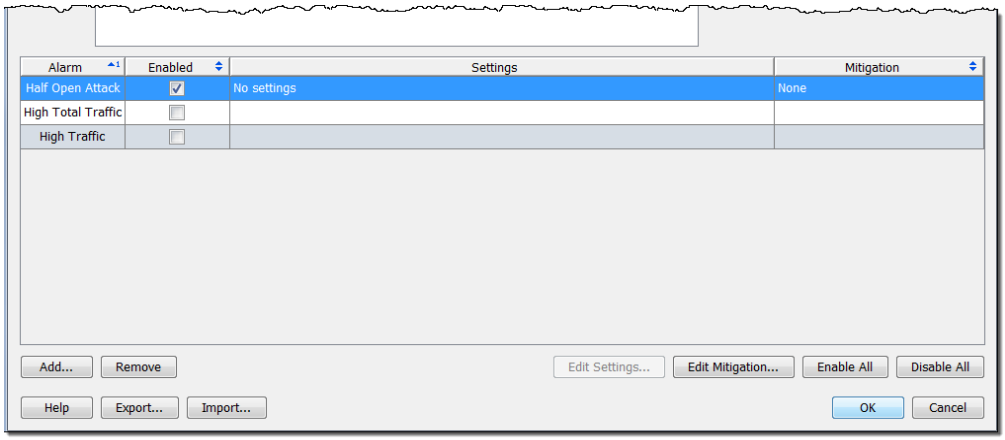
2. In the **Role Policies** section, click the desired Role Policy, and then click **Edit**. The Edit Role Policy dialog opens.

3. In the **Assign to: Host Groups:** section, click **Browse** to select the host group(s) to which the policy applies, and then click **OK** to return to the Edit Role Policy

dialog. (You can also specify specific host IP addresses or ranges in the IP Address Ranges field.)



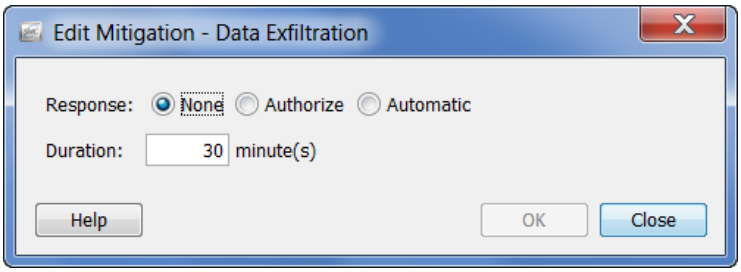
4. On the Edit Role Policy dialog, click the check box(s) to add a check mark(s) in the Enabled column for each alarm for which you want to enable mitigation. (If the desired alarms aren't listed, click **Add** to add them.)



Defining Mitigation Actions for Alarms

You can now define the mitigation actions for the desired individual alarms. To do this, complete the following steps:

1. Continuing from step 4 in the previous section, from the Edit Role Policy dialog that is now open, select the row that contains the alarm for which you want to enable mitigation, and then click **Edit Mitigation**. The Edit Mitigation dialog opens (the contents may vary depending on the alarm).



Note:

Cisco provides recommended default settings for each mitigation action. You can change these settings to suit your network needs whenever desired.

2. Click the desired mitigation response on the pop-up menu based on the following descriptions.

Response	Description
None	To disable all mitigation actions for the alarm, click **None**.
Authorize	To cause the system to ask you for authorization before it performs the selected mitigation actions when the alarm occurs, click **Authorize**. Use this setting if you prefer to manually block connections rather than allow the system to block them for you automatically.
Automatic	To allow the system to immediately and automatically perform the selected mitigation actions when the alarm occurs, click **Automatic**.

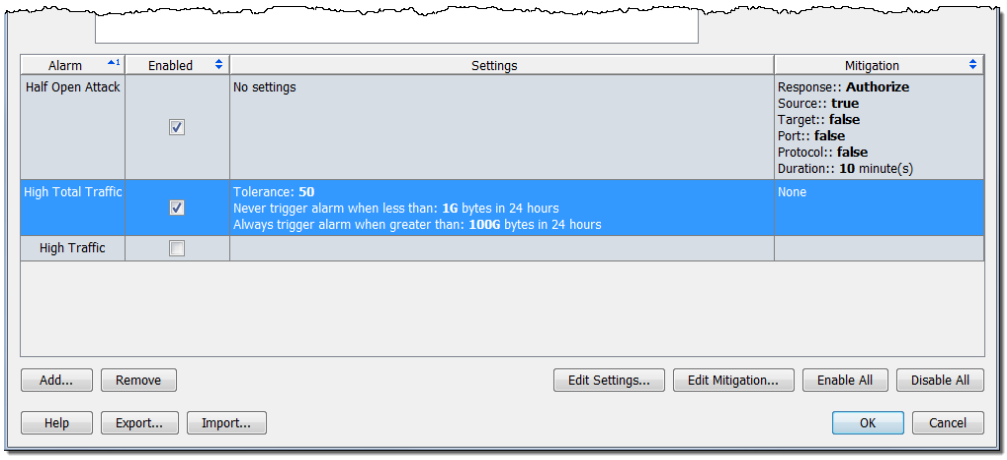
3. Specify the other mitigation settings as indicated in the following table. You can customize mitigation actions for each alarm based on a combination of source or target IP address, protocol, and/or port number. You can even specify how long the mitigation action is to run.

Mitigation Option	Purpose
Source	Blocks traffic coming from the host that originated the suspicious activity.
Target	Blocks traffic going to the host that is the target of the suspicious activity.
Port	Blocks the interface through which the suspicious traffic has traveled.
Protocol	Blocks the protocol being used to transmit the suspicious traffic.
Duration	The length of time (in minutes) that you want the blocking action to be in effect. When this time period expires, the mitigation process ends. **Note:** A duration of 0 (zero) indicates infinity, meaning the mitigation action will be in effect until the mitigation process is manually ended.

Notes:

- Cisco routers do not support the Port or Protocol mitigation actions.
- OPSEC devices require that you enable both the Source and the **T**arget mitigation actions. Otherwise, these devices cannot block a connection.

4. When you have specified the mitigation settings for the alarm, click **OK**. Your settings are displayed on the Edit Role Policy dialog.



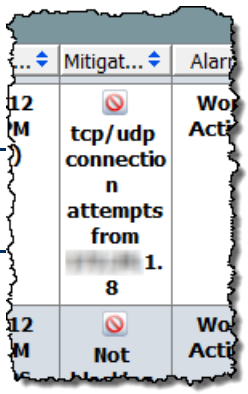
5. Repeat steps 1 through 4 for each alarm for which you want to configure the mitigation settings.
6. When finished, click **OK**, and then click **Close** to close the Host Policy Manager.

Mitigation and the Alarm Table

Based on whether you enabled a mitigation action in Authorize or in Automatic mode, when the corresponding alarm occurs, the Alarm Table shows you whether or not the blocking action is being conducted.

Authorize (Manual) Mode

When an alarm occurs with a mitigation action in Authorize mode, the Alarm Table displays the red "Not Blocking" icon in the Mitigation column.



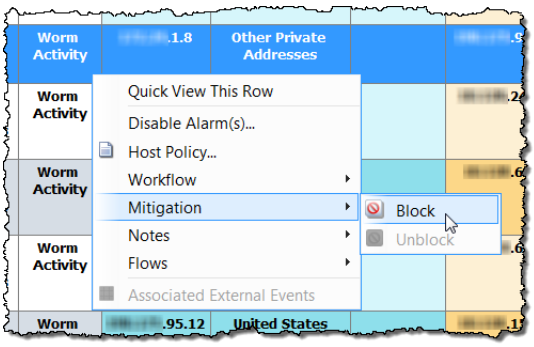
Note:

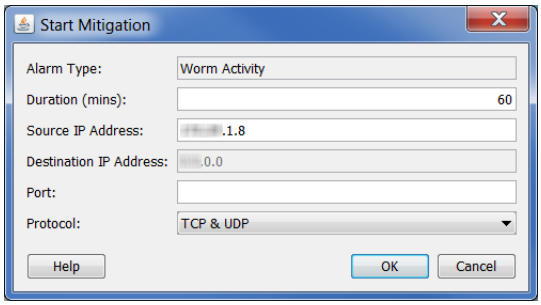
To display the Mitigation column, right-click in a column header and select **Mitigation**.

To manually mitigate against a specific alarm in the Alarm Table when a mitigation action is in Authorize mode, complete the following steps:

1. Right-click an alarm and select **Mitigation > Block**.

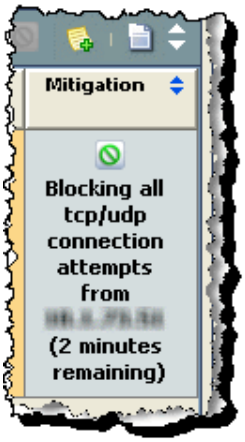
   The Start Mitigation dialog opens.





2. If desired, change the mitigation action parameters, and then click **OK**. The Start Mitigation dialog closes and the Alarm Table refreshes.

3. Find the alarm condition. The red "Not Blocking" icon is now replaced with the green "Blocking" icon.



Note:

If you want to unblock the connection before the mitigation action expires, simply right-click the alarm and select **Mitigation > Unblock**.

Automatic Mode

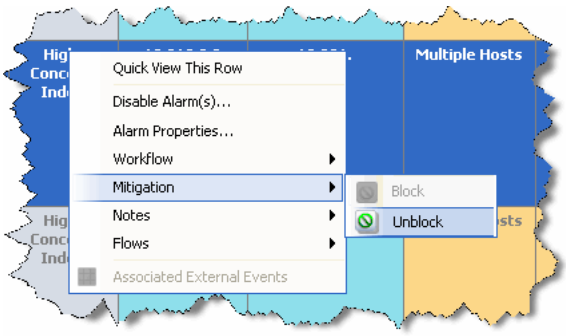
When an alarm occurs with a mitigation action in Automatic mode, the Alarm Table displays the green "Blocking" icon in the Mitigation column, as shown in the previous example.

Note:

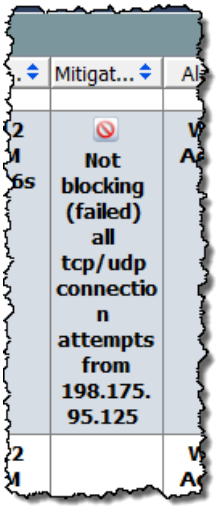
To display the Mitigation column, right-click in a column header and select **Mitigation**.

Because the mitigation action is in Automatic mode, you do not need to do anything to start it when the alarm occurs. However, if you need to stop the mitigation action, complete the following steps:

1. In the Alarm Table, right-click the alarm and select **Mitigation > Unblock**. The Alarm Table refreshes.

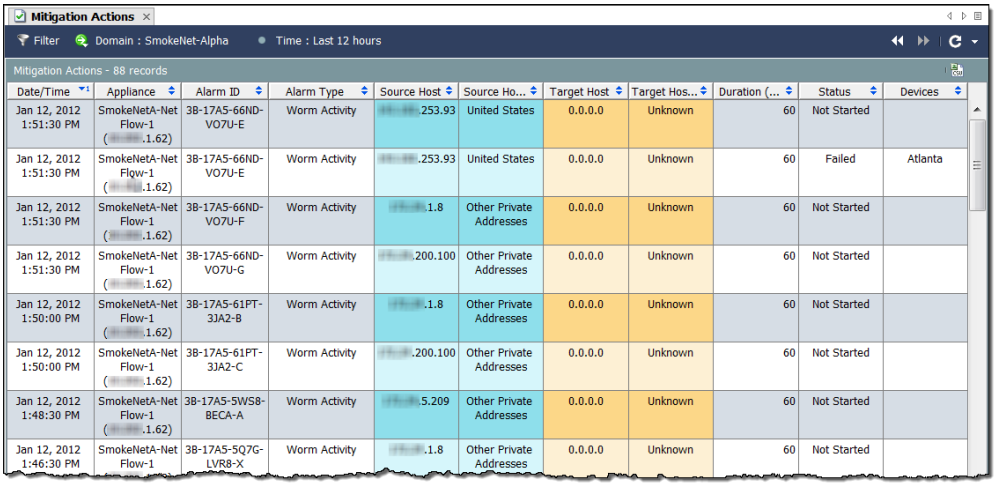


2. Refresh the document again, and then re-select the alarm condition. The green "Blocking" icon is now replaced with the red "Not Blocking" icon.



Mitigation Actions Document

The Mitigation Actions document allows you to see the status of all mitigation actions that have occurred in a domain since the last archive hour. To access the Mitigation Actions document, right-click the domain in question, and then select **Status > Mitigation Actions**. The Mitigation document opens.



Date/Time	Appliance	Alarm ID	Alarm Type	Source Host	Source Ho...	Target Host	Target Hos...	Duration (...	Status	Devices
Jan 12, 2012 1:51:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-66ND-VO7U-E	Worm Activity	.253.93	United States	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:51:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-66ND-VO7U-E	Worm Activity	.253.93	United States	0.0.0.0	Unknown	60	Failed	Atlanta
Jan 12, 2012 1:51:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-66ND-VO7U-F	Worm Activity	.1.8	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:51:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-66ND-VO7U-G	Worm Activity	.200.100	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:50:00 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-61PT-3JA2-B	Worm Activity	.1.8	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:50:00 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-61PT-3JA2-C	Worm Activity	.200.100	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:48:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-5WS8-BECA-A	Worm Activity	5.209	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:46:30 PM	SmokeNetA-Net Flow-1	3B-17A5-5Q7G-LVR8-X	Worm Activity	.1.8	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	

11

Reducing Unnecessary Alarms

Overview

If certain policy settings are set too low, or services or applications that are identified as okay are mistakenly disallowed for a particular host group, alarms can occur as the result of behavior that is seen as suspicious, when in fact the behavior is normal. This chapter describes how to reduce the number of unnecessary alarms you see.

This chapter includes the following topics:

- Baselining
- Host Policy Management
- Creating and Editing Policies
- Alarms
- Recommendations

BASELINING

Baselining is critical to network monitoring because it builds a profile of what is considered normal behavior for your network. This allows Stealthwatch to trigger alarms when it observes abnormal behavior.

As soon as Stealthwatch is installed on a network, it begins identifying every host on the network. During the first 7 days, Stealthwatch establishes a baseline of what appears to be normal behavior, based on approximately 90 attributes, such as the following:

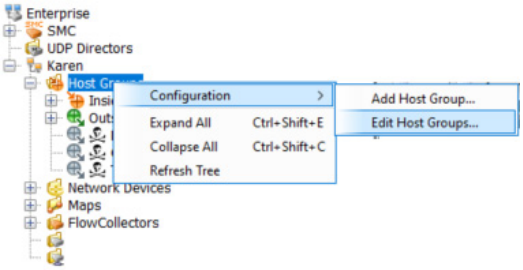
- Regular bandwidth consumption.
- Communication with other hosts.
- Number of concurrent flows.
- Packets per second.

This baseline represents the expected behavior for the day. Baseline is used in conjunction with the tolerance to calculate the threshold values to use for that day.

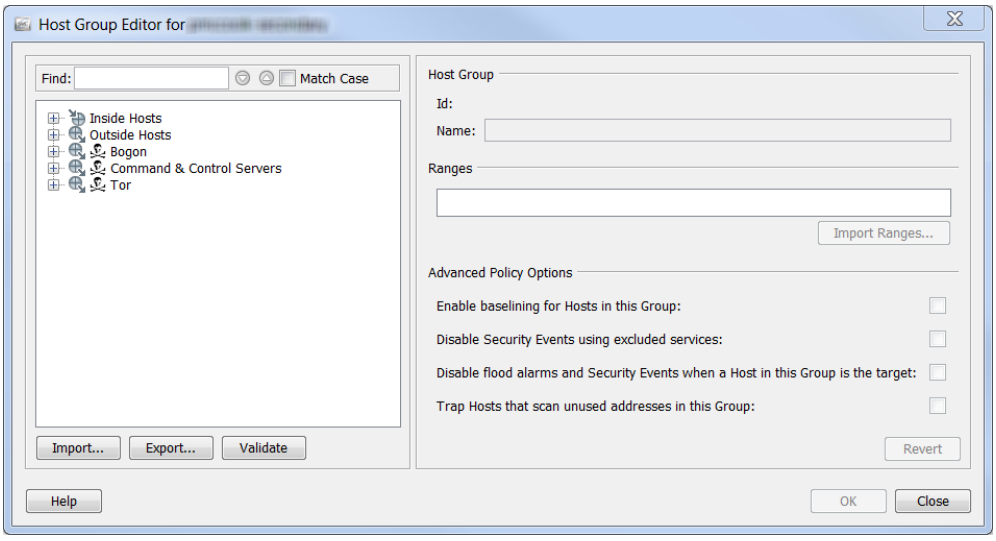
Note:

For information about the concept of tolerance related to alarms, refer to "Alarms" on page 266.

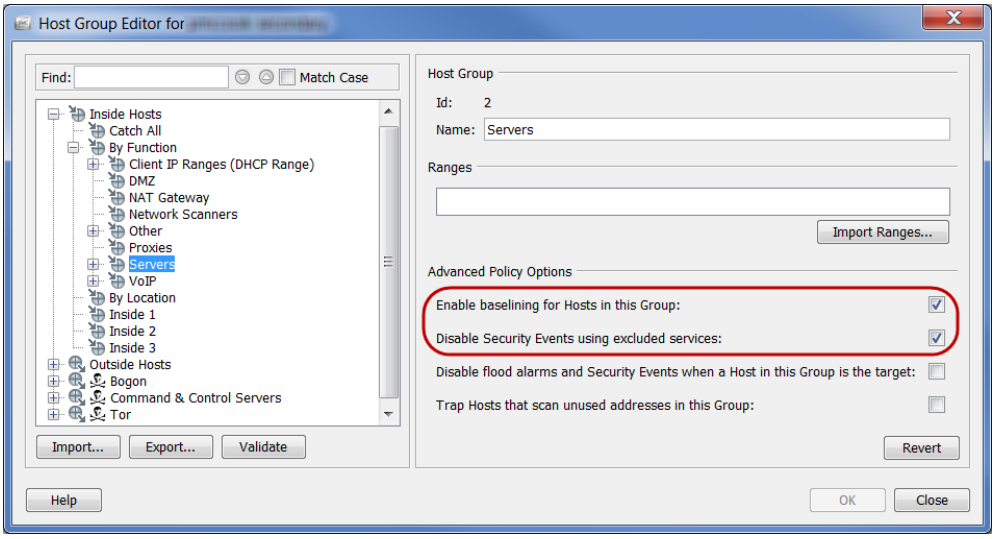
These 90 attributes become part of the host profile mentioned earlier. By default, Stealthwatch baselines every host within the Inside Hosts host group. However, for the Outside Hosts host group, Stealthwatch baselines only aggregate host behavior at the host group level. You can change the baselining method at any time in the Host Group Editor dialog.



To access this dialog, right-click **Host Group** in the Enterprise tree, and then select **Configuration > Edit Host Groups**.



In the Enterprise Tree on the left side of the dialog, click the host for which you want to change the baselining method. In the Advanced Policy Options section, the check boxes will auto-populate with check marks to indicate the current settings for the host you clicked.



A unique host level baseline will be established for each host in a host group *only if* the **Enable baselining for Hosts in this Group** check box contains a checkmark; otherwise, Stealthwatch will baseline aggregate host behavior at the host group level.

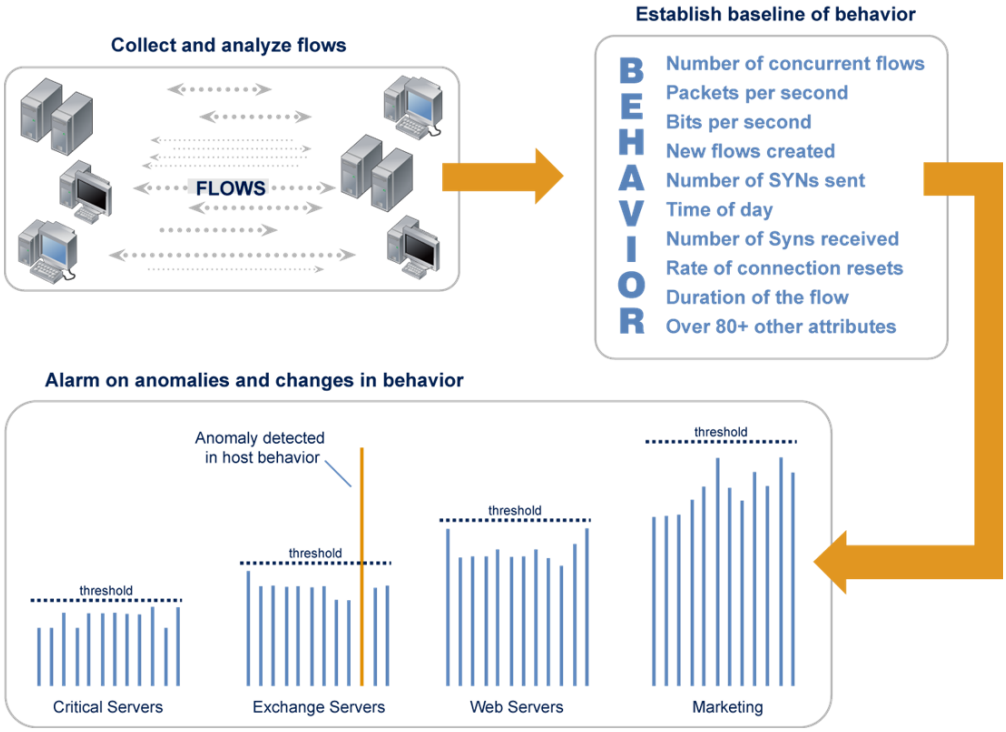
As previously stated, by default, Stealthwatch baselines every host within the Inside Hosts group; therefore, by default this option in enabled for Inside Hosts (refer to the circled area in the previous example).

Note:

You can disable this feature for very dynamic environments, such as DHCP scopes, where IPs change frequently. If you do, this will cause a baseline for expected behavior of any DHCP host to behave like all DHCP hosts.

However, by default, Stealthwatch baselines only aggregate host behavior at the host group level for the Outside Hosts group; therefore, by default this option is disabled for Outside Hosts.

The following diagram illustrates the baselining process:

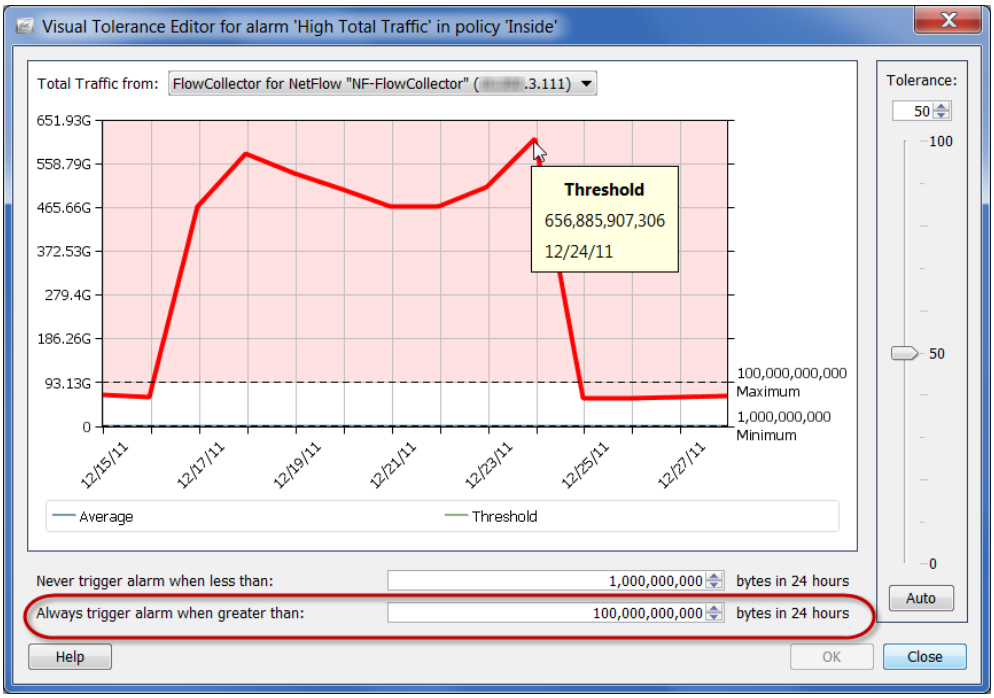


After the initial 7 days, Stealthwatch tracks 14 key attributes to create a rolling 28-day baseline. This baseline is the average of the daily attribute values for the past 28 days, heavily weighted for the last 7 days. Since the baseline incorporates the last seven days, these are used to represent weekly values. Therefore, the baseline includes values for the previous month, but is heavily weighted to the most recent week.

Stealthwatch uses the following guidelines when baselining:

- For Host Baselining, Stealthwatch stores the host daily maximum value seen for each alarm that has been enabled (e.g., the High Total Traffic alarm).
- For Host Group Baselining, Stealthwatch stores the average of the maximum values for all hosts in the group (e.g., the max high total traffic for all hosts, averaged out).

- If a host has no daily values, it uses the baseline from the group with the least amount of hosts that it belongs to. For example, if a host belongs to two groups (Group A defined as 10.201.0.0/16, and Group B defined as 10.201.3.0/24), the baseline will inherit Group B, which has fewer hosts.
- If a host group baseline is zero (0), the maximum is used (e.g., the High Total Traffic maximum bytes in 24 hours).
- For a new installation, all hosts use the configuration policy maximum for the first day until the baselines are established. Hosts do not alarm unless they exceed the maximum values (refer to the circled option in the following example).



Going forward, Stealthwatch looks for and highlights changes in behavior, such as the following:

- One host contacting large numbers of other hosts in a short period of time (e.g., peer-to-peer applications, worms).
- Long flow durations (e.g., covert channels, VPNs).
- Use of unauthorized ports (e.g., rogue servers/applications).
- Bandwidth anomalies (e.g., Warezserver, denial of service).
- Unauthorized communications (e.g., a VPN host communicating with an accounting server).

Whenever a host exceeds its threshold of what Stealthwatch has baselined as “normal” behavior, Stealthwatch triggers an alarm. By observing a host’s behavior as the behavior occurs and by using several proprietary algorithms, Stealthwatch avoids generating false positive alarms like those often generated by signatured-based solutions.

HOST POLICY MANAGEMENT

Depending on your login privileges, you can use policies to control how Stealthwatch monitors and responds to host behavior. A policy contains settings that determine how Stealthwatch reacts when it observes certain behavior. Stealthwatch uses the following three types of policies, which you can modify whenever needed.

- *Default policies*, which pertain to all Inside Hosts and all Outside Hosts.
- *Role policies*, which pertain to collections of hosts (IP addresses) that serve a common purpose (e.g., Web servers, firewalls, trusted Internet hosts, etc.).
- *Host policies*, which pertain to specific IP addresses.

A host policy takes precedence over all other policies. Therefore, a host policy is more specific than a role policy, which is more specific than a default policy. Only the most specific policy settings for a host will trigger an alarm.

Note:
A host cannot be assigned to more than one host policy.

For instance, if an alarm is added to a role policy, whether it is disabled, enabled, or the alarm settings have been changed, it will override that same alarm in the default policy.

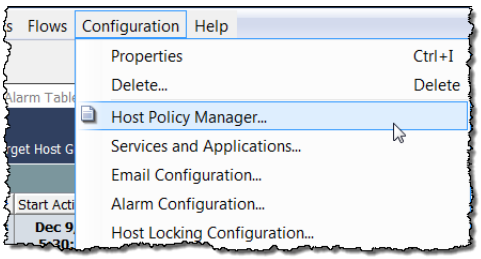
Likewise, if an alarm is added to a host policy for a particular host, whether it is disabled, enabled, or the alarm settings have been changed, it will override that same alarm in any role policy or default policy that may apply to that host.

If a host is not assigned to a host policy but is assigned to two or more role policies, Stealthwatch determines for each alarm which policy's settings are used in the host's effective policy. For more information about how the effective policy is determined, see "Effective Host Policy" on page 241.

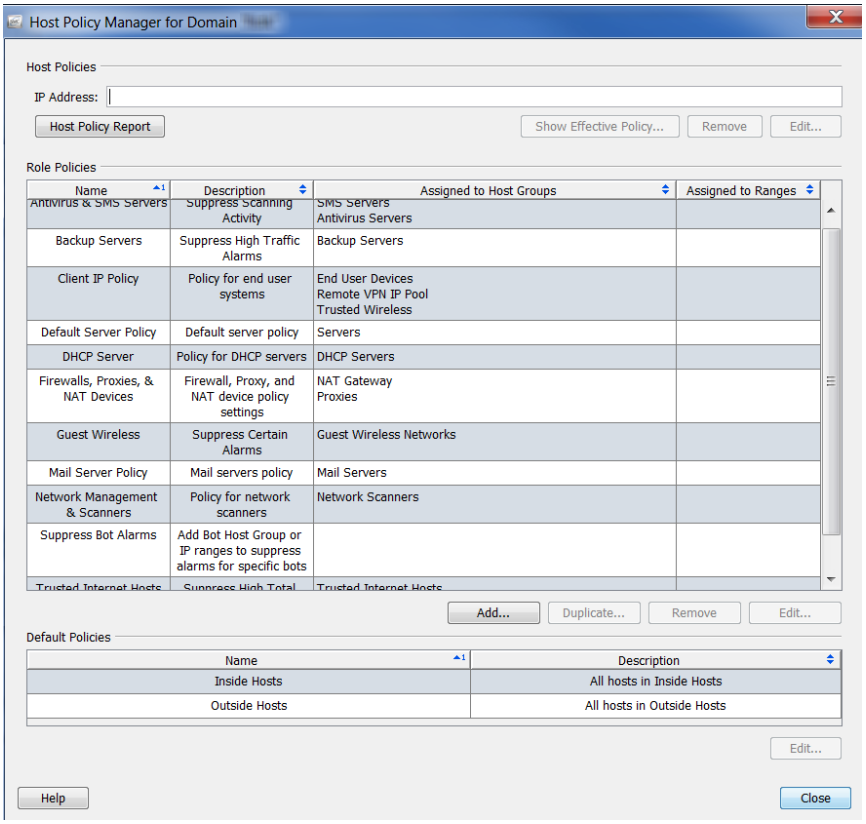
If you want to change the threshold of behavior that is allowed for a domain, a host group, or a particular host, you will need to create or edit the appropriate type of policy, depending on how many host groups or hosts you want to affect.

Two default policies exist within Stealthwatch: the Inside Hosts default policy and the Outside Hosts default policy. These settings will apply when no role policies or host policies have been created.

You may determine that you need to edit the default policy for one or both of these groups. To do this, you need to access the Host Policy Manager. To access this dialog, from the Main Menu select **Configuration > Host Policy Manager**.



The Host Policy Manager dialog opens.



This dialog allows you to configure policies using the following sections:

- Host Policies – Allows you to manage a policy for a single host.
- Role Policies – Allows you to manage policies for hosts according to the roles they perform in your system.

- Default Policies – Allows you to manage the default policies for inside hosts or outside hosts.

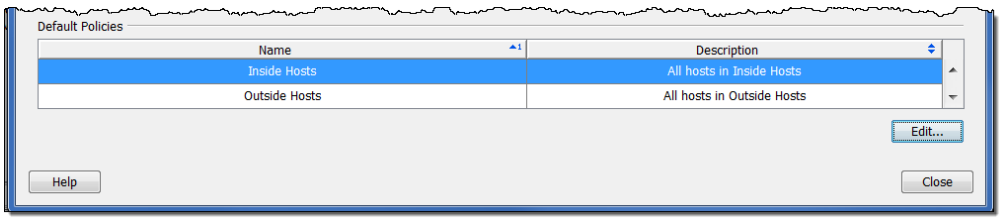
Note:

For information about creating and editing role policies and host policies, refer to "Creating and Editing Policies" on page 251.

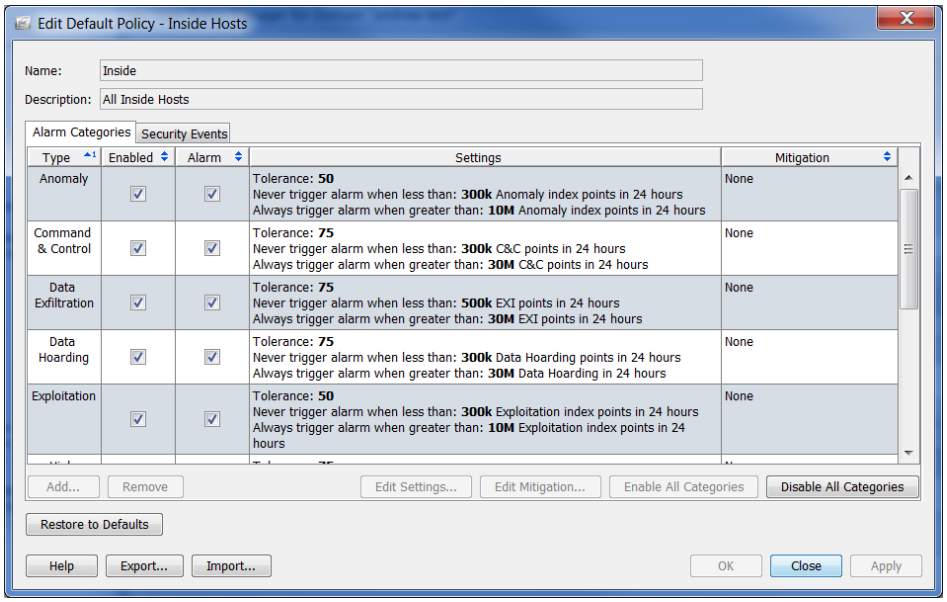
Editing Inside Hosts/Outside Hosts Default Policies

To edit an Inside Hosts default policy or Outside Hosts default policy, complete the following steps:

1. From the Main Menu select **Configuration > Host Policy Manager**. The Host Policy Manager dialog opens, as shown in the previous screen.
2. Within the **Default Polices** section, select the name of the host whose default policy you want to edit, and then click **Edit**.



The Edit Default Policy dialog opens.



CAUTION:

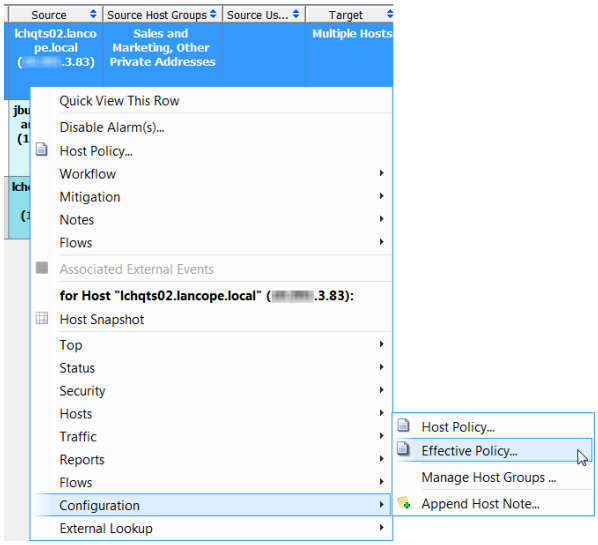
If you click Restore to Defaults, you will override the current policy with the factory default policy settings, so use this feature with extreme caution.

3. If you want to add alarm categories to policies, edit settings or mitigation of alarms associated with the alarm categories, and enable or disable alarm categories, go to "Configuring Alarm Categories in Host Policies" on page 245.
4. If you want to configure the security events used by a policy, edit settings or mitigation of alarms associated with a CI, and enable or disable security events, go to "Configuring Security Events in Host Policies" on page 248.

Effective Host Policy

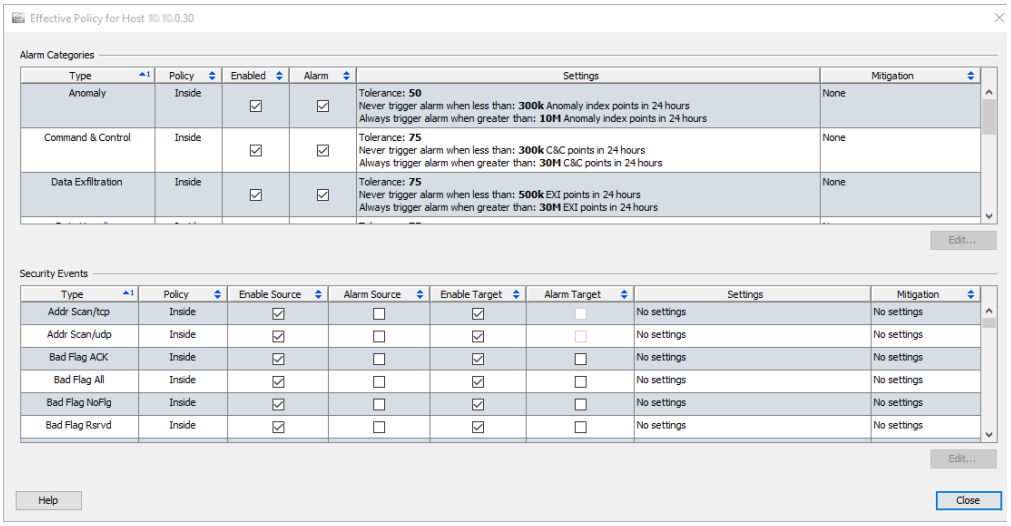
When you are responding to an alarm, you first need to determine which policy triggered that particular alarm. If an IP address is visible, you can right-click the IP address and select **Configuration > Effective Policy.**

The Effective Host dialog opens, as shown in the following example.



Tip:

If you are in the Alarm Table, a quicker way to find the controlling policy is to enable the Policy column to be visible by right-clicking within a header and selecting **Policy** from the pop-up menu. By looking at this column, you can determine by which policy the alarm is controlled. From this point, if you want to see the policy settings for a particular policy, double-click the policy name in the **Policy** column.



As you can see in the previous example, the High File Sharing Index alarm is controlled by the Servers role policy, and the High Traffic alarm is controlled by the Inside Hosts policy.

There may be situations where a host is not assigned to a host policy but is assigned to two or more differently configured role policies. When this occurs, Stealthwatch first checks to see if any of the following four columns are de-selected in any of the role policies to which that host is assigned:

- Enable Source
- Alarm Source
- Enable Target
- Alarm Target

If even only one of the four columns named in the previous bulleted list is de-selected in any of the policies, then that column is de-selected in the effective policy. In other words, any column that is de-selected (which equals a "false" setting) overrides the same column in any other role policy to which that host is assigned if that column is selected (which equals a "true" setting); in other words, false settings override true settings.

Any column that is selected in ALL of the assigned role policies remain selected in the effective policy.

Example 1

If Role Policy 1 is...			
Enable Source	**Alarm Source**	**Enable Target**	**Alarm Target**
True	True	False	False
And Role Policy 2 is...			
Enable Source	**Alarm Source**	**Enable Target**	**Alarm Target**
False	False	True	True
Then the Effective Policy is...			
Enable Source	**Alarm Source**	**Enable Target**	**Alarm Target**
False	False	False	False

Example 2

If Role Policy 1 is...			
Enable Source	**Alarm Source**	**Enable Target**	**Alarm Target**
True	True	True	False
And Role Policy 2 is...			
Enable Source	**Alarm Source**	**Enable Target**	**Alarm Target**
True	False	True	True
Then the Effective Policy is...			
Enable Source	**Alarm Source**	**Enable Target**	**Alarm Target**
True	False	True	False

The effective policy for a host will display in the Policy column the names of all effective policies. When both a source policy and a target policy exists for a security event, then the Policy column lists the source policy first and the target policy second.

Note:

For the next steps in responding to an alarm, refer to "Creating and Editing Policies" on page 251.

Alarm Categories

Use this section to configure the alarm category with which this role policy is used. Categories provide a way to group specific types of security events. Each of the alarm categories can generate an alarm, depending on the number and type of events that occur.

You can do the following:

- Add or edit alarm category settings
- Edit mitigation of alarms associated with the alarm categories
- Enable or disable alarm categories

The types of alarm categories available are:

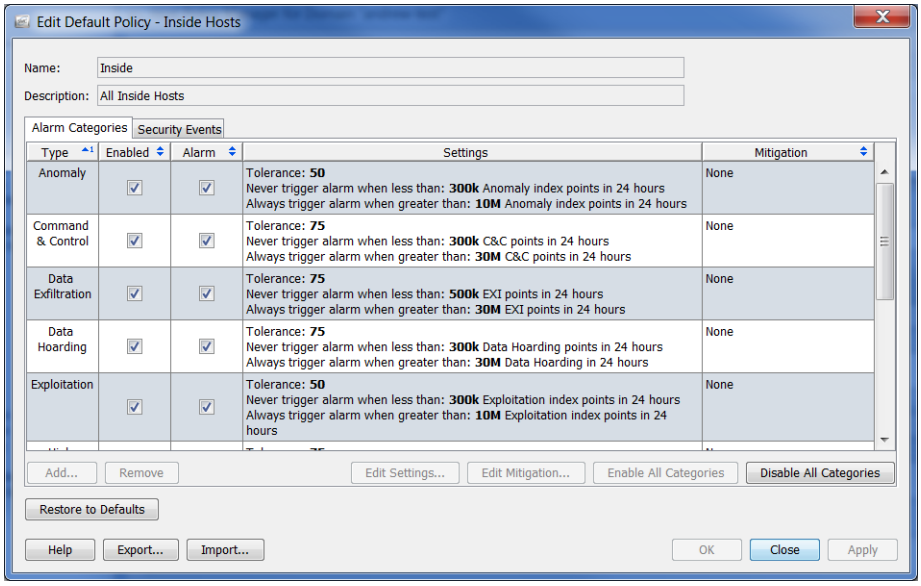
Item	Description
Anomaly	Tracks events that indicate that hosts are behaving abnormally or generating traffic that is unusual, but is not consistent with another category of activity.
C&C (Command & Control)	Indicates the existence of bot-infected servers or hosts in your network attempting to contact a C&C server.

Item	Description
Data Exfiltration	Tracks inside and outside hosts to whom an abnormal amount of data has been transferred. If a host triggers a number of these events exceeding a configured threshold, it results in a high exfiltration alarm.
Data Hoarding	Indicates that a source or target host within a network has downloaded an unusual amount of data from one or more hosts.
Exploitation	Tracks direct attempts by hosts to compromise each other, such as through worm propagation and brute force password cracking.
High Concern Index	Tracks hosts whose concern index has either exceeded the CI threshold or rapidly increased. High Concern Index and High Target Index categories use the same events. If an event is triggered by a source host, it results in a High CI category alarm. If an event is triggered by a target host, it results in a High TI alarm.
High DDoS Source Index	Indicates that a host has been identified as the source of a DDoS attack.
High DDoS Target Index	Indicates that a host has been identified as the target of a DDoS attack.
High Target Index	Tracks inside hosts that have been the recipient of more than an acceptable number of scan or other malicious attacks. High Concern Index and High Target Index categories use the same events. If an event is triggered by a source host, it results in a High CI category alarm. If an event is triggered by a target host, it results in a High TI alarm.
Policy Violation	The subject is exhibiting behavior that violates normal network policies.
Recon	Indicates the presence of unauthorized and potentially malicious scans using TCP or UDP and being run against your organization's hosts. These scans, referred to as "reconnaissance," are early indicators of attacks against your network, and the scans may come from outside or inside your organization.

Configuring Alarm Categories in Host Policies

To configure an alarm category, complete the following steps:

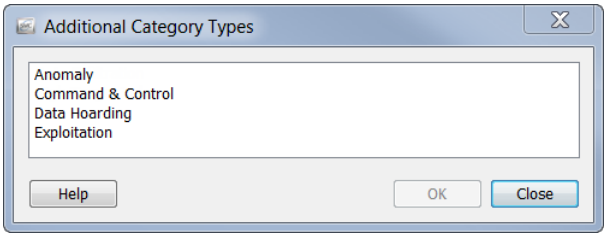
1. From an Edit Policy dialog, click the **Alarm Categories** tab.



2. Do one of the following:

   - If you need to add an alarm category, go to step 3.
   - If you need to edit an alarm category, go to step 5.

3. To add an alarm category, click **Add**. The Alarm Categories dialog opens.

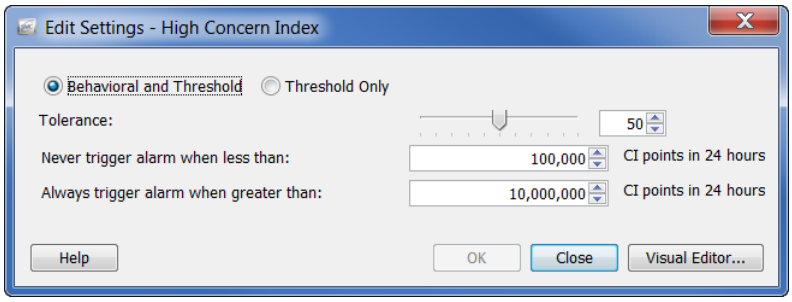


4. Select one or more alarm categories and click **OK**:

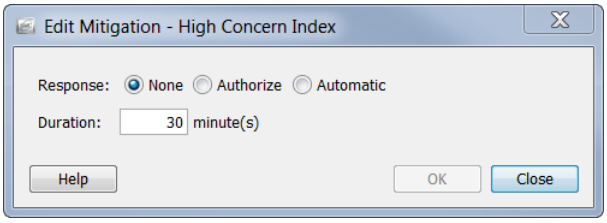
   You are returned to the Edit Policy dialog.

5. To edit behavior, tolerance, or threshold settings for an alarm category, select the alarm category you want to edit.

6. Click **Edit Settings**. The Edit Settings dialog opens.



7. Change settings as necessary and click **OK** when finished. You are returned to the Edit Policy dialog.
8. To specify when and how mitigation should occur, select the alarm category you want to edit.
9. Click **Edit Mitigation**. The Edit Mitigation dialog opens.



10. Change settings as necessary and click **OK** when finished. You are returned to the Edit Policy dialog.

Note:

- When settings are not configured for an alarm category, *No Settings* appears in the Settings column.
- When mitigation settings are not configured for an alarm category, *None* appears in the Mitigation column.

11. To enable an alarm category, select the check box for the alarm category in the Enabled column.

Tip:

Use the Enable All Categories or Disable All Categories button to affect all alarm categories at once.

12. To issue an alarm for the security event, select the check box in the Alarm column.
13. Do one of the following:
    - To apply the settings without exiting the Edit Policy dialog, click **Apply > Close**.

- To apply the settings and exit the Edit Policy dialog, click **OK**.

Notes:

- For information about the different types of settings for alarms, refer to "Alarms" on page 266.
- For recommended settings for specific alarms, refer to "Recommendations" on page 272.

Security Events

Use this section to configure the security events used by a policy, edit settings or mitigation of alarms associated with a CI, and enable or disable security events. Refer to the following table for an explanation of the check boxes on the Security Events tab.

Select this check box...	To do the following...
Impact Source Policy	If you want a host policy or role policy to override the source setting defined in the existing effective policy. **Note:** This column is available only when you are editing a host policy or role policy.
Enable Source	If you want a security event that is enabled for the source to contribute points to any applicable alarm categories.
Alarm Source	If you want a security event that is enabled for the source to also trigger its associated alarm.
Impact Source Target	If you want a host policy or role policy to override the source setting defined in the existing effective policy. **Note:** This column is available only when you are editing a host policy or role policy.
Enable Target	If you want a security event that is enabled for the target to contribute points to any applicable alarm categories.
Alarm Target	If you want a security event that is enabled for the target to also trigger its associated alarm.

Refer to the following regarding situations in which specific types of security events will not alarm:

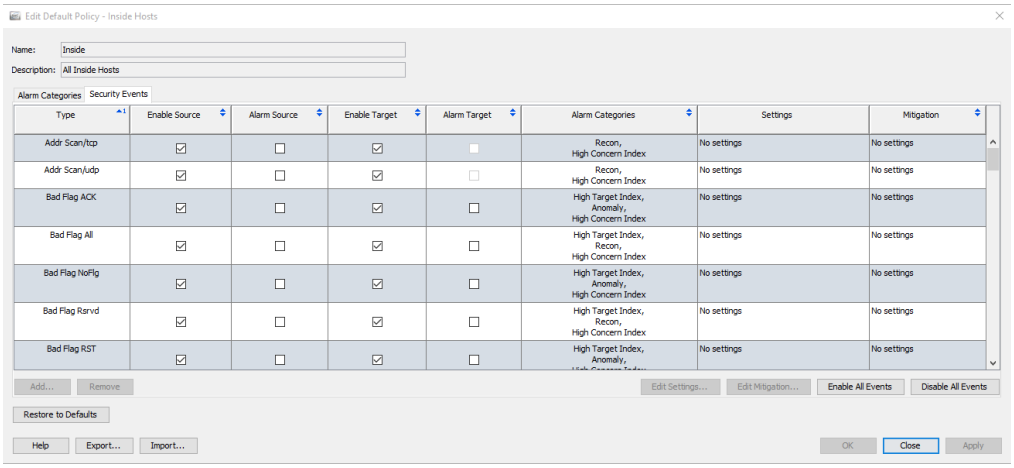
- One to Many (e.g., Max Flows Initiated) - This type of security event cannot alarm at the target, so therefore you cannot select the Alarm Target check box for this security event.
- Many to One (e.g., SYNs Received) - This type of security event cannot alarm at the source, so therefore you cannot select the Alarm source check box for this security event.

You can disable an alarm in the Alarm Table by right-clicking and selecting Disable Alarm(s). This will de-select the Alarm Source and Alarm Target check boxes for the corresponding security event; the Enable Source and Enable Target check boxes remain selected. This creates a new host policy where the Enable Source and Enable Target columns are selected but the Alarm Source and Alarm Target columns are de-selected.

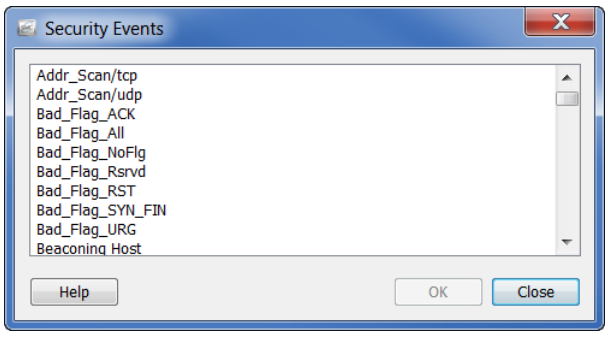
Configuring Security Events in Host Policies

To configure a security event, complete the following steps:

1. From an Edit Policy dialog, click the **Security Events** tab.



2. Do one of the following:
   - If you need to add a security event, go to step 3.
   - If you need to edit a security event, go to step 5.
3. To add a security event, click **Add**. The Security Events dialog opens.



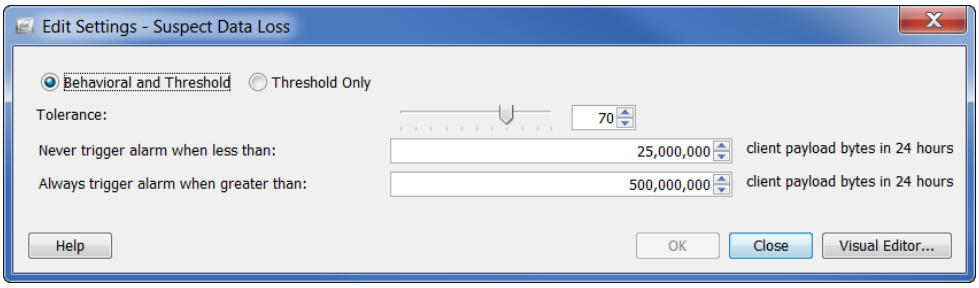
4. Do one of the following:
   - To add one security event, select the event and click **OK**.
   - To add several events listed in sequence, select the first event, press the **Shift** key, select the last event in the sequence, and click **OK**.

- To add several events not listed in sequence, press the **Ctrl** key, select each event, and click **OK**.

You are returned to the Security Events tab.

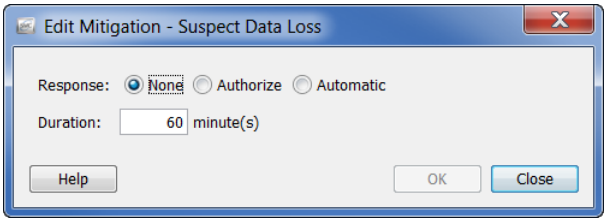
5. To edit behavior, tolerance, or threshold settings for a security event, select the security event you want to edit.
6. Click **Edit Settings**.

   The Edit Settings dialog opens.



7. Change settings as necessary and click **OK** when finished. You are returned to the Edit Policy dialog.
8. To specify when and how mitigation should occur, select the security event you want to edit.
9. Click **Edit Mitigation**.

   The Edit Mitigation dialog opens.



10. Change settings as necessary and click **OK** when finished. You are returned to the Edit Policy dialog.

Note:

- When settings are not configured for an alarm category, *No Settings* appears in the Settings column.
- When mitigation settings are not configured for an alarm category, *None* appears in the Mitigation column.

11. Depending on whether you want to enable the source security event, target security event, or both to contribute points to any applicable alarm categories, click the applicable Enable check boxes.

Tip:

Use the Enable All Events or Disable All Events button to affect all events at once.

12. Depending on whether you want to issue an alarm for the source security event, target security event, or both, click the applicable Alarm check boxes.
13. Do one of the following:
    - To apply the settings without exiting the Edit Policy dialog, click **Apply > Close**.
    - To apply the settings and exit the Edit Policy dialog, click **OK**.

Notes:

- For information about the different types of settings for alarms, refer to "Alarms" on page 266.
- For recommended settings for specific alarms, refer to "Recommendations" on page 272.

CREATING AND EDITING POLICIES

As stated in the previous section, when you are responding to an alarm, you need to determine which policy triggered that particular alarm. It is very likely that you will be in the Alarm Table or within the **Alarm** section of the Host Snapshot when you are ready to edit or disable an alarm. So, for our following examples we will use a scenario in which you, the user, are inside the Alarm Table and ready to edit or disable an alarm.

When responding to an alarm, complete the following steps:

1. Determine what the triggering host is. For example, is it a server, is it a desktop, etc.? Also, determine if the behavior is normal. If the behavior is normal, proceed to the following steps. If the behavior is not normal, follow standard escalation procedures to investigate the cause of the alarm.
2. If the triggering host is not a member of a pre-defined group (e.g., backup servers, firewalls, proxies) that already has a default role policy created for it, but it can logically belong to one, then assign this host to the pre-defined group to which it logically fits. (Refer to "Assigning Hosts to a Pre-defined Group" on page 252.)

   For example, if the triggering host is a backup server, then since there is a pre-defined group called "Backup Servers," a default role policy has already been created for it. Therefore, you can assign this triggering host to the Backup Servers group. It will then automatically be assigned to the default role policy for Backup Servers.
3. If the triggering host is not a member of a pre-defined group and does not logically fit into one, but it does belong to another role policy, then edit the role policy to which it belongs. (Refer to "Editing Role Policies" on page 258.)

   If the triggering host is not a member of a pre-defined group and does not logically fit into one, but it does belong to a host policy, then edit the host policy to which it belongs. (Refer to "Editing Host Policies" on page 264.)
4. If the triggering host does not belong to any role policy or host policy, you can do one of the following:

   - Edit either the Inside Hosts default policy or the Outside Hosts default policy that manages this host (whichever one applies). (Refer to "Editing Inside Hosts/Outside Hosts Default Policies" on page 239.)

CAUTION:

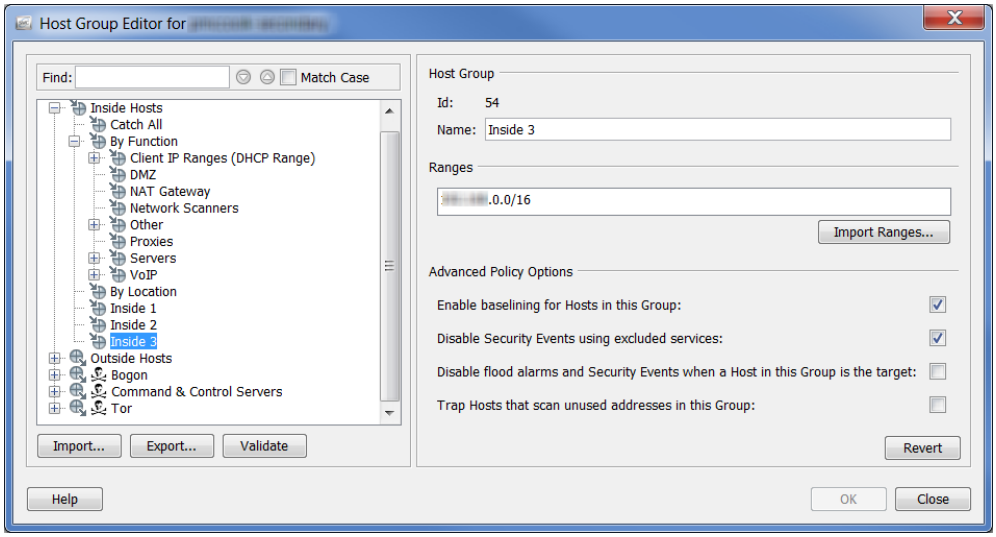
Remember that any edits you make to the Inside Host default policy or the Outside Hosts default policy will affect global settings.

   - Create a role policy for this host. (Refer to "Creating Role Policies" on page 253.)
   - Create a host policy for this host. (Refer to "Creating Host Policies" on page 260.)

Assigning Hosts to a Pre-defined Group

To assign a host to a pre-defined group, complete the following steps:

1. On the Enterprise page tree menu, click the domain to which the triggering host(s) belongs.
2. From the Main Menu select **Configuration > Edit Host Groups**. The Host Group Editor dialog for the domain you clicked in the Enterprise Tree opens.
3. In the left window, click the group to which you want to assign the triggering host(s). The IP addresses of any hosts already a member of this group are displayed in the Ranges field on the right side of the dialog.



Tip:

To quickly move a single host to a group, right-click the host within any document and select **Configuration > Manage Host Groups**. When the Host Groups dialog for that host opens, select the desired group from the top section of the dialog, and then click **OK**.

4. Complete any of the following steps to add IP addresses to the group you specified in step 3.
   - In the Ranges field, type the IP address of the triggering host(s).
   - If you are adding more than one host and they exist within a range, then in the Ranges field type the desired IP address ranges of the triggering hosts.
   - If you are adding more than one host and you have an existing file containing the IP addresses of the triggering hosts, then click **Import Ranges** to import the IP addresses.
5. Click **OK**. The Enterprise page tree menu automatically updates to include all newly added IP addresses to the group you specified in step 3.

Creating Role Policies

Remember, you create role policies when you want a group of hosts that share a common function or similar attributes to be assigned the same alarm thresholds.

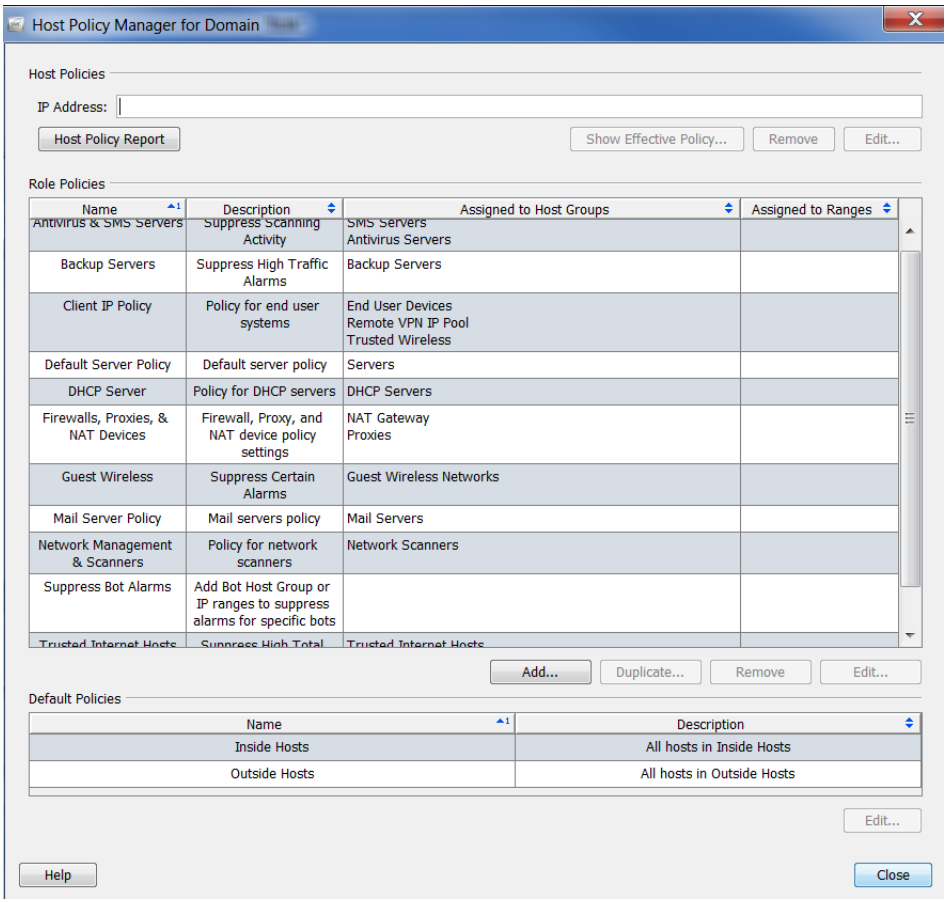
If no host policy exists for an IP address, Stealthwatch uses the corresponding alarm settings from the Role Policy governing that host. A host could exist in multiple Role Policies and inherit **all** the settings of the Role Policies. So, since more than one Role Policy can be applied to a specific host and the threshold settings for each policy can be different, multiple alarms could be triggered if the host behavior exceeds values defined within each role policy.

Note:

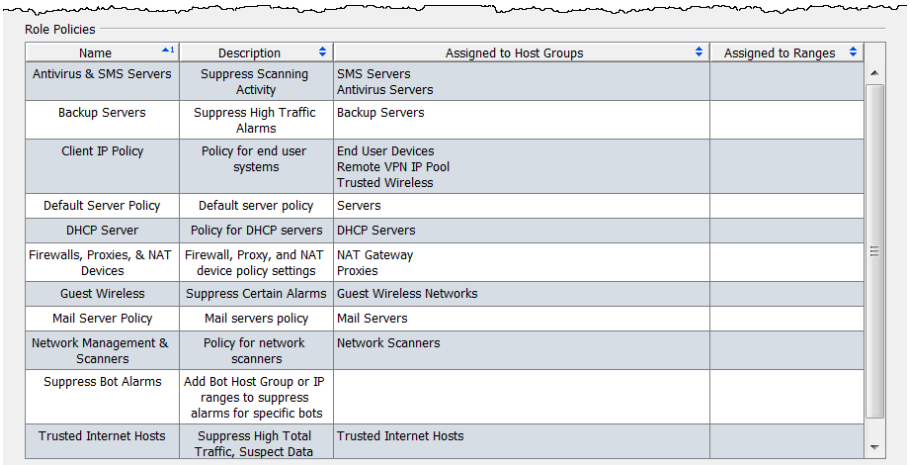
To prevent confusion, it is best if you do not use multiple role policies with the same alarm unless there is a need to trigger alarms based on different values (e.g., for different teams).

To add a role policy, complete the following steps:

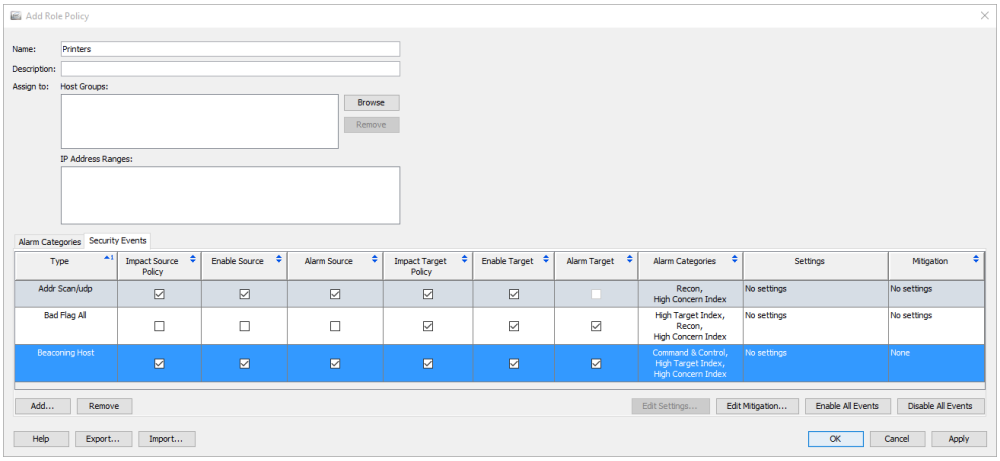
1. From the Main Menu select **Configuration > Host Policy Manager**. The Host Policy Manager dialog opens.



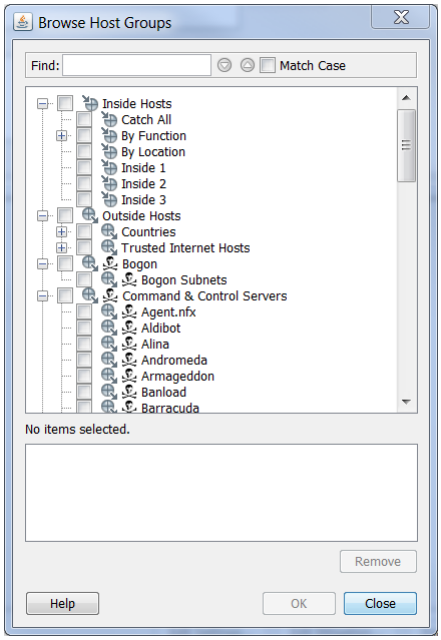
2. In the Host Policy Manager dialog, within the **Role Policies** section, click **Add**.



The Add Role Policy dialog opens.



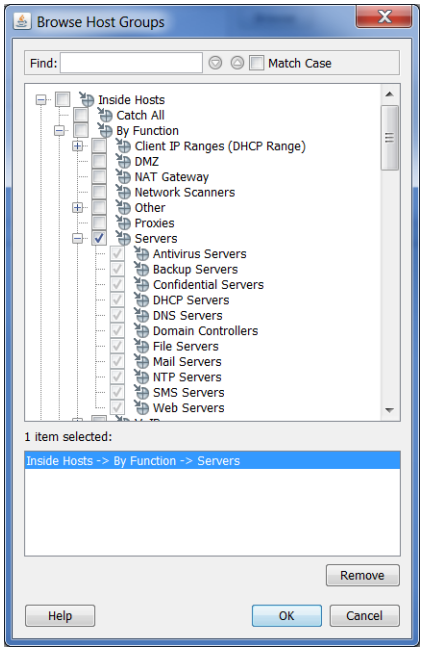
3. In the Name field, type a name for the policy you are adding (e.g., Accounting Department).
4. In the Description field, type a description (optional).
5. Complete one of the following steps:
   - Type specific host IP addresses or ranges in the IP Address Ranges field.
   - In the "Assign to: Host Groups" field, click **Browse**. The Browse Host Groups dialog opens.



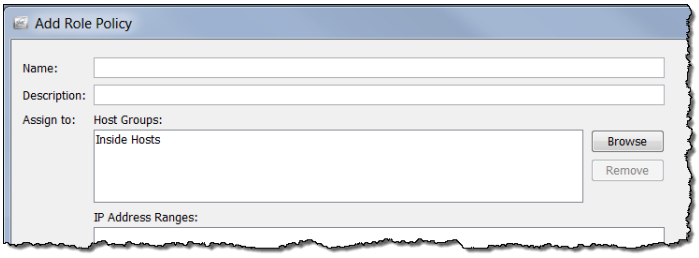
Note:

Each host group has property settings that can prevent certain alarms. To view these settings, right-click a host group in the Enterprise tree menu and select **Configuration > Host Group Properties**. The Edit Host Group dialog opens. The Advanced Policy Options are listed at the bottom.

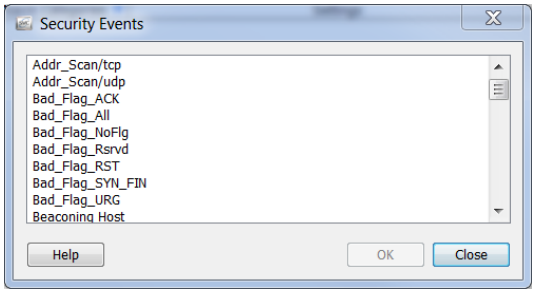
6. Click the host group(s) to which the policy applies. If you click a parent host, all hosts under it will automatically be selected.



7. Click **OK**. The group(s) is now displayed in the **Assign to: Host Groups:** section in the Add Role Policy dialog.



8. Click **Add** at the bottom of the Add Role Policy dialog. The Security Events dialog opens.

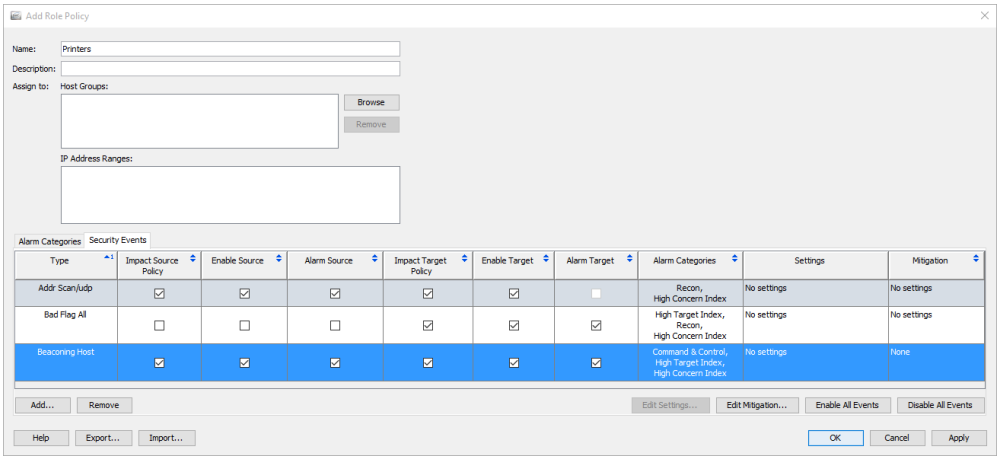


9. Click the alarm(s) to edit, and then click **OK**.

Note:

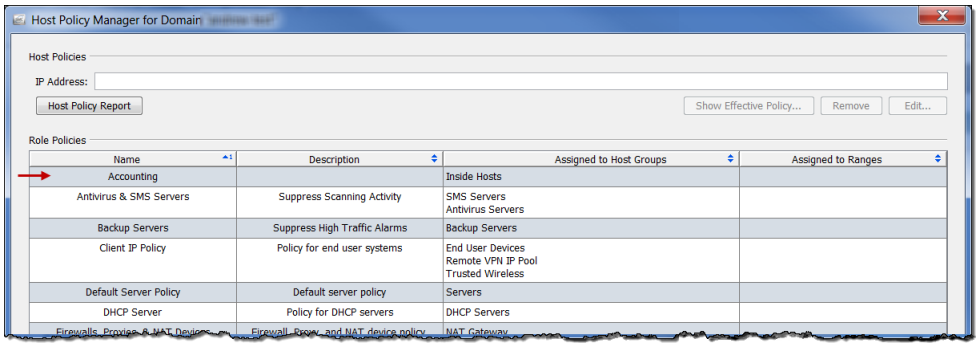
To select more than one alarm, hold the **Ctrl** key and click each alarm you want to add. To select a range of alarms, click the alarm that is at the top of the range you want to select, hold the **Shift** key, and then click the alarm that is at the bottom of the range you want to select.

The alarms display on the Add Role Policy dialog.



10. Select the check box for each alarm that you want this policy to trigger.

11. Click **Apply > Close**. The policy appears on the Host Policy Manager dialog in the Role Policies section.



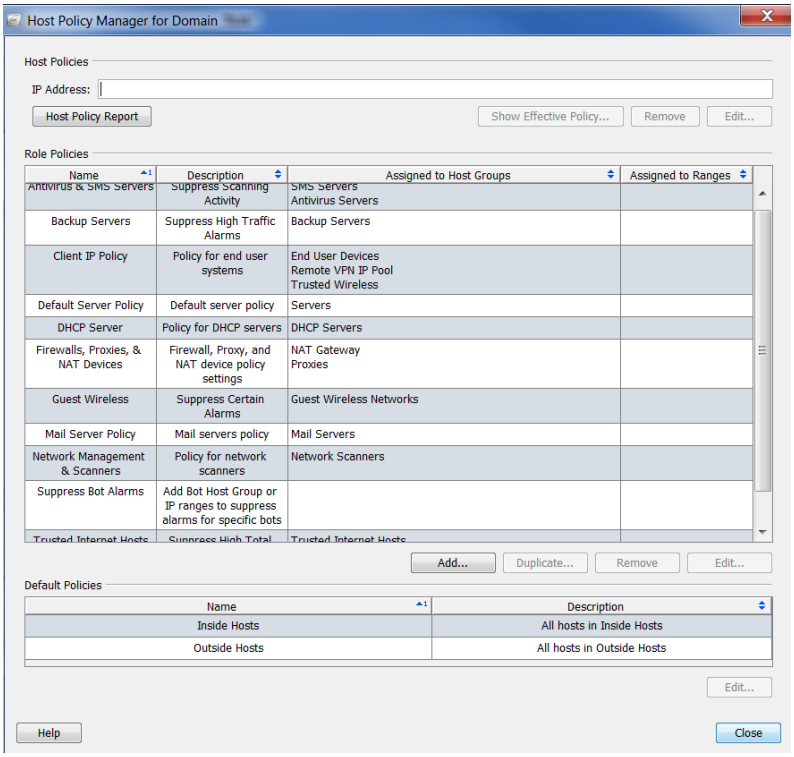
Tip:

If you find that you are about to assign a role policy to a range of IP addresses or to multiple ranges of IP addresses, then instead create a host group for these IP addresses, and then assign to this host group a role policy.

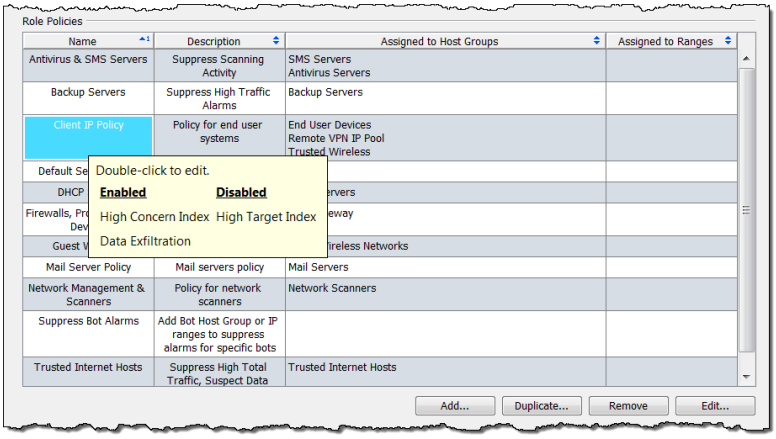
Editing Role Policies

To edit a Role Policy, complete the following steps:

1. From the Main Menu select **Configuration > Host Policy Manager**. The Host Policy Manager dialog opens.



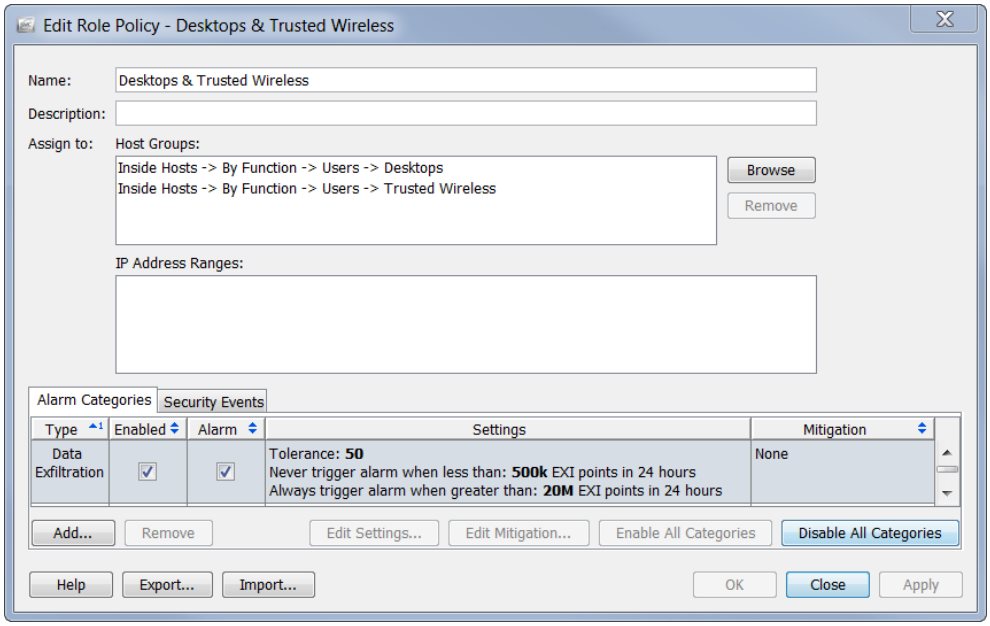
2. In the Host Policy Manager dialog, within the **Role Policies** section, click the name of the role policy you want to edit, and then click **Edit**.



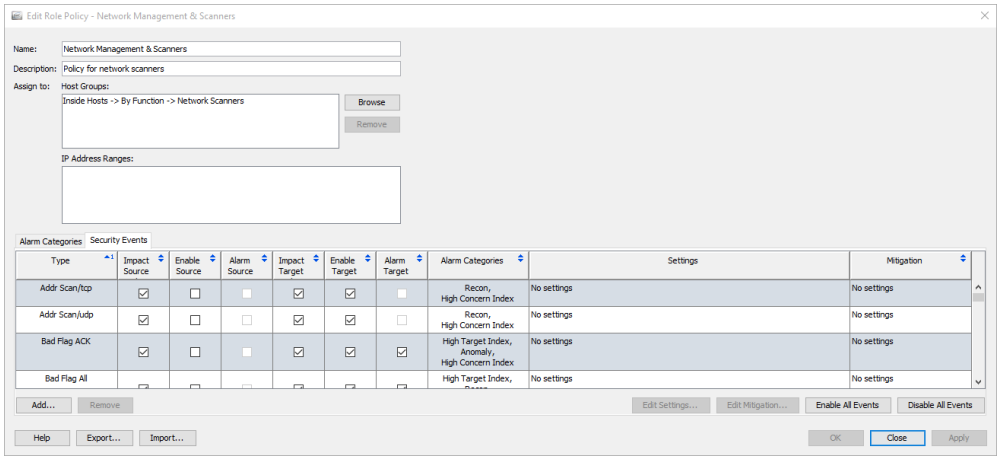
Note:

If you hover the cursor over an entry, a list of all enabled and disabled alarms appears. In the previous example, no alarms have been disabled; therefore, there are no disabled alarms listed.

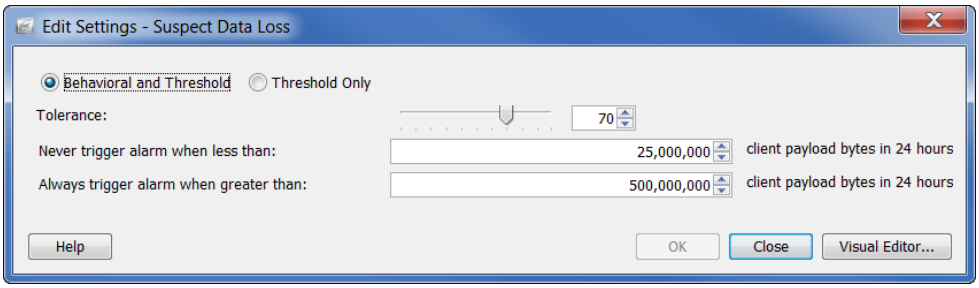
The Edit Role Policy dialog opens. The Alarm Categories tab opens by default.



Depending on which alarm you want to edit, you may need to click the Security Events tab.



3. Double-click the alarm you want to edit (ensure you click within the Settings column). The Edit Settings dialog for that alarm opens.



4. Complete your edits and click **Close** when finished.

Notes:

- For information about the different types of settings for alarms, refer to "Alarms" on page 266.
- For recommended settings for specific alarms, refer to "Recommendations" on page 272.

Creating Host Policies

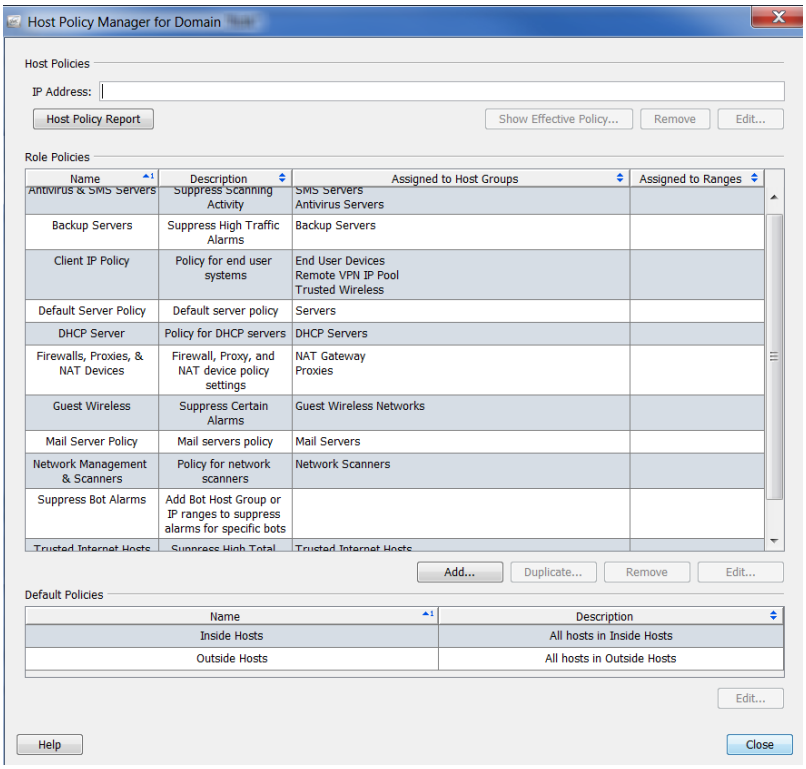
As you have learned, if a host policy exists for an IP address, Stealthwatch will use the corresponding alarm category settings from the host policy to determine when to trigger an alarm against that host, regardless of whether or not this IP address is assigned to other alarms at the role or default policy levels. Remember, the host policy always overrides both the role policy and the default policy.

You will want to edit the host policy (as opposed to editing the role policy or the default policy) for an individual host. If you are looking at an individual host and

notice, for example, that in the alarm table you see a certain alarm triggered for a particular host that should not be triggered, or should be triggered at a different threshold, you will want to modify the effective host policy for that particular host.

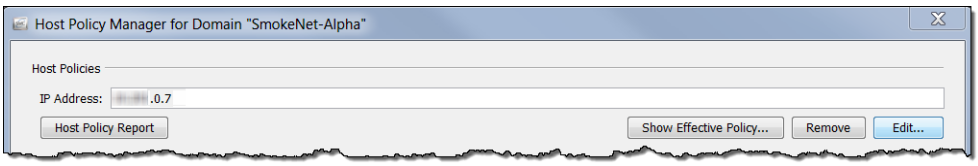
To add a host policy, complete the following steps:

1. From the Main Menu select **Configuration > Host Policy Manager**. The Host Policy Manager dialog opens.

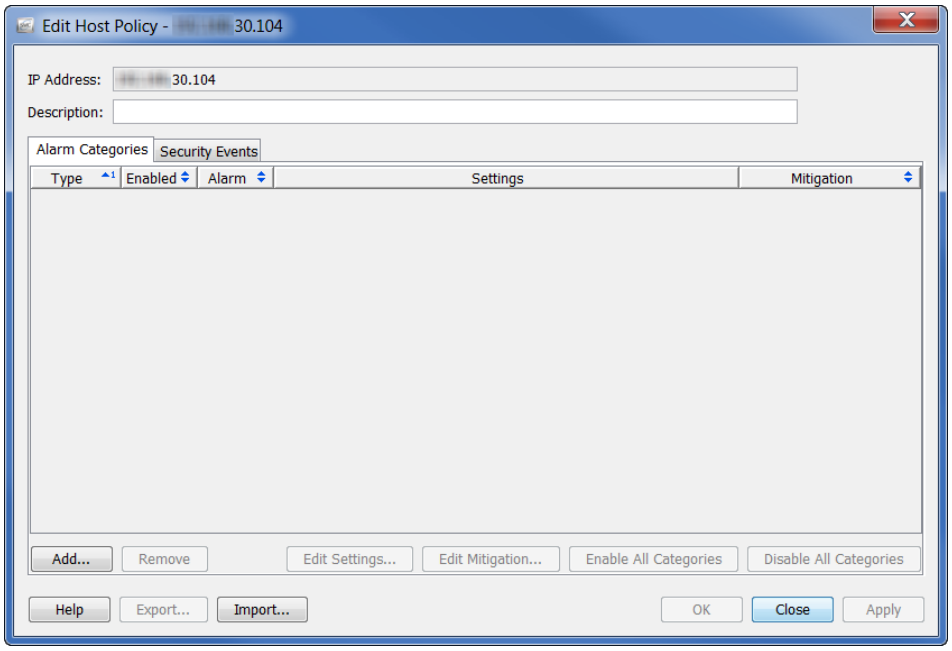


2. Within the **Host Policies** section, enter the IP address of the host to which you are adding a host policy.

3. Click **Edit**.

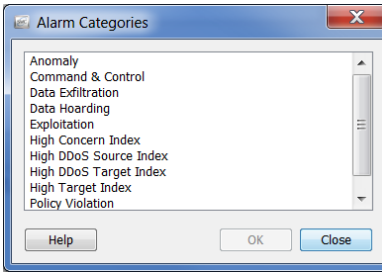


The Edit Host Policy dialog opens. The Alarm Categories tab is open by default.



4. Click **Add**. The Alarm Categories dialog opens.

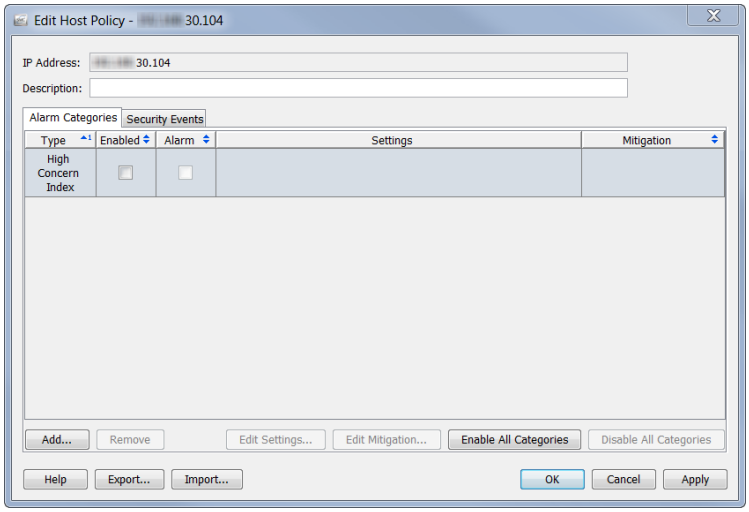
5. Click the alarm categories you want to add to this Host Policy, and then click **OK**.



Note:

To select more than one alarm, hold the **Ctrl** key and click each alarm you want to add. To select a range of alarms, click the alarm that is at the top of the range you want to select, hold the **Shift** key, and then click the alarm that is at the bottom of the range you want to select.

The alarm categories display on the Edit Host Policy dialog.



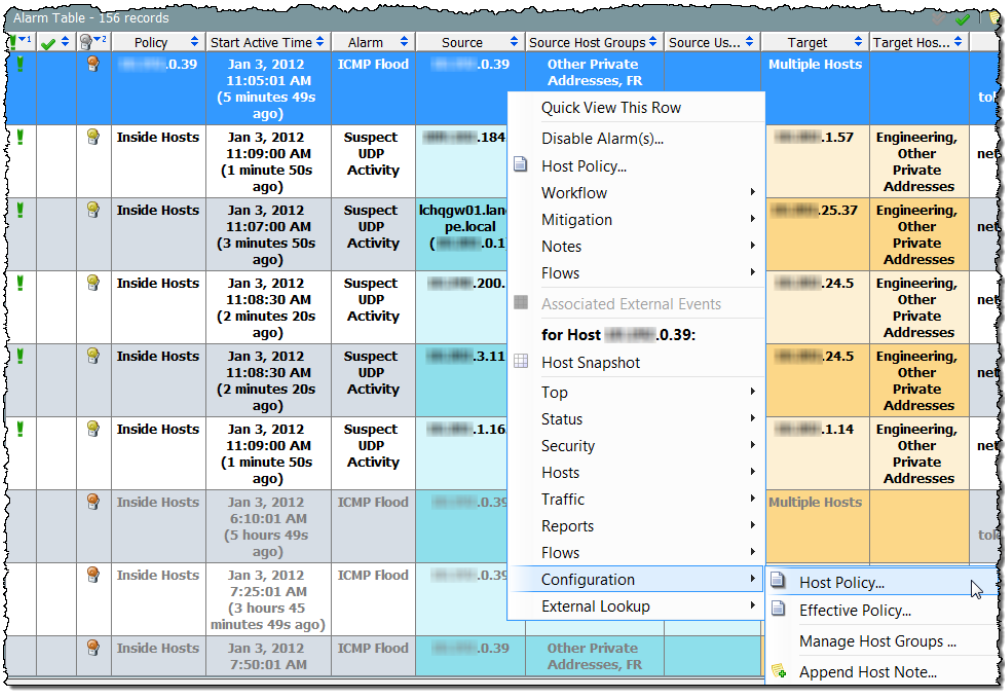
Note:

Ensure that the Enabled column contains a checkmark for every alarm that you want this policy to trigger.

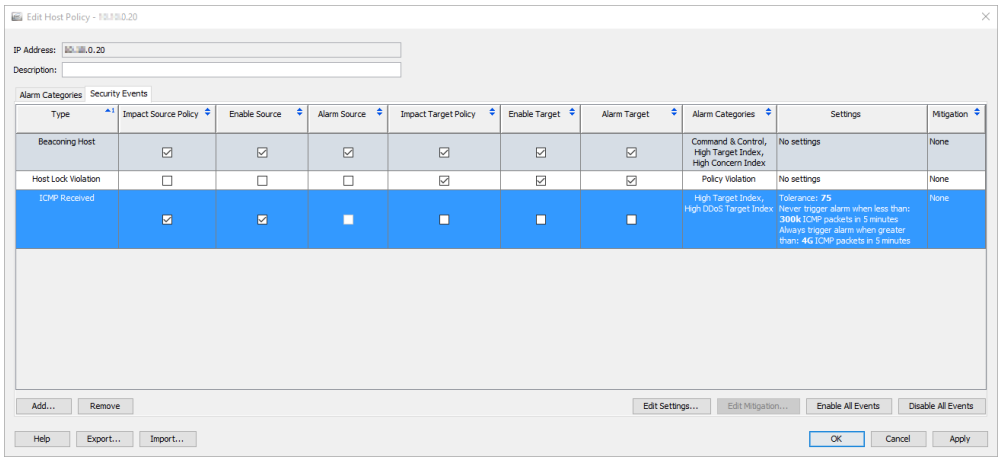
Editing Host Policies

To edit a host policy, complete the following steps:

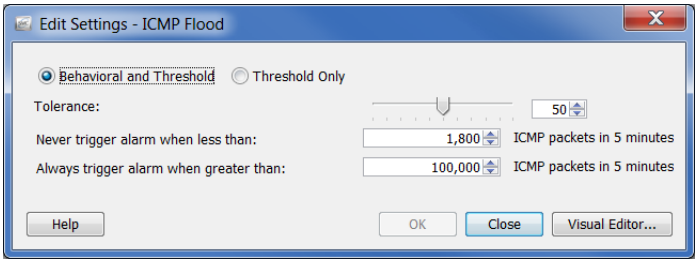
1. Right-click the host IP address and select **Configuration > Host Policy**.



The Host Policy dialog for that host opens.



2. Double-click the alarm that you want to modify. The Edit Settings dialog for that alarm opens.



3. Make your changes and click **Close**.

Notes:

- For information about the different types of settings for alarms, refer to "Alarms" on page 266.
- For recommended settings for specific alarms, refer to "Recommendations" on page 272.

Variance-based Alarms vs. On/Off Alarms

Alarms are triggered when host activity experiences a significant change from past behavior. The tolerance (i.e., sensitivity) of these types of alarm can be changed using the Host Policy Manager. These alarms are referred to as variance-based alarms. The following table lists the variance-based alarms:

Note:

The alarm categories are also variance-based.

Variance-based Alarms	
Anomaly	Port Scan
Brute Force Login	Relational High Total Traffic
Command & Control	Relational High Traffic
Data Exfiltration	Relational ICMP Flood
Data Hoarding	Relational Low Traffic
Exploitation	Relational Max Flows Initiated
High Concern Index	Relational Max Flows Served
High DDoS Source Index	Relational SYN Flood
High DDoS Target Index	Relational UDP Flood
High File Sharing Index	Relational Round Trip Time
High SMC Peers	Relational Server Response Time
High Target Index	Relational TCP Retransmission Ratio
High Traffic	Relational High Total Traffic
High Volume Email	Slow Connection Flood
ICMP Flood	Span Source
ICMP Received	SSH Reverse Shell
Mail Rejects	Suspect Data Hoarding
Mail Relay	Suspect Data Loss
Max Flows Initiated	SYN Flood
Max Flows Served	SYNs Received

Variance-based Alarms	
Packet Flood	Target Data Hoarding
New Flows Initiated	Touched
New Flows Served	Trapped Host
Policy Violation	UDP Flood
Recon	UDP Received

The main advantage of this approach is that you can adjust the system so that the number of alarms that occur matches your organizational needs. That is, if you prefer many alarms (i.e., you can tolerate only a slight change from the expected behavior), you can lower the tolerance setting in the associated policy. Conversely, if you prefer fewer alarms (i.e., you can tolerate significant change from the expected behavior), you can raise the tolerance setting. Essentially, each of the settings for the variance-based alarm is attached to a numerical value, and this value can be adjusted up or down.

The thresholds used in variance-based alarms are generated from a baseline based on recent activity and a configured tolerance. This gives a host the ability to change its behavior over time without losing the capability to alarm if its behavior changes too radically. Tolerance provides a way to control how much change is acceptable. In essence, you have the ability to adjust the sensitivity of the alarm's threshold level (i.e., to "turn down the noise" to whatever level you want).

With variance-based alarms, a host must reach a certain level of deviation from its baseline before an alarm will trigger. For instance, if the tolerance level for the High Total Traffic alarm has been set to 50, then the system ignores the lowest 50% of the values over the expected value (the host's baseline), but will alarm on the ones above that value.

Note:

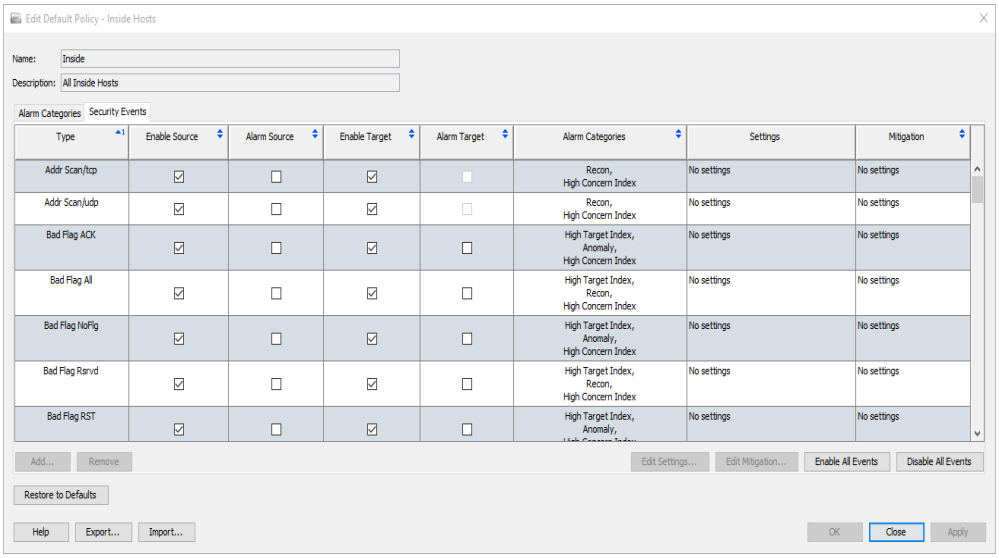
For detailed information about alarm settings, refer to "Settings for Variance-based Alarms" on page 269.

The second type of alarm is the alarm which you can either turn on or off. The criteria for triggering this type of alarm differs from that of the variance-based alarm. In the case of the alarm that simply has an on/off setting, the host's behavior must match certain conditions that must all coincide with each other before this type of alarm is triggered. If all of these conditions do not exist, then the alarm will not trigger. For instance, in order for a worm activity alarm to trigger, **all** of the following behavior must have occurred:

- A source host has scanned multiple sub-nets.
- At least one of the target hosts has connected to the source host.
- This target host has transferred information to the source host.

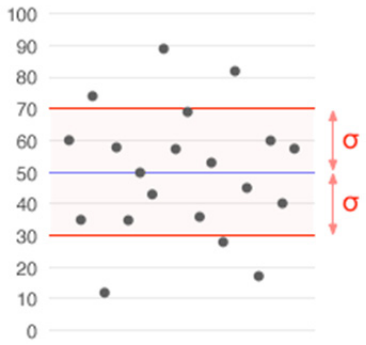
If even one of these conditions does not exist, the alarm will not trigger.

You can determine which alarms are variance-based and which alarms are on/off by looking in the Settings column in the Edit Default Policy dialog. If an alarm is variance-based, then the tolerance values that have been indicated for that alarm are displayed. If an alarm is on/off, then the entry “No settings” is displayed.



Settings for Variance-based Alarms

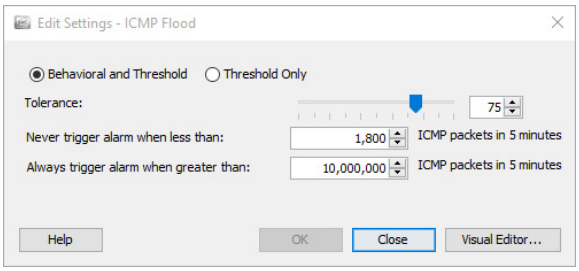
As stated in the previous section, the thresholds used in variance-based alarms are generated from a baseline based on recent activity and a configured tolerance. Tolerance is defined as “the number of standard deviations from the norm,” and provides a way for you to adjust the sensitivity of the alarm’s threshold level.



A data set with a mean of 50 (shown in blue) and a standard deviation (σ) of 20.

Standard deviation is a widely-used measurement of variability or diversity used in statistics. It shows how much variation there is from the average (i.e., mean, or expected value). A low standard deviation indicates that the data points tend to be very close to the mean, whereas high standard deviation indicates that the data points are spread out over a large range of values.

The following example shows the Edit Settings dialog for a variance-based alarm.



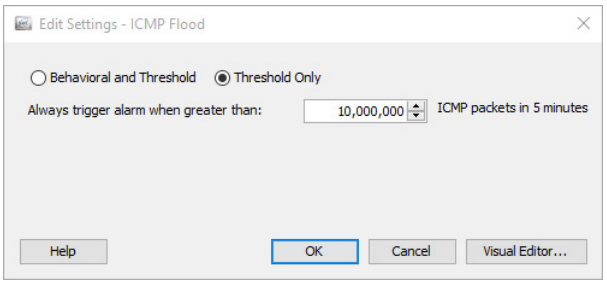
Variance-based alarms contain the following adjustable settings:

- Behavioral and Threshold – When this option is selected, the dialog shows the tolerance setting, the minimum threshold, and the maximum threshold.
  - Tolerance – A relative number between 0 and 100 that indicates how much to allow actual behavior to exceed expected behavior before alarming. This allows the user to define what is “significantly different”.
    - A tolerance of 0 means to alarm for any values over the expected value; it is very sensitive and will result in a lot of alarms.
    - A tolerance of 100 is the highest level at which the alarm is tolerated. It greatly reduces the number of times an alarm is triggered; however, only disabling an alarm will result in the alarm never being triggered.

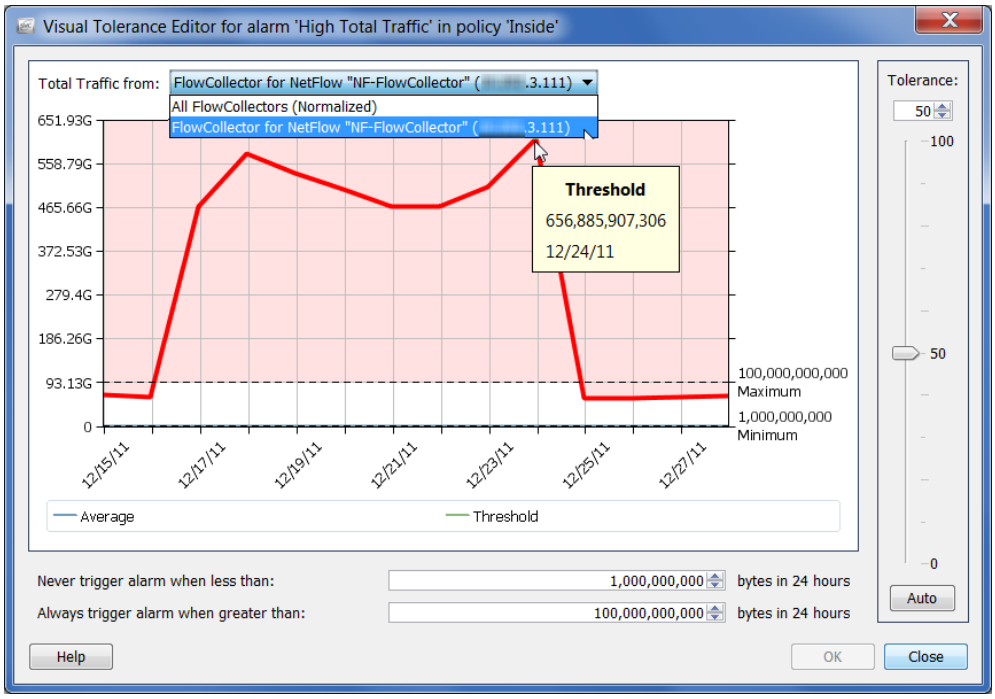
- A tolerance of 50 indicates that the host will ignore the lowest 50% of the values over the expected value, but it will alarm on the ones above that value.

- *Never trigger alarm when less than:* Also known as the *minimum threshold*, this is a static value that indicates the lowest value to allow for triggering an alarm. The alarm will not trigger when the observed value falls below this setting. In other words, even if a host is greatly over its expected value, if it is not more than the minimum indicated in this dialog, then do not trigger an alarm.
- *Always trigger alarm when greater than:* Also known as the *maximum threshold*, this is a static value that indicates the highest value to allow without triggering an alarm. The alarm will trigger when the observed value exceeds this setting. In other words, if a host's value exceeds the maximum indicated in this dialog, even if it is expected for that host, then trigger an alarm.

- Threshold Only – When this option is selected, the dialog shows only the maximum threshold setting.



Click **Visual Editor** to access the Visual Editor dialog. The Visual Tolerance Editor is a graphical way to adjust the settings of a host or host group policy for a specific alarm, as shown in the following example.



Note:

If only one Flow Collector is being used, then from the **Total Traffic from** drop-down list at the top of the screen, click the **Flow Collector** option to see the actual values for the related alarm. If multiple Flow Collectors are being used, then click the **Normalized** option to normalize the values.

RECOMMENDATIONS

This section provides recommendations for fine-tuning your network in the event you are receiving an excessive number of unnecessary alarms. The recommendations are broken down in this section according to some of the most common alarm types, listed in alphabetical order.

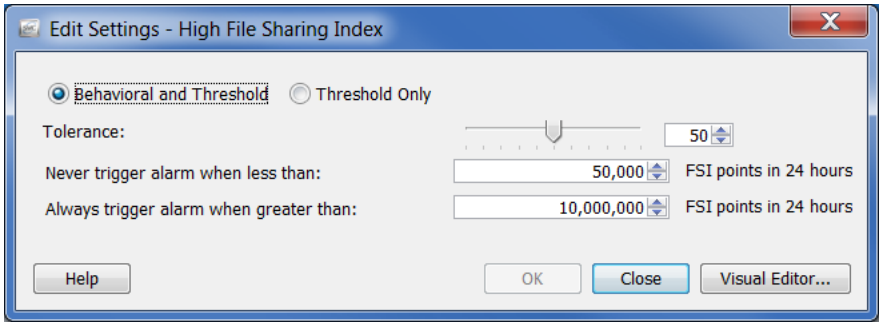
Notes:

- To read detailed descriptions of these alarms and others, refer to the "Alarm List" topic in the *Stealthwatch Desktop Client Online Help*.
- For more information about how you can adjust the settings for the alarms listed below, refer to "Settings for Variance-based Alarms" on page 269.

High File Sharing Index

The High File Sharing Index (FSI) alarm indicates that file sharing activity has exceeded the FSI threshold as defined in the Host Policy Manager. If the hosts causing the High FSI alarms are used for file sharing, you can complete one of the following steps to reduce the number of unnecessary alarms you are seeing:

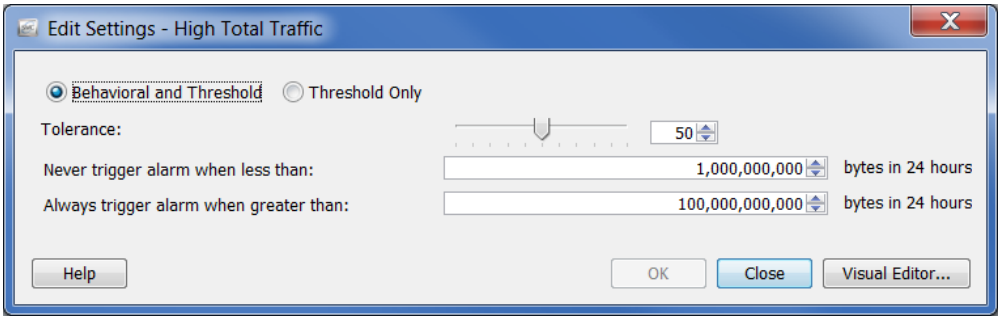
- Disable the High File Sharing Index alarm for policies affecting the hosts/host groups in question by clicking the **Enabled** check box in the corresponding policy/policies to removed the checkmark.
- Raise the High File Sharing Index alarm threshold or tolerance setting for policies affecting the hosts/host groups in question.



High Total Traffic

The High Total Traffic alarm indicates that the total traffic inbound plus the total traffic outbound exceeds the policy setting for the host. If you are uncomfortable with the amount of high total traffic alarms being seen, adjust the settings in the corresponding policy/policies.

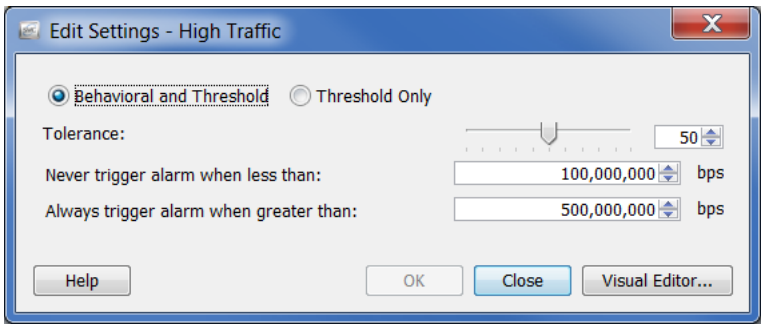
Raise the policy setting for the hosts or host groups in question above the average number of bytes being reported.



High Traffic

The High Traffic alarm indicates that the host traffic rate averaged over a five-minute period has exceeded the limit of the acceptable traffic values. If you are uncomfortable with the amount of high traffic alarms being seen, adjust the settings in the corresponding policy/policies.

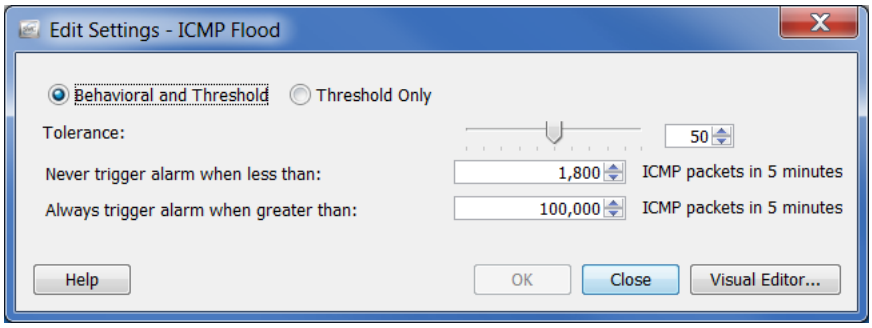
Raise the policy setting for the hosts or host groups in question above the average number of bytes being reported.



ICMP Flood

The ICMP Flood alarm indicates that the source host has sent an excessive number of ICMP packets in the last five minutes. This may indicate a Denial of Service (DoS) attack or a non-stealthy scanning activity. To troubleshoot this situation, find out what kind of host is causing the alarm. It may be a management server sending a large number of pings to a host on the network.

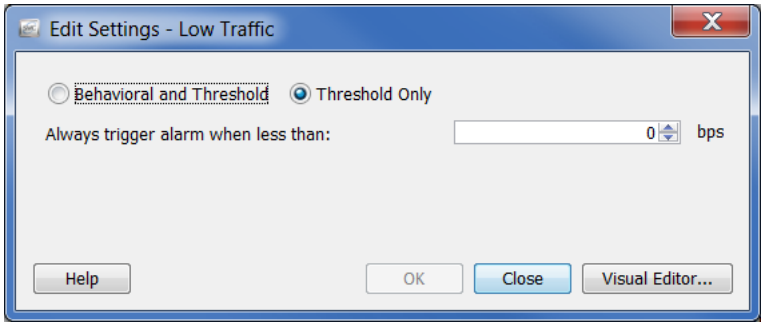
To stop the alarm, disable the ICMP Flood alarm for the hosts/host groups in question by clicking the **Enabled** check box in the corresponding policy/policies to remove the checkmark.



Low Traffic

The Low Traffic alarm indicates that the host traffic rate averaged over a five-minute period has fallen below the minimum acceptable traffic values. If you are uncomfortable with the amount of low traffic alarms being seen, adjust the settings in the corresponding policy/policies.

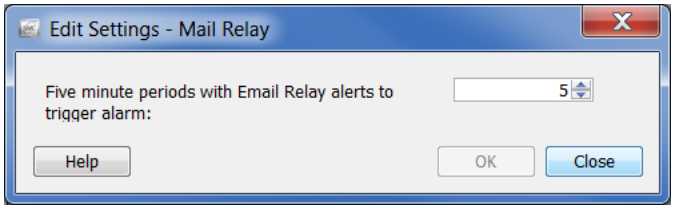
Raise the policy setting for the hosts or host groups in question above the average number of bytes being reported.



Mail Relay

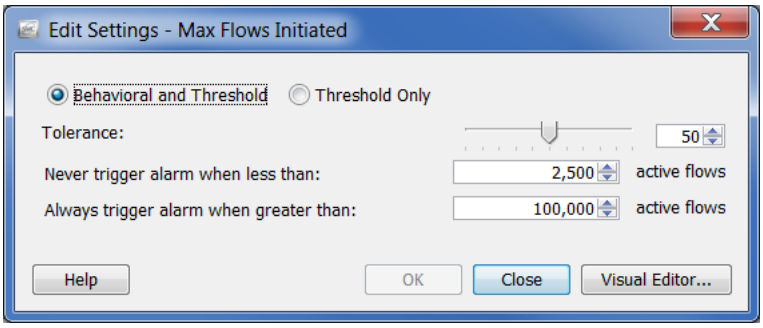
The Mail Relay alarm indicates that the target host may be operating as an Email relay. If these are true mail servers, you can disable the Mail Relay alarm for the hosts/

host groups in question by clicking the **Enabled** check box in the corresponding policy/policies to remove the checkmark.



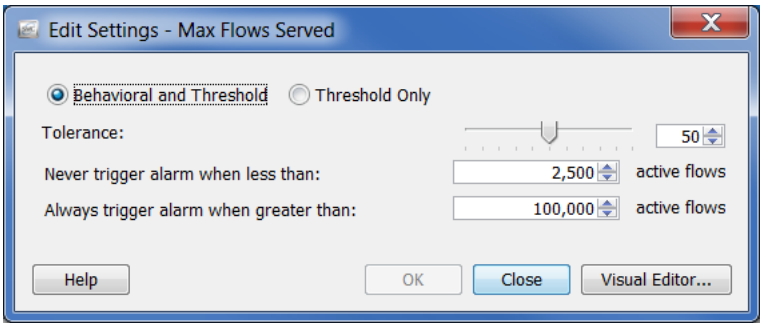
Max Flows Initiated

The Max Flows Initiated alarm indicates that a host has initiated more flows than allowed, that number having been specified in the corresponding *Always trigger alarm when greater than* policy setting. Adjust the settings, especially if this is a domain controller.



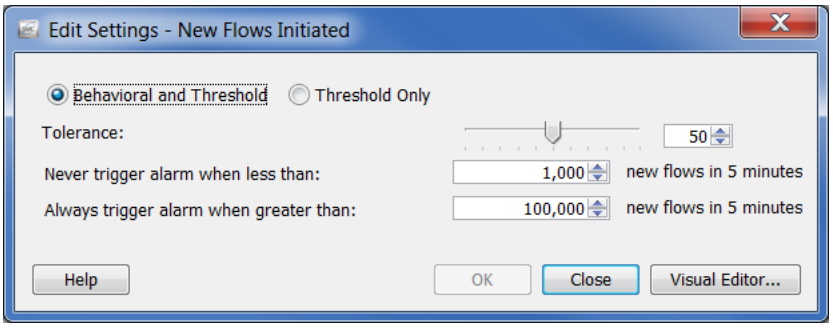
Max Flows Served

The Max Flows Served alarm indicates that a host has served more flows than allowed, that number having been specified in the corresponding *Always trigger alarm when greater than* policy setting. Adjust the settings, especially if this is a domain controller.



New Flows Initiated

The New Flows Initiated alarm indicates that a host has exceeded a policy setting for the total number of new flows initiated in a five-minute period. Adjust the settings, especially if this is a domain controller.



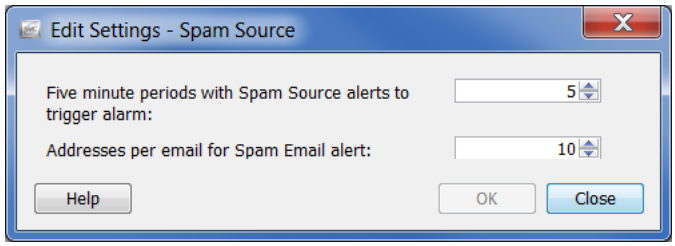
New Flows Served

The New Flows Served alarm indicates that a host has exceeded a policy setting for the total number of new flows served in a five-minute period. Adjust the settings, especially if this is a domain controller.

Spam Source

The Spam Source alarm indicates that the source host may be sending Email spam. If the host is a mail server, disable the Spam Source alarm for the hosts/host groups in question by clicking the **Enabled** check box in the corresponding policy/policies to remove the checkmark.

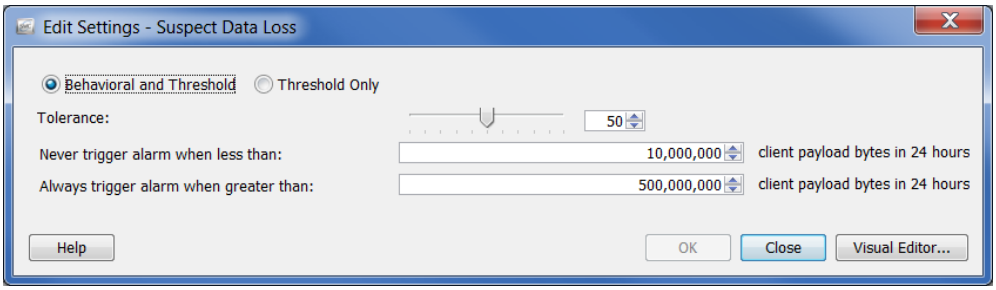
If the host is not a mail server, it may be infected.



Suspect Data Loss

The Suspect Data Loss alarm indicates that the total TCP and UDP payload data for an Outside host group exceeds the policy setting. If you are uncomfortable with the number of Suspect Data Loss alarms being seen, disable this alarm for known high-traffic outside host groups (e.g., YouTube, Facebook, business partners).

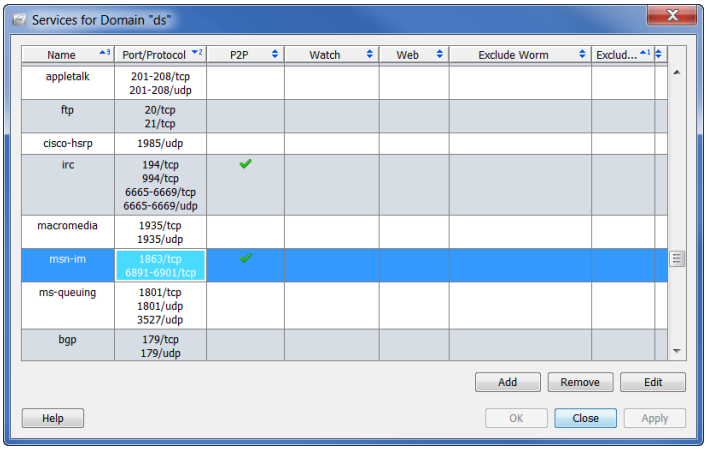
Then, adjust the settings on the policy/policies for important hosts or host groups. Raise the threshold above the average number of bytes being reported.

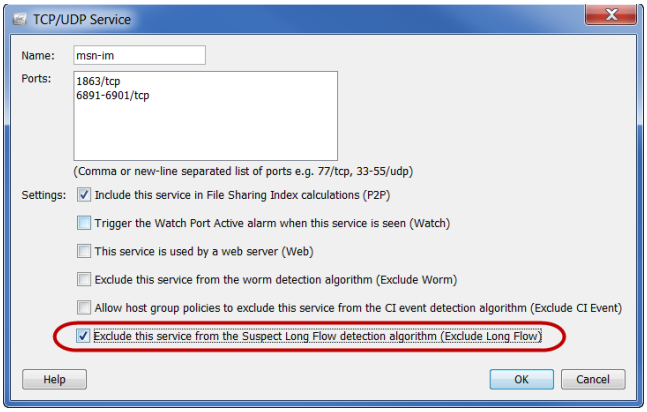


Suspect Long Flow

The Suspect Long Flow alarm indicates that an IP communication between an inside and an outside host exceeds the setting for "seconds required to qualify a flow as long duration." This alarm detects suspicious channels of communication such as spyware, remote desktop technologies (such as gotomypc.com), VPNs, IRC botnets, and other covert means of communication. Inside hosts using IM technologies are prone to causing this kind of alarm due to the flow lasting longer than the maximum value allowed (default = 9 hours).

You can exclude IM technologies, such as AOL AIM (port 5190), Yahoo IM (TCP port 5050), and MSN Messenger (TCP port 1863) from generating Suspect Long Flow alarms by modifying the configured service. From the Main Menu select **Configuration > Services**. The Services dialog for the applicable domain opens.





Select the row that contains the name of the service you are editing, and then click **Edit** at the bottom of the screen. Click the **Exclude this service from the Suspect Long Flow detection algorithm (Exclude Long Flow)** check box to add a checkmark.

Alternatively, you can create an Outside host group for an authorized network, such as a business partner, and then disable the Suspect Long Flow alarm in the corresponding policy/policies.

Note:

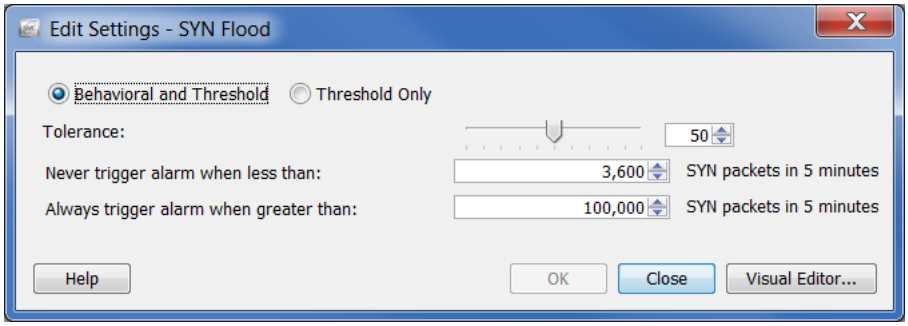
The Suspect Long Flow alarm is always raised against the Inside Host, regardless of the client/server relationship. If this alarm is disabled for an Outside Host, any Inside Host connecting to that Outside Host is excluded from this alarm.

Suspect UDP Activity

The Suspect UDP Activity alarm indicates that a host that has been scanning multiple hosts on UDP ports has successfully sent a single large packet to another host. This type of behavior is consistent with many single-packet UDP-based worms such as SQL Slammer and Witty. Investigate this alarm immediately.

SYN Flood

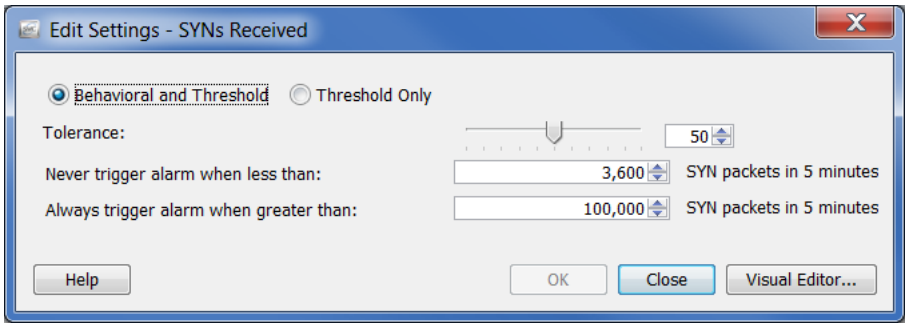
The SYN Flood alarm indicates that a host has sent an excessive number of TCP connection requests (SYN packets) in a five-minute period. Investigate this alarm to see if a DOS attack or non-stealth scanning activity is under way.



SYNs Received

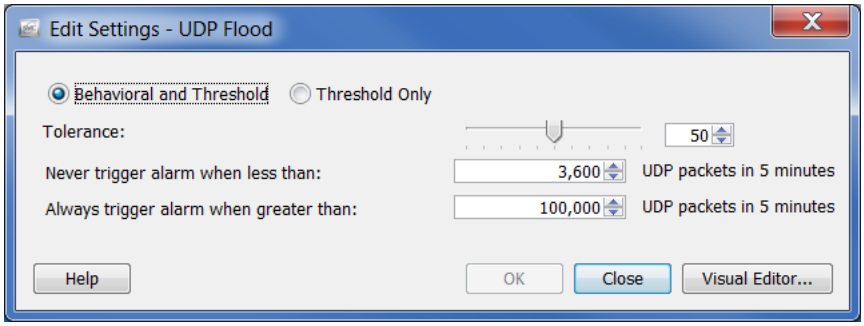
The SYNs Received alarm indicates that a host has received too many unanswered TCP connection requests (SYN packets) in a five-minute period. This alarm may indicate a distributed (many-to-one) DoS attack.

However, it is common for servers to receive a large number of SYN packets. If this is the case, raise the *Never trigger alarm when less than* setting above the average number of alarms you are seeing. You may want to isolate servers that receive more SYN packets than others into a separate host group, such as Web servers versus application servers.



UDP Flood

The UDP Flood alarm indicates that the source IP has sent an excessive number of UDP packets in the last five minutes. Investigate this alarm to see if a DOS attack or a non-stealth scanning activity is under way.



Worm Activity

The Worm Activity alarm indicates that a host has scanned and connected on a particular port across more than one subnet. The details section of this alarm specifies the port on which the activity was observed.

It is normal for domain controllers to perform address scanning on UDP ports and ping scanning. If the Worm Activity alarms are occurring in host groups with domain controllers, you can help prevent these alarms by removing the checkmarks from the **Addr_Scan/udp** and **Ping** check boxes on the Security Events tab for the High Concern Index alarm in the corresponding policy/policies.

12

WORKING WITH DOCUMENTS

OVERVIEW

This chapter describes processes such as how to save an SMC document with a specific set of layout settings and filter settings, add a document to your list of login documents, create a DAR file, share a document, generate a document on a regular basis, and email a document to others.

This chapter includes the following topics:

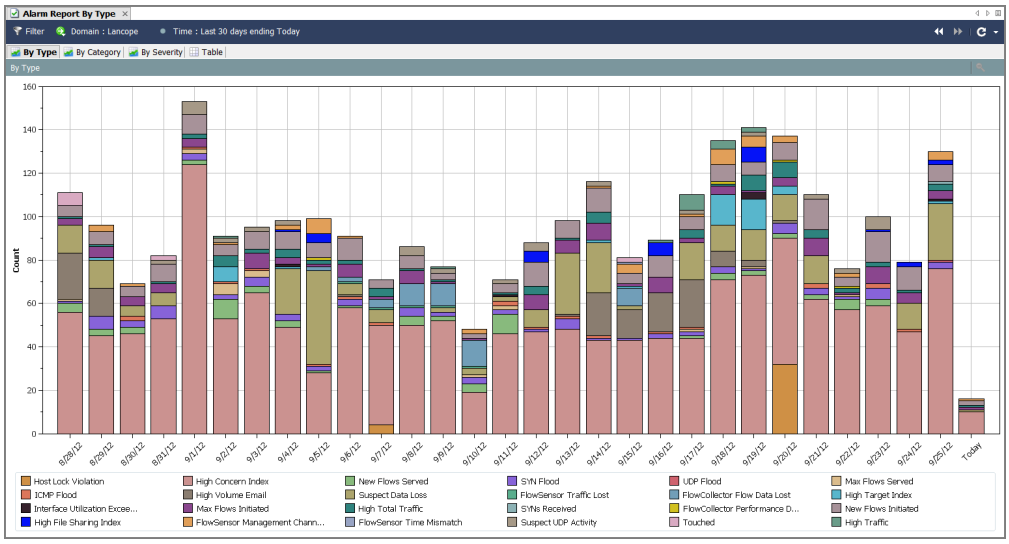
- Saving Documents
- Sharing Documents
- Scheduling Documents

SAVING DOCUMENTS

If you have rearranged the layout of an SMC document and you want to save that layout to be used later, save the document. When you save a document, it is saved to the SMC appliance for retrieval at any time.

To save a document, complete the following steps:

1. Open the document you want to save. As an example, we will open the Alarm Report By Type document.



2. Make any desired changes to the layout or filter settings.
3. (Optional) From the SMC Main Menu select **File > Print Settings**, and within the dialog that opens configure how you would like the document to look each time it is printed. Click **OK** to save changes.
4. (Optional) To see how the document would appear as a PDF, select **File > Print Preview**.

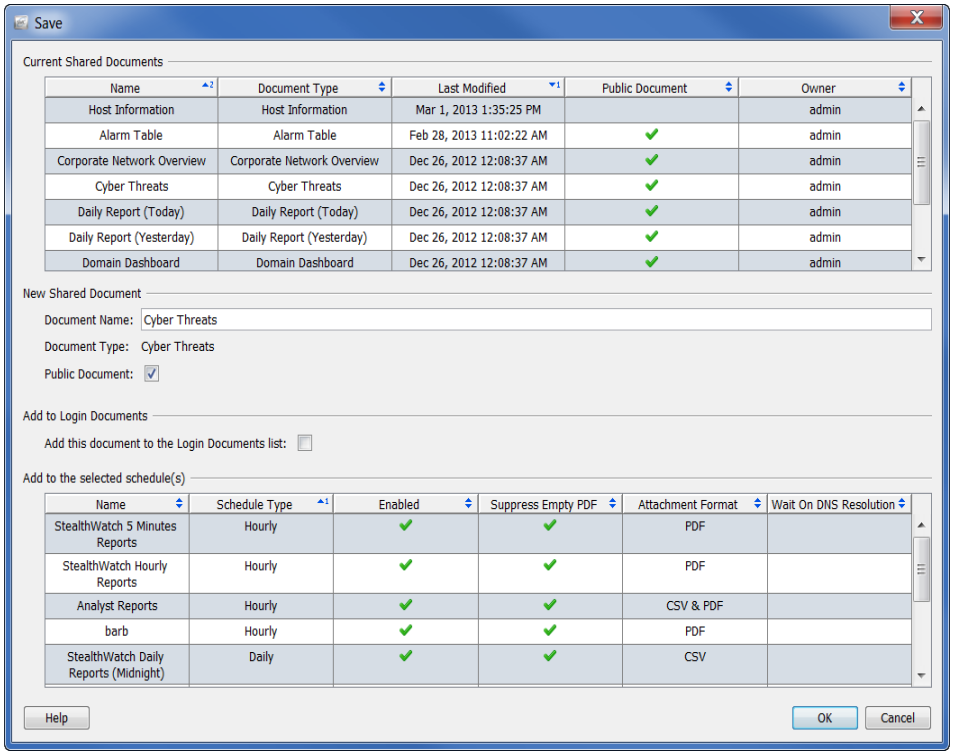
Note:

If you want to make and retain changes to the document layout (such as change the column positions or change which columns appear), select File > Use Settings as Default. These changes will be in effect the next time you open the document.

5. Do one of the following:
   - From the SMC Main Menu, select **File > Save** if you simply want to replace the previous version using the same name.
   - From the SMC Main Menu, select **File > Save As** if any of the following situations are applicable:
     - If you want to save a copy of the document with a new name.

- If you have created a new document and are saving the document for the first time.

  The Save dialog opens:



6. In the Name field, type a name for the document that you can easily recognize. (The system suggests a name for you.)
7. (Optional) If you want other users to be able to open this document under their user names, select the **Public** check box.

Note:

For more information about public documents, refer to "Public Documents" on page 291.

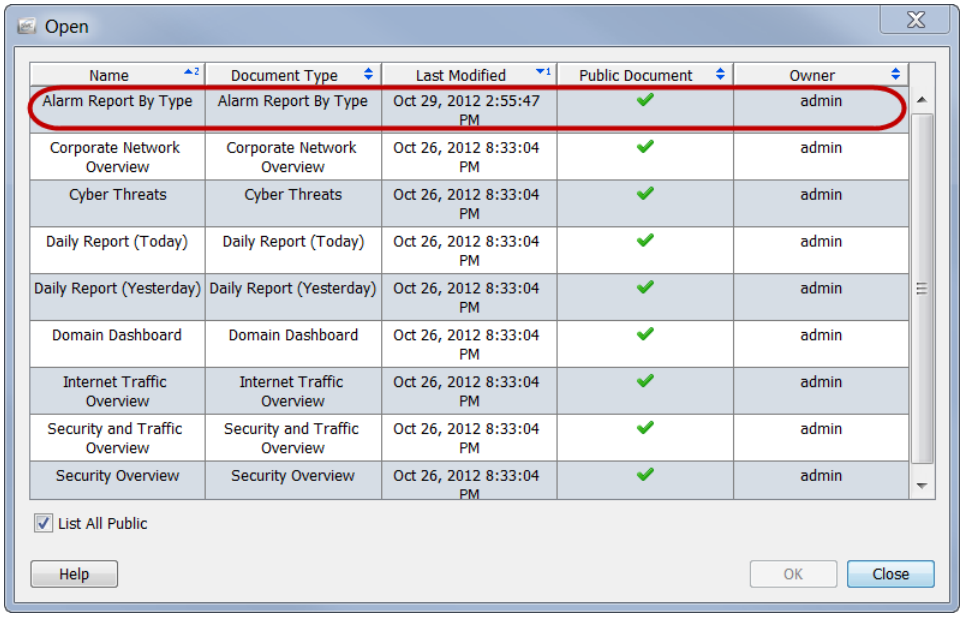
8. (Optional) If you want the document to open automatically every time you log in to the Stealthwatch Desktop Client under your user name, select the "Add this document to the Login Documents list" check box.

Note:

For more information about login documents, refer to "Login Documents" on page 286.

9. Click **OK**. The document is saved to the SMC appliance. You can now open this document under your user name, with the layout and/or filter settings you specified, on any computer with SMC access.

10. To open this document, from the SMC Main Menu, select **File > Open**. The Open dialog opens.



11. Select the document and click **OK**.

Note:

By default, only documents saved under your user name appear. To list all documents, including those created by other users, select the List All Public check box.

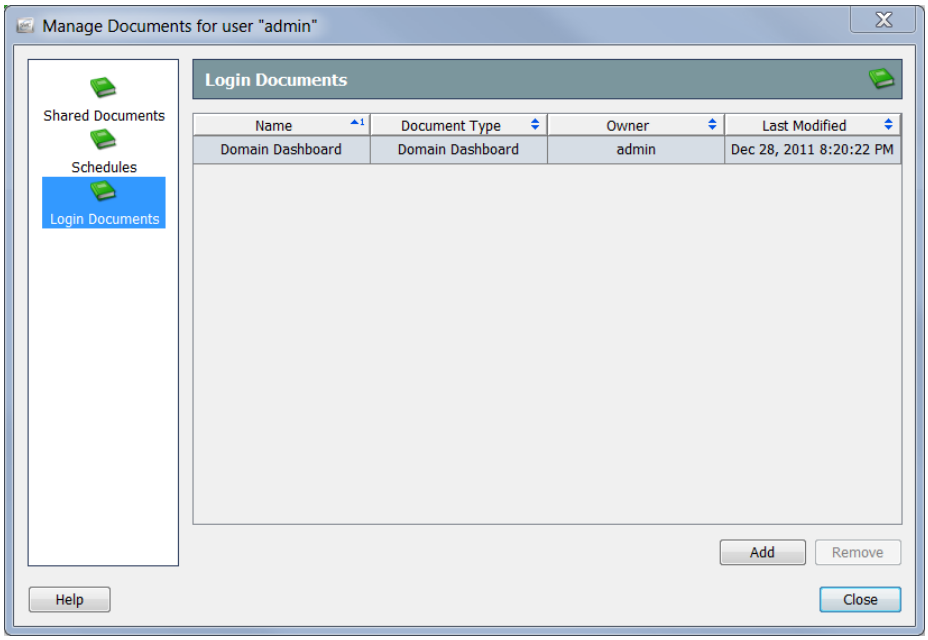
Login Documents

You may add any document to your list of login documents. A login document automatically opens each time you log in to the Stealthwatch Desktop Client. This feature is useful for viewing documents that you otherwise would open manually on a regular basis.

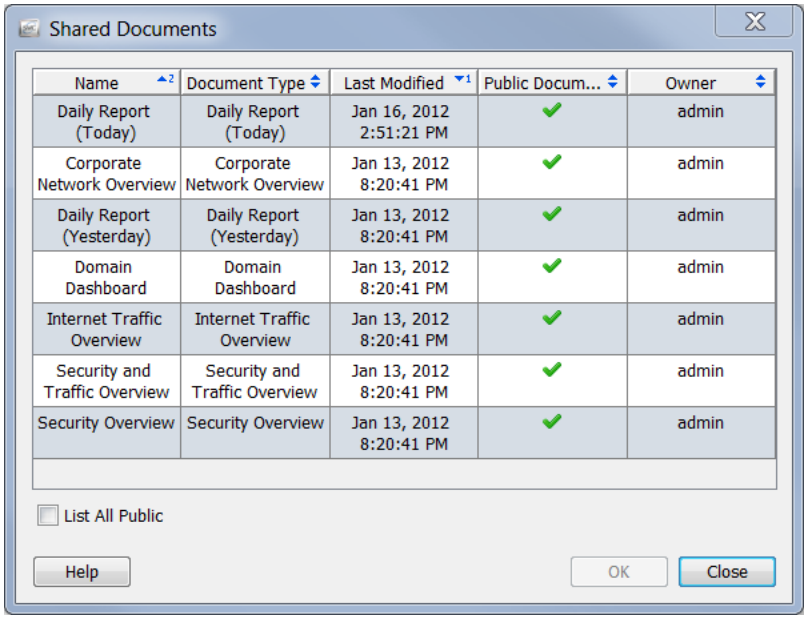
To make a document a login document, complete the following steps:

1. From the SMC Main Menu, select **File > Manage Documents**. The Manage Documents dialog opens.

2. Click the **Login Documents** icon. The Login Documents page opens.



3. Click **Add**. The Shared Documents dialog opens.



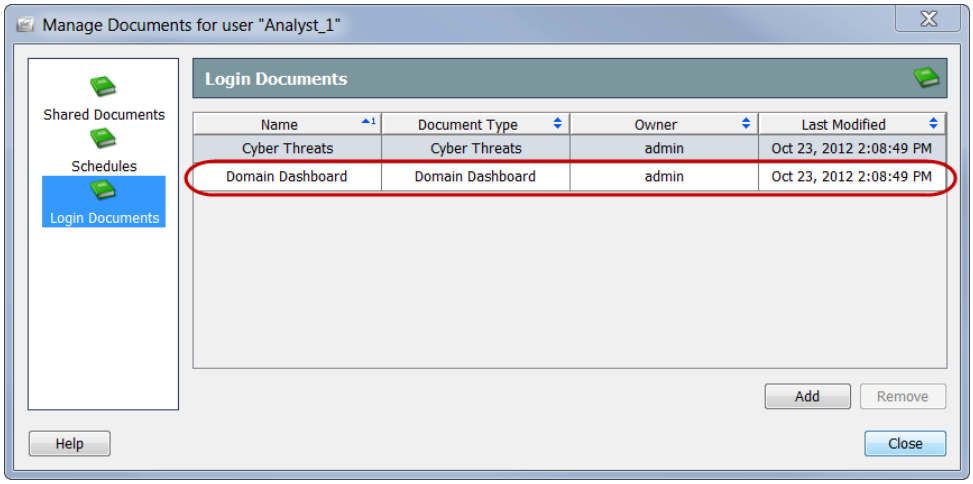
4. Select the “List All Public” check box to see all public documents that have been saved by other users.

5. Select the document(s) you want to add to the user's list of login documents. For this example, we will select the Domain Dashboard document.

Note:

To select more than one document, hold the **Ctrl** key and click each document you want to add. To select a range of documents, click the document that is at the top of the range you want to select, hold the **Shift** key, and then click the document that is at the bottom of the range you want to select.

6. Click **OK**. The Shared Documents dialog closes. The document(s) you selected appears in the user's list of login documents.



7. Click **Close** to exit the Manage Documents dialog.

SHARING DOCUMENTS

Two ways to share documents with other users are:

- Exporting them as DAR files
- Making them public

DAR Files

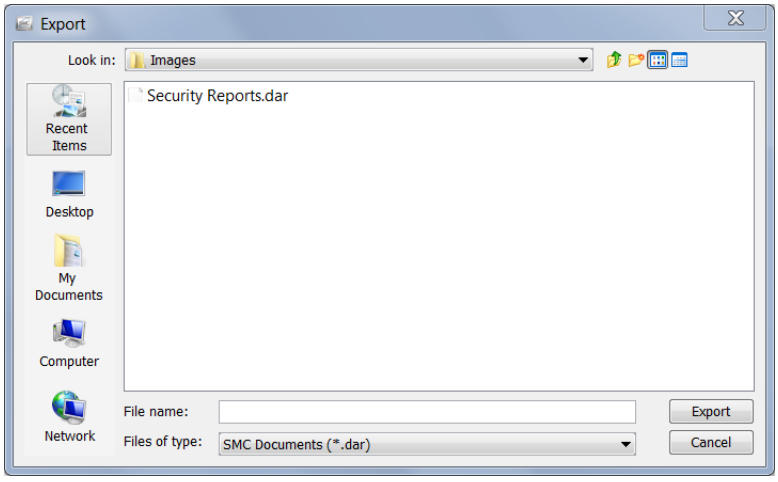
Exporting a document as a DAR file allows you to do things with a document such as the following:

- Copy it to your computer's hard drive.
- Copy it to a flash drive to use on another computer that has access to the SMC appliance.
- Share it with someone.

Exporting DAR Files

To export a document as a DAR file, complete the following steps:

1. Open the document you want to export.
2. Make any desired changes to the layout or filter settings.
3. From the SMC Main Menu, select **File > Export to DAR file**. The Export dialog opens.



4. Navigate to the location to which you want to export the document.
5. In the File name field, type a name for the file.

6. Click **Export**. The document is saved as a DAR file in the location you selected. In addition, the document tab assumes the new name.

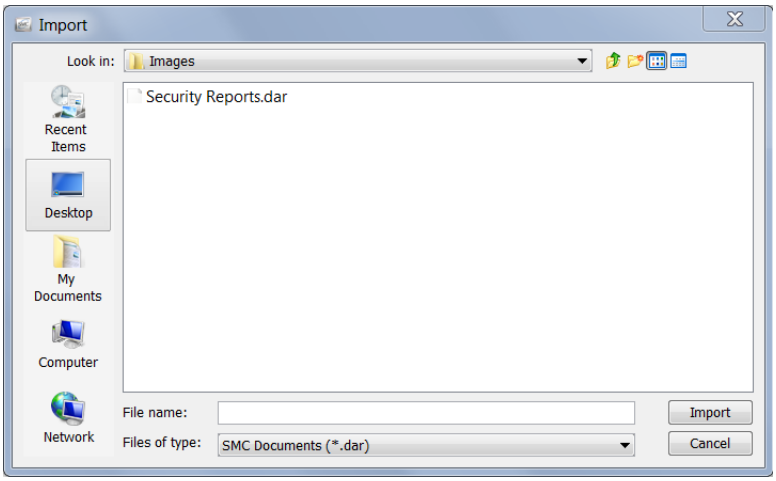
Note:

If you hover your cursor over the document tab, a tool tip appears, showing details about the document, such as the original document name and who created (“owns”) it.

Importing DAR Files

Once anyone has exported a document as a DAR file and provided it to you, you can open it any time in the Stealthwatch Desktop Client by importing it. To do this, complete the following steps:

1. From the SMC Main Menu select **File > Import DAR file**. The Import dialog opens.



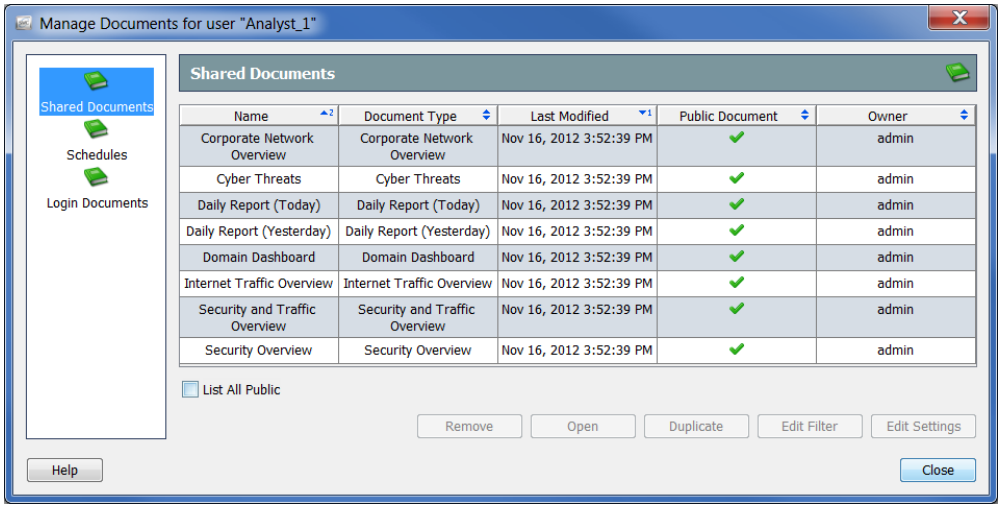
2. Navigate to where the DAR file is located.
3. Select the DAR file.
4. Click **Import**. The document opens in the Stealthwatch Desktop Client.

Public Documents

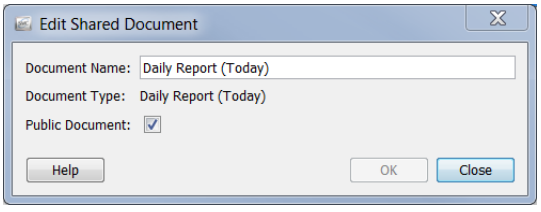
When you make a document public, you enable other users with access to the SMC appliance to view the document under their user names.

You can make a document public as you are saving it as described in "Saving Documents" on page 284. You can make a previously saved document public by completing the following steps:

1. From the Main Menu, select **File > Manage Documents**. The Manage Documents dialog opens.



2. Click the **Shared Documents** icon. The Shared Document page opens.
3. Select the desired document.
4. Click **Edit Settings**. The Edit Settings dialog opens.



5. Select the **Public Document** check box.
6. Click **OK** to exit the Edit dialog.
7. Click **Close** to exit the Manage Documents dialog.

   Any user with access to the Stealthwatch Desktop Client can view this document and all other documents that have been made public.

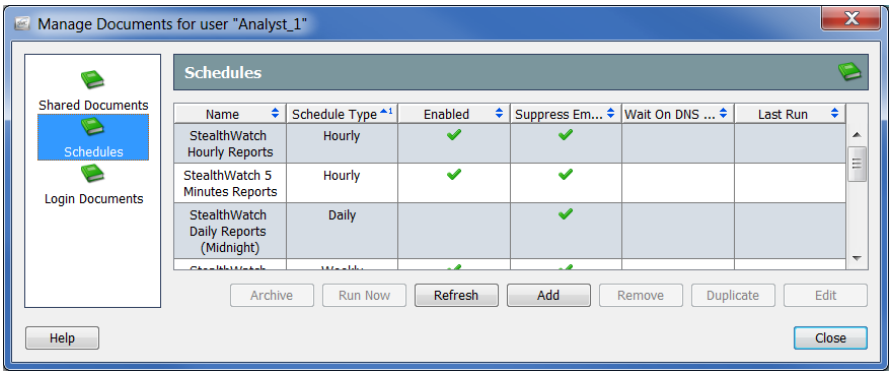
SCHEDULING DOCUMENTS

There may be situations in which you want to generate a document automatically using the same settings (e.g., filters, layout, time interval) every time. To do this, you need to add the document to a schedule that contains the settings you want.

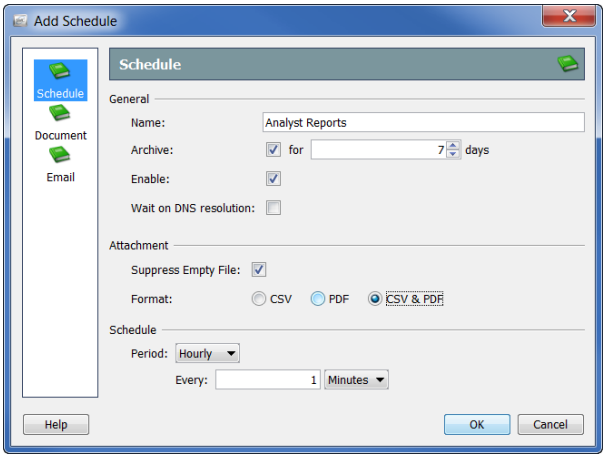
Adding a New Schedule

To add a new schedule to your account, complete the following steps:

1. From the SMC Main Menu, select **File > Manage Documents**. The Manage Documents dialog opens.



2. Click the **Schedules** icon. The Schedules page opens.
3. Click **Add**. The Add Schedule dialog opens.



4. Click the **Schedule** icon. The Schedule page opens.
5. In the Name field, type a name for the schedule. For this example, we will name the schedule “Analyst Reports.”

6. Define the parameters in the General section as shown in the following table:

If you want...	Then select...
To store the document(s) generated by this schedule in the SMC database	The **Archive** check box. Then, click the corresponding dropdown list and select how many days you want to store the document(s).
To activate this schedule as soon as it is created	The **Enable** check box.
If you want the system to wait to generate a scheduled document until the IP addresses referenced in the document have been resolved to names	The “Wait on DNS resolution” check box. **Note:** Enabling this feature may delay document generation. Each IP address may take up to two seconds to resolve. If an IP address is not resolved within two seconds, the IP address is shown without the DNS name.
To prevent the SMC from archiving or emailing generated documents that have no data	The “Suppress Empty File” check box.
To specify the type of data you want to print	▶ CSV (comma-separated value) - Select this option if you want to print only table data contained in the generated document(s). • Each table is placed in a CSV file. • All other types of data (e.g., maps, graphs, charts) do not print. • All CSV files for each document are zipped in a file (i.e., one zipped file per document). • All zipped files are emailed to each user who is designated to receive email copies of the document(s) generated by the selected schedule.
	▶ PDF - Select this option if you want to print all data contained in the generated document(s). • Each generated document is placed in a PDF file. • Each PDF file is zipped in a file. • All zipped files are emailed to each user who is designated to receive email copies of document(s) generated by the selected schedule.
- continued -	

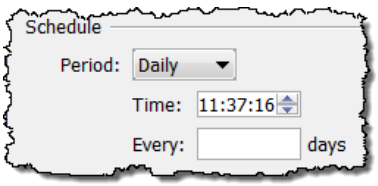
If you want...	Then select...
To specify the type of data you want to print	▸ CSV & PDF - Select this option if you want to print table data in CSV format and all other data in PDF format. • Each table is placed in a CSV file. • All other types of data in each generated document are placed in a PDF file (i.e., one PDF file per document). • All files belonging to a document are zipped in a file (i.e., one zipped file per document). • All zipped files are emailed to each user who is designated to receive email copies of document(s) generated by the selected schedule.

Notes:

- If you do not enable a table on the Pages page in the Print Settings dialog, then the schedule will not create a CSV file for that table even if the schedule is configured to create CSV files.
- The filter summary will be included in a generated document if you designate this on the Print Setup page in the Print Settings dialog. Note that you must select either the "As the first page" option or the "As the last page" option (in the Cover Sheet section) to enable the Filter summary check box (in the Cover Sheet Options section) so that you can select it.

7. Click the Period drop-down list and select how often you want the SMC to generate any document that is associated with this schedule. You may choose to generate scheduled documents on an hourly, daily, weekly, or monthly basis. Depending on which option you choose, different fields appear for you to specify more detail.

   For example, if you select **Daily**, two fields appear for you to specify the time of day you want the schedule to run and if you want the schedule to run every day, every other day, every third day, etc.

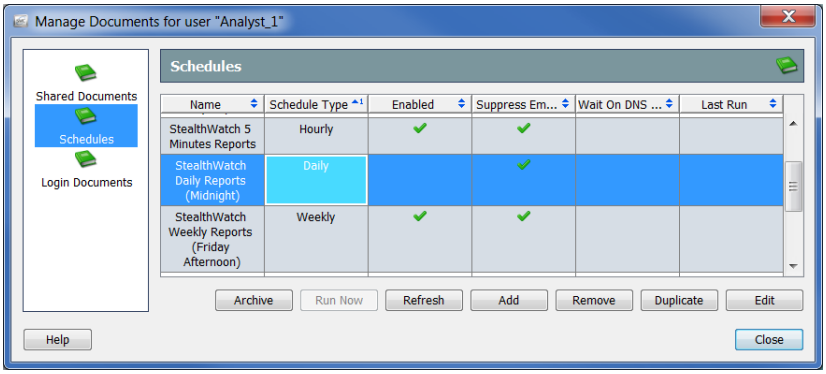


8. Continue to "Adding a Document to a Schedule" on page 295.

Editing an Existing Schedule

If the schedule you want to associate with your account already exists, complete the following steps to edit the schedule accordingly:

1. From the SMC Main Menu, select **File > Manage Documents**. The Manage Documents dialog opens.

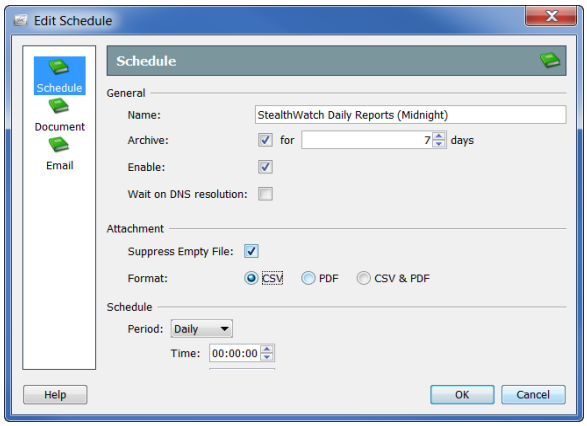


2. Click the **Schedules** icon. The Schedules page opens.
3. Select the schedule you want to edit.

Note:

In the above example, the Stealthwatch Daily Reports (Midnight) schedule has been selected. Note that there is no checkmark in the Enabled column, signifying that this schedule has not been enabled for your account. If the schedule is not enabled, none of the documents in the schedule will be generated.

4. Click **Edit**. The Edit Schedule dialog opens.

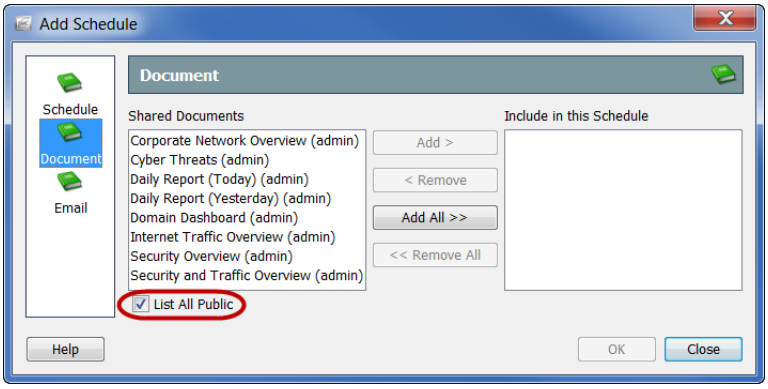


5. Click the **Schedule** icon. The Schedule page opens.
6. Change the settings as desired. For more information on any option, click **Help**.
7. Continue to "Adding a Document to a Schedule" next in this chapter.

Adding a Document to a Schedule

To add one or more documents to a schedule, complete the following steps:

1. On the Add (or Edit) Schedule dialog, click the **Document** icon. The Document page opens.

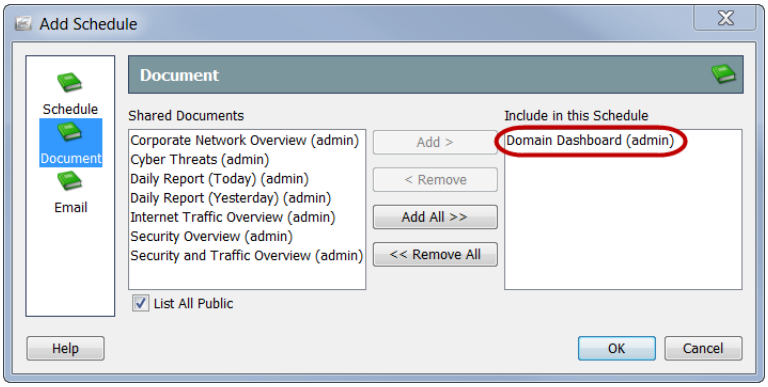


2. Select the **List All Public** check box if it is not already selected. (For more information, refer to "Public Documents" on page 291.)
3. Select the document(s) you want to add to the schedule. For this example, we will select the Domain Dashboard document.

Note:

To select more than one document, hold the **Ctrl** key and click each document you want to add. To select a range of documents, click the document that is at the top of the range you want to select, hold the **Shift** key, and then click the document that is at the bottom of the range you want to select.

4. Click **Add**. The document(s) appears in the Include in this Schedule field.



5. Do you want the SMC to automatically email the scheduled document(s) to you?
   - If yes, continue to "Adding a User's Email Address to a Schedule" on page 298.
   - If no, click **OK** to save the information, exit the Add (or Edit) Schedule dialog, and return to the Manage Documents dialog.
6. Close the remaining dialogs.

Emailing a Scheduled Document

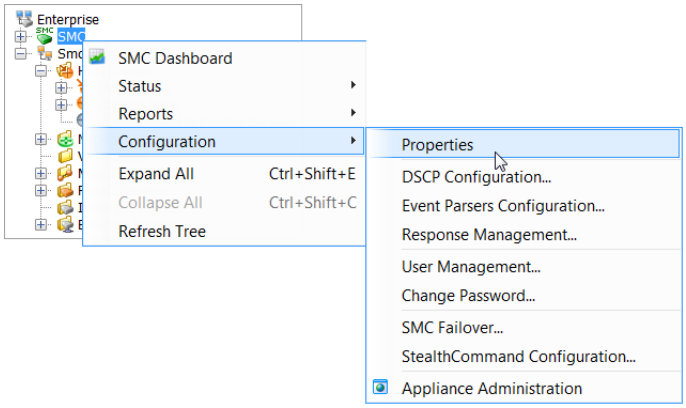
If you want the SMC to automatically email scheduled documents to you, you must complete the following two procedures:

1. Add the email server's IP address to the SMC. (Refer to the next section, "Adding the Email Server to the SMC.")
2. Add the user's email address to the schedule. (Refer to "Adding a User's Email Address to a Schedule" on page 298.)

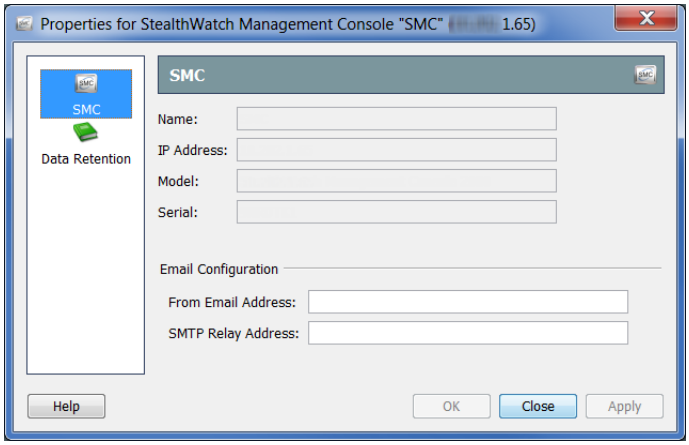
Adding the Email Server to the SMC

If you have not done so previously, you must add the email server's IP address to the SMC before the SMC can email any scheduled documents. To do this, complete the following steps:

1. Right-click the **SMC** branch in the Enterprise tree and select **Configuration > Properties** from the pop-up menu. The Properties dialog opens.



2. Click the **SMC** icon. The SMC page opens.



3. (Optional) In the From Email Address field, type an address using the following format:

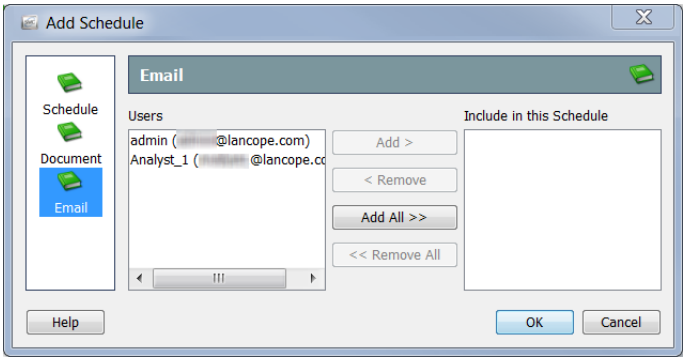
[FromUser]@[hostname].[domain]

4. In the SMTP Relay Address field, type your email server's IP address.
5. Click **OK** to save the information and close the Properties page.

Adding a User's Email Address to a Schedule

If you want the SMC to automatically email scheduled documents to you, you must add your email address to the schedule by completing the following steps:

1. On the Add (or Edit) Schedule dialog, click the **Email** icon. The Email page opens.



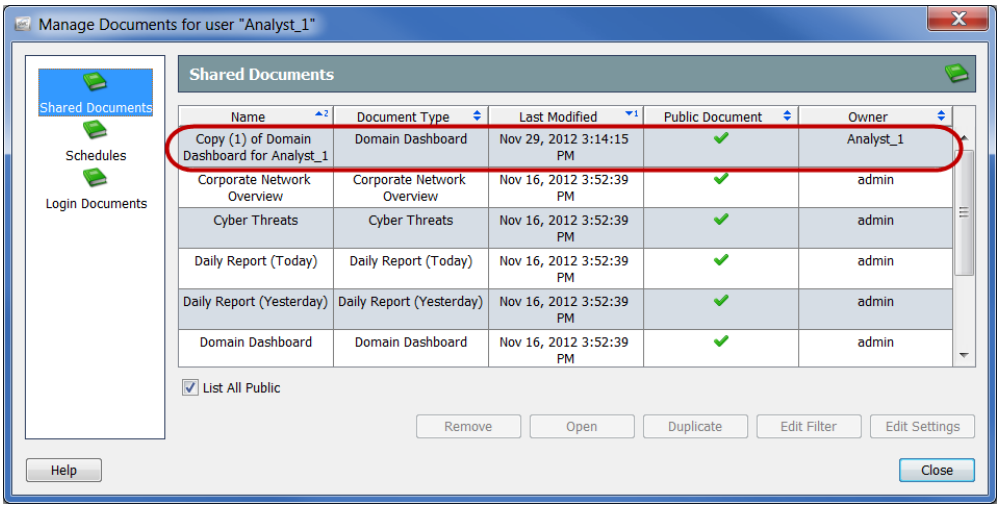
2. In the Users field, select your email address.
3. Click **Add**. Your email address appears in the Include in This Schedule field.
4. Click **OK** to save the information, close the Add (or Edit) Schedule dialog, and return to the Manage Documents dialog.
5. Close the remaining dialogs.

Pre-Filtering Shared Documents

You can edit the filter settings of any shared document so that when it is generated per a schedule, it will use those filter settings automatically.

These edits are saved in one of the following ways:

- If you are not the owner of the document, the original document is left unmodified, and a duplicate document is created with the new filter settings. Only the duplicate document will contain the new filter settings.



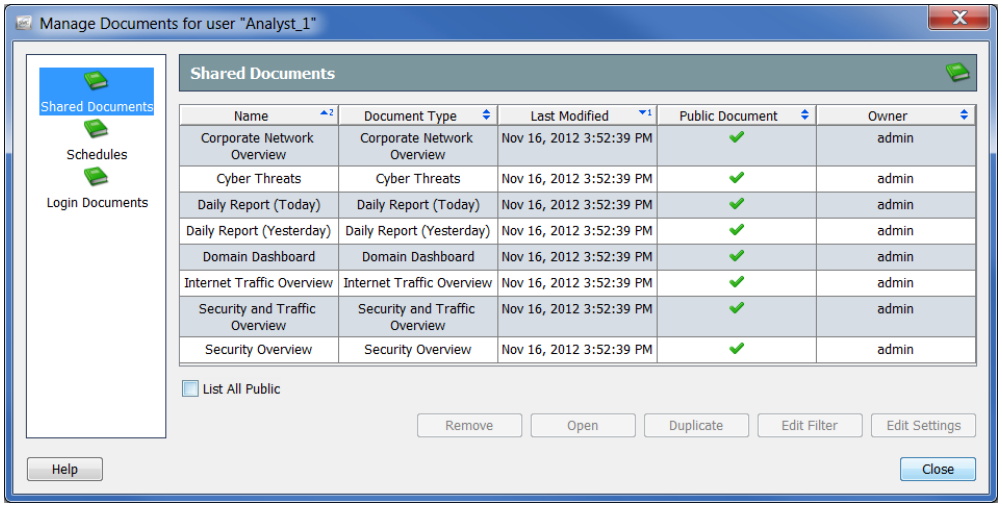
- If you are the owner of the document, the new filter settings take effect in the original document. From this point on, any time this document is generated or opened by anyone who has the privileges to access this document, the new filter settings will be in effect.

You can edit the filter settings of a shared document so that when it is generated per a schedule, it will use those filter settings automatically. To do this, complete the following steps:

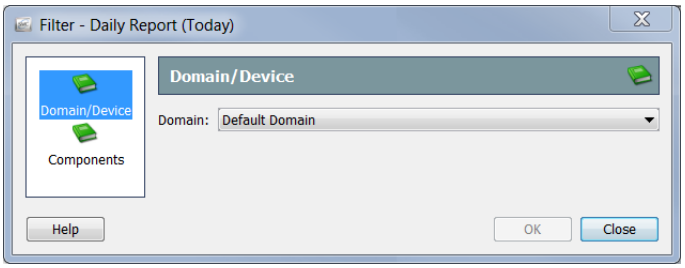
Note:

For more information about filtering documents, refer to "Filtering Document Data" in Chapter 2, “Navigating the Stealthwatch Desktop Client.”

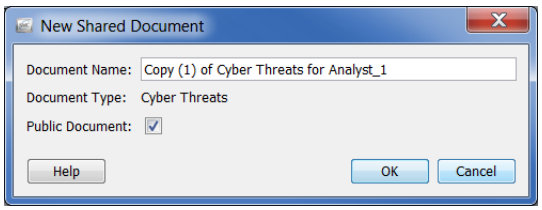
1. From the Main Menu, select **File > Manage Documents**. The Manage Documents dialog opens.



2. Click the **Shared Documents** icon. The Shared Documents page opens.
3. Select the desired document.
4. Click **Edit Filter**. The Filter dialog opens.



5. Make any desired changes to the filter settings. If you are editing the filter settings of a document someone else owns, the New Shared Document dialog opens, as shown in the example below.



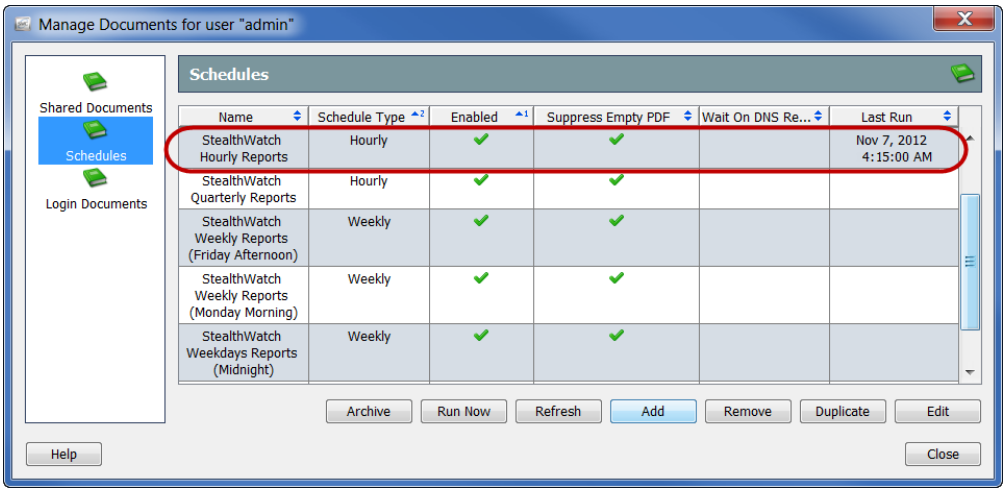
6. Do one of the following:
   - Click **OK** to accept the default name in the Document Name field and exit the New Shared Document dialog.
   - Change the name in the Document Name field and click **OK** to exit the New Shared Document dialog.
7. Click **OK** to exit the Managed Documents dialog.

Retrieving Archived Documents

If you do not want the SMC to automatically email scheduled documents to you, or you do not have the ability to receive emails from the SMC, then you can choose to retrieve scheduled documents at your convenience.

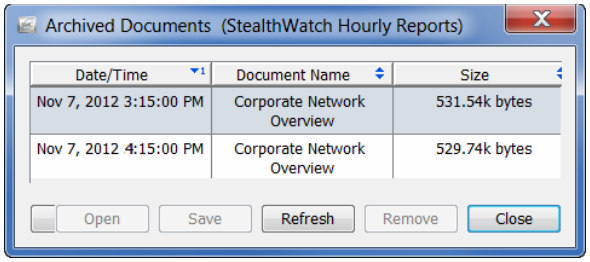
To retrieve generated documents, complete the following steps:

1. From the SMC Main Menu, select **File > Manage Documents**. The Manage Documents dialog opens.



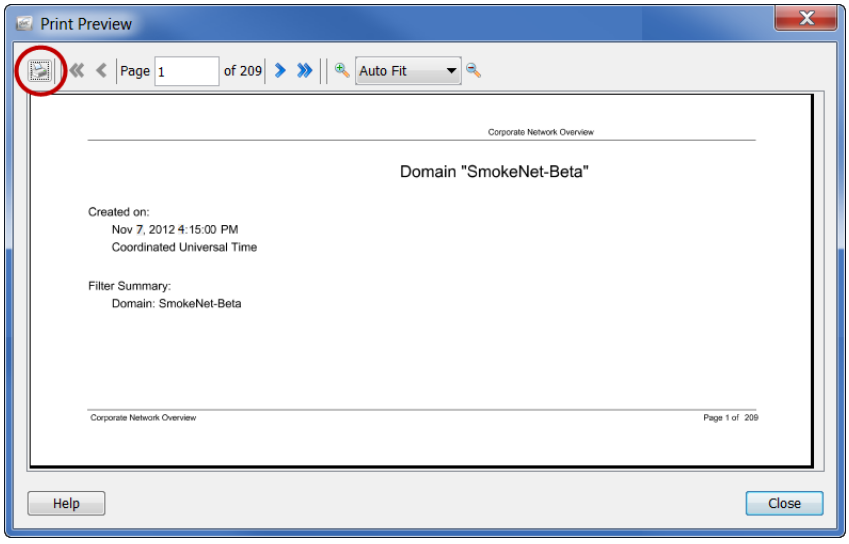
2. Click the **Schedules** icon. The Schedules page opens.
3. Click the schedule that includes the generated document(s) you want to view. Note that the Last Run column contains the date and time that the schedule was last run.

4. Click **Archive**. The Archived Documents dialog opens, as shown at right.

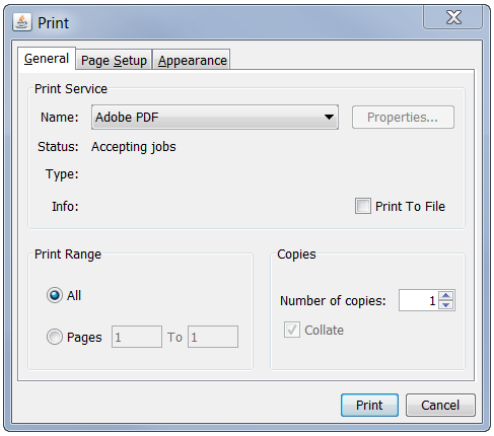


5. Click the document you want to view.

6. Click **Open**. The Print Preview dialog opens.



7. Click the **Print** icon (circled in the previous image). The Print dialog opens.



You can either print a hard copy of the document or download it to your local hard drive.

13

DESKTOP CLIENT ROLES

OVERVIEW

The Stealthwatch Management Console (SMC) provides a great deal of flexibility in setting up users with different levels of privileges. For example, you can allow one user to view and modify every area of the network. Alternatively, you can restrict certain users so that they can view only specific areas of the network without the ability to do anything else.

Desktop client roles (formally known as user functional roles) control which functionality (e.g., flow search, policy management, reports, etc.) users can view and configure in the Stealthwatch Desktop Client.

Note:

You must now use the Stealthwatch Web App to manage users, data roles, and authentication services. For more information, see the Stealthwatch Web App online help.

The only exception is that you can create and edit desktop client roles (formally known as user functional roles) only in the Stealthwatch Desktop Client. However, you must use the Stealthwatch Web App to assign desktop client roles to users.

This chapter includes the following topics:

- Desktop Client Roles
- Adding and Editing a Desktop Client role

DESKTOP CLIENT ROLES

When you create and edit desktop client roles (formally known as user functional roles) in the Stealthwatch Desktop Client, these changes will also be listed in the Stealthwatch Web App (on the Desktop tab on the User Management: User page).

To access the Desktop Client Roles dialog in the Stealthwatch Desktop Client, do one of the following:

- On the Enterprise tree, select **Configuration > Desktop Client Roles** from the context menu.
- From the main menu, select **Configuration > Desktop Client Roles**.

If you change a desktop client role, the changes do not become effective until the users who are assigned that role log in. Therefore, any users who are already logged in when the changes are made must log out and log in again.

Stealthwatch comes with the following default set of desktop client roles.

Select this option...	To allow the user to view...
Desktop Client Manager	All menu items and change anything within the Stealthwatch Desktop Client.
Configuration Manager	All menu items and configure all appliances, devices, and domain settings.
Network Engineer	All traffic-related menu items within the Stealthwatch Desktop Client, append alarm and host notes, and perform all alarm actions, except mitigation.
Security Analyst	All security-related menu items, append alarm and host notes, and perform all alarm actions, including mitigation.
Stealthwatch Power User	All menu items, acknowledge alarms, and append alarm and host notes, but without the ability to change anything.

Adding and Editing a Desktop Client role

Use the Add Desktop Client Role dialog to add, edit, and remove desktop client roles. Desktop client roles control which functionality (e.g., flow search, policy management, reports, etc.) users can view and configure in the Stealthwatch Desktop Client.

To access the Add Desktop Client Role dialog, do the following:

- From the Desktop Client Roles dialog, select **Add** or highlight an entry in the table and select **Edit**.

When you select a parent function, its children are automatically selected. If you want to select children of a parent function, you must first deselect the parent function.

After you duplicate a desktop client role, the name "Copy [x] of [desktop client role name you are duplicating] is assigned by default to the duplicated desktop client role. Double-click the duplicated role in the table and then click Edit to rename it.

INDEX

A

abbreviations 15
absolute time setting 63
acknowledging alarms 213
active documents 36
Add Role Policy dialog 254
Alarm Summary 195
Alarm Table 197
alarms
  acknowledging 213
  behavioral settings 269
  botnet alarms 190
  closing 215
  indicators 26
  mitigation, authorize mode 227
  mitigation, automatic mode 228
  on/off 266
  reopening closed alarms 218
  responding to 251
  severity levels 25
  threshold settings 269
  tolerance settings 269
  triggering 236
  unacknowledging 215
  variance-based 266
  variance-based settings 269
anomalous behavior 109
archive hour 112
archived documents 301
assigning hosts to pre-defined groups 252

B

baselining 232
behavioral settings for alarms 269
building custom dashboards 103
buttons
  Acknowledge Selection 213
  Close Selection 216
  Concern Index Filter 40, 113
  Dashboard Filter 60, 61
  File Sharing Index Filter 117
  Filter 57
  Flow Table 197
  Go to Document 39, 101, 106
  Hide Others 122
  Highlighter 75
  List 36
  Refresh 35
  Search 75
  Search Favorite 74
  Show/Hide 55
  Target Index Filter 115
  Tool Bar 37
  Topic Favorite 75
  Up/Down 47
  View Later Data 35
  Zoom-out 54

C

Chart Properties dialog 55
charts
  legends 55
  X axis, Y axis 55
  zooming in and out 54
CIDR format 139
closing
  alarms 215
  documents 46
Collapse All command 23
columns
  hiding 49
  moving 48
  resizing 48
  showing 49
  sorting 47
common alarms
  High File Sharing Index 272
  High Total Traffic 272

High Traffic 273
ICMP Flood 274
Low Traffic 274
Mail Relay 274
Max Flows Initiated 275
Max Flows Served 276
New Flows Initiated 276
New Flows Served 277
Spam Source 277
Suspect Data Loss 278
Suspect Long Flow 278
Suspect UDP Activity 279
SYN Flood 280
SYNs Received 280
UDP Flood 281
Worm Activity 281
communication status 27
Concern Index 110, 111
filter button 40, 113
incrementing 111
percent 113
points 109
Configuration menu 34
configured threshold
File Sharing Index 117
Target Index 115
Corporate Network Overview 122
creating
host policies 260
role policies 253
CSV files 50
custom dashboards 22, 30, 103

D

DAR files 289
exporting 289
importing 290
dashboards
Host Group 99
Host Group Alarm Summary 102
Host Group Network 100
Host Group Security 101
default policies 237
diagrams
baselining process 234
host identification process 194
stages in incrementing the CI 111
display preferences 29
Document Builder 103
Document Refresh Status icons 37
documentation icons, descriptions 14
documents
active 36
archived 301
closing 46
customizing print settings 66
header 39
inactive 36
login 286
moving between 36
opening 28
orientation of 37
print preview 65
printing 65, 67
public 291
refreshing 35
saving 68, 284
saving as PDF files 71
scheduling 292
sharing 289
tabs 36
tool bar 37
double-click functionality 42

E

Edit Default Policy dialog 240
Edit Host Policy dialog 262
Edit menu 29
Edit Role Policy dialog 259
Edit Settings dialog 265
editing
host policies 264
role policies 258
editing default policies
Inside Host 239
Outside Host 239
Effective Host dialog 241
effective host policies 241
Enterprise tree 23, 26
branches 24
Expand All command 23
exporting

data 50
exporting DAR files 289
external lookup 176

F

File menu 29
file sharing 204
File Sharing Index 110, 116
configured threshold 117
filter button 117
percent 116
fine-tuning the network 272
flow analysis scenario workflows
high concern index hosts 155
network slow 167
overloaded interface 164
spike in service traffic 159
flow query 136
flow scenario workflows
high concern index host 155
network slow 167
overloaded interface 164
spike in application traffic 159
Flow Table 40, 137
button 197
Short List tab 152
Table tab 151
Flow Table filter
Advanced page 60, 149
Application Details page 60, 148
Date/Time page 58, 137
Hosts page 58, 139
Interfaces page 59, 142
Performance page 60, 147
Ports & Protocols page 60, 144
Routing page 60, 145
Services & Applications page 59, 143
Traffic page 60, 146
Flows menu 33
fonts, changing 67

G

global search 44, 199

H

Help
menu 34
online 72
Hide Tree command 23
high bandwidth hosts, finding 172
High Concern Index alarm 111
High File Sharing Index alarm 272
High Total Traffic alarm 272
High Traffic alarm 273
host
baselining 232
behavior 31
Host Group Alarm Summary Dashboard 102
Host Group Dashboard 99
Host Group Editor dialog 252
Host Group Membership Report 92
Host Group Network Dashboard 100
Host Group Security Dashboard 40, 101
host groups 84
Catch All 85
Command & Control Servers 87, 187
IP addresses 90
pre-defined 252
host identification process 194
Host Information
document 210
filter 209
Host IQ 210
performing 209
host policies 237
host policy management 237
Host Policy Manager dialog 238
Host Snapshot 195, 201
Alarms tab 203
Exporter Interfaces tab 207
Identification tab 202
Identity, DHCP & Host Notes tab ... 206
Security Events tab 205
Security tab 204
Top Active Flows tab 206
hosts
touched 204
with common characteristics 209
Hosts menu 31

I

ICMP Flood alarm 274
icons
  Document Refresh Status 37
importing DAR files 290
inactive documents 36
incrementing the Concern Index 111
indexes 109
Internet Traffic Overview 120
Internet, slow 129
investigating flows 40
IP addresses
  for host groups 90
  locating 168

K

keyboard shortcuts 77

L

live data 35
login
  privileges 22
login document 286
Low Traffic alarm 274

M

Mail Relay alarm 274
Main Menu 28
Max Flows Initiated alarm 275
Max Flows Served alarm 276
menus
  Configuration 34
  Edit 29
  File 29
  Flows 33
  Help 34
  Hosts 31
  pop-up 51
  Reports 33
  Security 31
  Status 30
  Top 30
  Traffic 32
  View 30
Mitigation Actions document 229
mitigation actions, defining 225
mitigation devices
  configuring 221
  enabling 223
  types 220
mitigation feature
  authorize mode 219, 226
  automatic mode 219, 226
  disable mode 226
  manual mode 219
  process 219
  response types 226
mitigation options, types 226
mitigation, corresponding alarm
  authorize mode 227
  automatic mode 228
monitoring traffic 120

N

NATed flows 58
network
  fine-tuning 272
  performance 129
Network and Server Performance document 130
network behavior analysis 119
New Flows Initiated alarm 276
New Flows Served alarm 277
normal behavior 208

O

on/off alarms 266
online Help 34, 72
  Contents option 73
  Favorites list 74
  Favorites option 75
  Glossary option 74
  Index option 73
  Quick Search option 75
  Search option 73
opening
  documents 28

P

page tabs 36
peer-to-peer activity 110

policies
creating host 260
creating role 253
default 237
editing host 264
editing Inside Host 239
editing Outside Host 239
editing role 258
effective host 241
host 237
role 237
pop-up menus 51
pre-defined host groups 252
preferences, display 29
print preview 65
printing
customizing print settings 66
documents 65, 67

Q

Quick View 52, 154

R

refreshing
documents 35
Enterprise tree 26
relational flow map 93
relative time setting 63
reopening closed alarms 218
repeat offender 194
Reports menu 33
responding to alarms 251
restoring table defaults 50
right-click functionality 41, 45
rogue hosts 86
role policies 237
round trip time (RTT) 130

S

saving
documents 68, 284
documents as PDF files 71
scheduled documents
adding a document 295
adding a new schedule 292
adding a user's email address 298
adding the email server to SMC 297
emailing 297
enabling an existing schedule 294
searching
in a document 44, 199
in the Enterprise tree 24
Security menu 31
server response time (SRT) 131
server, performance 129
shortcuts, keyboard 77
SLIC
botnet alarms 190
Command & Control Servers host group 187
process 187
slow Internet 129
source host 193
Spam Source alarm 277
static data 35
Status menu 30
Suspect Data Loss alarm 278
Suspect Long Flow alarm 278
Suspect UDP Activity alarm 279
SYN Flood alarm 280
SYNs Received alarm 280

T

tables
restoring defaults 50
row colors 47
tabs
arranging 38
changing tab group contents 38
document 36
page 36
Target Index 110, 114
configured threshold 115
filter button 115
percent 114
threshold settings for alarms 269
tolerance settings for alarms 269
tool bars 37
tool tips 27
Top menu 30
touched hosts 204
Touched Hosts document 204
traffic

Corporate Network Overview 122
identifying the direction of 161
Internet Traffic Overview 120
monitoring 120
Traffic menu 32
tree branches 24

U

UDP Flood alarm 281
unacknowledging alarms 215
unnecessary alarms 208

V

variance-based alarms 266
settings 269
version information 34
View menu 30
Visual Editor dialog 270

W

Worm Activity alarm 281

© 2021 Cisco Systems, Inc. and/or its affiliates. All Rights Reserved.

© 2021 Cisco Systems, Inc. and/or its affiliates. All Rights Reserved.