



---

Junos<sup>®</sup> OS

## UTM Feature Guide for Security Devices

Release

15.1X49-D70



---

Modified: 2016-11-22

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*Junos<sup>®</sup> OS UTM Feature Guide for Security Devices*  
15.1X49-D70  
Copyright © 2016, Juniper Networks, Inc.  
All rights reserved.

The information in this document is current as of the date on the title page.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	About the Documentation . . . . .	xv
	Documentation and Release Notes . . . . .	xv
	Supported Platforms . . . . .	xv
	Using the Examples in This Manual . . . . .	xvi
	Merging a Full Example . . . . .	xvi
	Merging a Snippet . . . . .	xvii
	Documentation Conventions . . . . .	xvii
	Documentation Feedback . . . . .	xix
	Requesting Technical Support . . . . .	xx
	Self-Help Online Tools and Resources . . . . .	xx
	Opening a Case with JTAC . . . . .	xx
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Understanding Unified Threat Management . . . . .</b>	<b>3</b>
	Unified Threat Management Overview . . . . .	3
	Understanding UTM Custom Objects . . . . .	4
<b>Chapter 2</b>	<b>Managing UTM Licensing . . . . .</b>	<b>7</b>
	Understanding UTM Licensing . . . . .	7
	Updating UTM Licenses (CLI Procedure) . . . . .	8
<b>Chapter 3</b>	<b>Configuring WELF Logging . . . . .</b>	<b>9</b>
	Understanding WELF Logging for UTM Features . . . . .	9
	Example: Configuring WELF Logging for UTM Features . . . . .	10
<b>Chapter 4</b>	<b>Configuring UTM for Chassis Cluster . . . . .</b>	<b>13</b>
	Understanding UTM Support for Active/Backup Chassis Cluster . . . . .	13
	Understanding Chassis Cluster Support for UTM Modules . . . . .	15
<b>Part 2</b>	<b>Configuring Antispam Filtering</b>	
<b>Chapter 5</b>	<b>Understanding Antispam Filtering . . . . .</b>	<b>19</b>
	Antispam Filtering Overview . . . . .	19
	Handling Spam Messages . . . . .	19
	Blocking Detected Spam . . . . .	19
	Tagging Detected Spam . . . . .	20
<b>Chapter 6</b>	<b>Configuring Server-Based Antispam Filtering . . . . .</b>	<b>21</b>
	Understanding Server-Based Antispam Filtering . . . . .	21
	Server-Based Antispam Filtering Configuration Overview . . . . .	22
	Example: Configuring Server-Based Antispam Filtering . . . . .	23

<b>Chapter 7</b>	<b>Configuring Local List Antispam Filtering . . . . .</b>	<b>29</b>
	Understanding Local List Antispam Filtering . . . . .	29
	Local List Antispam Filtering Configuration Overview . . . . .	30
	Example: Configuring Local List Antispam Filtering . . . . .	30
<b>Chapter 8</b>	<b>Configuring Whitelists . . . . .</b>	<b>39</b>
	Understanding MIME Whitelists . . . . .	39
	Example: Configuring MIME Whitelists to Bypass Antivirus Scanning . . . . .	40
	Understanding URL Whitelists . . . . .	40
	Configuring URL Whitelists to Bypass Antivirus Scanning (CLI Procedure) . . . . .	41
<b>Part 3</b>	<b>Configuring and Managing Sophos Antivirus Protection</b>	
<b>Chapter 9</b>	<b>Configuring Sophos Antivirus Protection . . . . .</b>	<b>45</b>
	Sophos Antivirus Protection Overview . . . . .	45
	Sophos Antivirus Features . . . . .	46
	Understanding Sophos Antivirus Data File Update . . . . .	47
	Sophos Antivirus Configuration Overview . . . . .	48
	Example: Configuring Sophos Antivirus Custom Objects . . . . .	48
	Example: Configuring Sophos Antivirus Feature Profile . . . . .	52
	Example: Configuring Sophos Antivirus UTM Policies . . . . .	58
	Example: Configuring Sophos Antivirus Firewall Security Policies . . . . .	59
	Example: Configuring Sophos Antivirus Scanner with SSL Forward Proxy . . . . .	61
	Managing Sophos Antivirus Data Files . . . . .	67
<b>Part 4</b>	<b>Configuring and Monitoring Content Filtering</b>	
<b>Chapter 10</b>	<b>Configuring Content Filtering . . . . .</b>	<b>71</b>
	Content Filtering Overview . . . . .	71
	Understanding Content Filtering Protocol Support . . . . .	72
	HTTP Support . . . . .	72
	FTP Support . . . . .	73
	E-Mail Support . . . . .	73
	Specifying Content Filtering Protocols (CLI Procedure) . . . . .	73
	Content Filtering Configuration Overview . . . . .	74
	Example: Configuring Content Filtering Custom Objects . . . . .	75
	Example: Configuring Content Filtering Feature Profiles . . . . .	77
	Example: Configuring Content Filtering UTM Policies . . . . .	80
	Example: Attaching Content Filtering UTM Policies to Security Policies . . . . .	82
	Monitoring Content Filtering Configurations . . . . .	84
<b>Part 5</b>	<b>Configuring Web Filtering</b>	
<b>Chapter 11</b>	<b>Configuring Web Filtering . . . . .</b>	<b>89</b>
	Web Filtering Overview . . . . .	89
	Enhanced Web Filtering Overview . . . . .	91
	Understanding Enhanced Web Filtering Process . . . . .	92
	Functional Requirements for Enhanced Web Filtering . . . . .	93
	Example: Configuring Enhanced Web Filtering . . . . .	97

Understanding the Quarantine Action for Enhanced Web Filtering . . . . .	105
Example: Configuring Site Reputation Action for Enhanced Web Filtering . . . . .	106
Understanding Local Web Filtering . . . . .	112
User-Defined URL Categories . . . . .	112
Local Web Filtering Process . . . . .	112
Local Web Filtering Profiles . . . . .	113
Profile Matching Precedence . . . . .	113
Example: Configuring Local Web Filtering . . . . .	114
Understanding Redirect Web Filtering . . . . .	120
Example: Enhancing Security by Configuring Redirect Web Filtering Using Custom Objects . . . . .	121
Monitoring Web Filtering Configurations . . . . .	129

## Part 6

### Chapter 12

## Configuration Statements and Operational Commands

<b>Configuration Statements . . . . .</b>	<b>133</b>
action (Security UTM Web Filtering) . . . . .	138
address-blacklist . . . . .	138
address-whitelist . . . . .	138
admin-email . . . . .	139
administrator-email (Security Fallback Block) . . . . .	139
administrator-email (Security Virus Detection) . . . . .	139
allow-email (Security Fallback Block) . . . . .	140
allow-email (Security Virus Detection) . . . . .	140
application (Security Policies) . . . . .	141
application-proxy (Security UTM) . . . . .	142
anti-spam (Security Feature Profile) . . . . .	142
anti-spam (Security UTM Policy) . . . . .	143
anti-virus (Security Feature Profile) . . . . .	144
anti-virus (Security UTM Policy) . . . . .	146
block-command . . . . .	146
block-content-type . . . . .	147
block-extension . . . . .	147
block-message (Security UTM) . . . . .	148
block-mime . . . . .	148
cache . . . . .	149
category (Security Logging) . . . . .	150
category (Security Web Filtering) . . . . .	151
content-filtering (Security Feature Profile) . . . . .	157
content-filtering (Security UTM Policy) . . . . .	158
content-size (Security Antivirus Sophos Engine) . . . . .	159
content-size-limit . . . . .	160
custom-block-message . . . . .	160
custom-message (Security Content Filtering) . . . . .	160
custom-message (Security Email Notify) . . . . .	161
custom-message (Security Fallback Block) . . . . .	161
custom-message (Security Fallback Non-Block) . . . . .	161
custom-message (Security Virus Detection) . . . . .	162
custom-message-subject (Security Email Notify) . . . . .	162

custom-message-subject (Security Fallback Block)	162
custom-message-subject (Security Fallback Non-Block)	163
custom-message-subject (Security Virus Detection)	163
custom-objects	164
custom-tag-string	164
custom-url-category	165
default (Security Antivirus Sophos Engine)	166
default (Security UTM)	166
default (Security Web Filtering)	167
display-host (Security Fallback Block)	167
display-host (Security Virus Detection)	168
download-profile (Security Antivirus FTP)	168
download-profile (Security Content Filtering FTP)	168
email-notify	169
engine-not-ready (Security Antivirus Sophos Engine)	169
exception (Security Antivirus Mime Whitelist)	170
exception (Security Content Filtering)	170
fallback-block (Security Antivirus)	171
fallback-non-block (Security Antivirus)	171
fallback-options (Security Antivirus Sophos Engine)	172
fallback-settings (Security Web Filtering)	172
fallback-settings (Security Web Filtering Juniper Local)	173
fallback-settings (Security Web Filtering Websense Redirect)	173
feature-profile	174
filename-extension	177
flag (SMTP)	178
format (Security Log Stream)	179
from-zone (Security Policies)	180
ftp (UTM Policy Anti-Virus)	182
ftp (UTM Policy Content Filtering)	183
host (Security Web Filtering)	183
http-profile (Security Antivirus)	184
http-profile (Security Content Filtering)	184
http-profile (Security Web Filtering)	184
imap-profile (Security UTM Policy Antivirus)	185
imap-profile (Security UTM Policy Content Filtering)	185
interval (Security Antivirus)	186
ipc	187
juniper-local	188
limit (UTM Policy)	188
list (Security Antivirus Mime Whitelist)	189
list (Security Content Filtering Block Mime)	189
log (Security)	190
mime-pattern	193
mime-whitelist	194
no-autoupdate	195
no-notify-mail-recipient	195
no-notify-mail-sender (Security Content Filtering Notification Options)	196
no-notify-mail-sender (Security Fallback Block)	196

no-notify-mail-sender (Security Virus Detection) . . . . .	197
no-sbl-default-server . . . . .	197
notification-options (Security Antivirus) . . . . .	198
notification-options (Security Content Filtering) . . . . .	199
notify-mail-recipient . . . . .	199
notify-mail-sender (Security Content Filtering Notification Options) . . . . .	200
notify-mail-sender (Security Fallback Block) . . . . .	200
notify-mail-sender (Security Virus Detection) . . . . .	201
no-uri-check . . . . .	201
out-of-resources (Security Antivirus Sophos Engine) . . . . .	202
over-limit . . . . .	202
packet-filter . . . . .	203
password (Security Antivirus) . . . . .	204
pattern-update (Security Antivirus) . . . . .	204
permit-command . . . . .	205
policies . . . . .	206
pop3-profile (Security UTM Policy Antivirus) . . . . .	210
pop3-profile (Security UTM Policy Content Filtering) . . . . .	210
port (Security Antivirus) . . . . .	211
port (Security Web Filtering Server) . . . . .	211
primary-server . . . . .	212
profile (Security Antispam SBL) . . . . .	212
profile (Security Content Filtering) . . . . .	213
profile (Security Sophos Engine Antivirus) . . . . .	214
profile (Security Web Filtering Juniper Enhanced) . . . . .	215
profile (Security Web Filtering Juniper Local) . . . . .	216
profile (Security Web Filtering Websense Redirect) . . . . .	217
protocol-command . . . . .	218
proxy (Security Antivirus) . . . . .	218
quarantine-message (Security UTM) . . . . .	219
sbl . . . . .	219
sbl-default-server . . . . .	220
scan-options (Security Antivirus Sophos Engine) . . . . .	220
secondary-server . . . . .	221
server (Security Antivirus) . . . . .	221
server (Security Web Filtering) . . . . .	222
server-connectivity . . . . .	222
sessions-per-client . . . . .	223
site-reputation-action . . . . .	224
size (Security Web Filtering Cache) . . . . .	224
smtp-profile (Security UTM Policy Antispam) . . . . .	225
smtp-profile (Security UTM Policy Antivirus) . . . . .	225
smtp-profile (Security UTM Policy Content Filtering) . . . . .	225
sockets . . . . .	226
sophos-engine . . . . .	227
spam-action . . . . .	228
sxl-retry . . . . .	229
sxl-timeout . . . . .	229
timeout (Security Antivirus Fallback Options Sophos Engine) . . . . .	230

timeout (Security Antivirus Scan Options) . . . . .	230
timeout (Security Web Filtering) . . . . .	231
timeout (Security Web Filtering Cache) . . . . .	231
timeout (Security Web Filtering Fallback Settings) . . . . .	232
too-many-requests (Security Antivirus Fallback Options Sophos Engine) . . . . .	232
too-many-requests (Security Web Filtering Fallback Settings) . . . . .	233
to-zone (Security Policies) . . . . .	234
traceoptions (Security Antispam) . . . . .	236
traceoptions (Security Antivirus) . . . . .	237
traceoptions (Security Application Proxy) . . . . .	238
traceoptions (Security Content Filtering) . . . . .	239
traceoptions (Security UTM) . . . . .	239
traceoptions (Security Web Filtering) . . . . .	240
traceoptions (SMTP) . . . . .	241
traffic-options . . . . .	241
trickling . . . . .	242
type (Security Antivirus Feature Profile) . . . . .	242
type (Security Content Filtering Notification Options) . . . . .	243
type (Security Fallback Block) . . . . .	243
type (Security Virus Detection) . . . . .	244
upload-profile (Security Antivirus FTP) . . . . .	244
upload-profile (Security Content Filtering FTP) . . . . .	244
uri-check . . . . .	245
url (Security Antivirus) . . . . .	245
url-blacklist . . . . .	245
url-pattern . . . . .	246
url-whitelist (Security Antivirus) . . . . .	246
url-whitelist (Security Web Filtering) . . . . .	247
username (Security Antivirus) . . . . .	247
utm . . . . .	248
utm-policy . . . . .	253
utm-policy (Application Services) . . . . .	254
virus-detection (Security Antivirus) . . . . .	254
web-filtering . . . . .	255
websense-redirect . . . . .	256
<b>Chapter 13</b>	
<b>Operational Commands . . . . .</b>	<b>257</b>
clear security utm anti-spam statistics . . . . .	258
clear security utm antivirus statistics . . . . .	259
clear security utm content-filtering statistics . . . . .	260
clear security utm session . . . . .	261
clear security utm web-filtering statistics . . . . .	262
request security utm anti-virus sophos-engine . . . . .	263
request system license update . . . . .	264
show configuration smtp . . . . .	265
show groups junos-defaults . . . . .	266
show security log . . . . .	267
show security policies . . . . .	270
show security utm anti-spam statistics . . . . .	279

show security utm anti-spam status . . . . .	280
show security utm anti-virus statistics . . . . .	281
show security utm anti-virus status . . . . .	283
show security utm content-filtering statistics . . . . .	285
show security utm session . . . . .	286
show security utm status . . . . .	287
show security utm web-filtering statistics . . . . .	288
show security utm web-filtering status . . . . .	291



# List of Figures

Part 5	Configuring Web Filtering	
Chapter 11	Configuring Web Filtering .....	89
	Figure 1: Websense Redirect Architecture .....	122



# List of Tables

	<b>About the Documentation</b> . . . . .	<b>xv</b>
	Table 1: Notice Icons . . . . .	xviii
	Table 2: Text and Syntax Conventions . . . . .	xviii
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 2</b>	<b>Managing UTM Licensing</b> . . . . .	<b>7</b>
	Table 3: UTM Feature Subscription Service License Requirements . . . . .	7
<b>Part 6</b>	<b>Configuration Statements and Operational Commands</b>	
<b>Chapter 12</b>	<b>Configuration Statements</b> . . . . .	<b>133</b>
	Table 4: List of Categories Predefined by Websense . . . . .	152
<b>Chapter 13</b>	<b>Operational Commands</b> . . . . .	<b>257</b>
	Table 5: show configuration smtp . . . . .	265
	Table 6: show security log Output Fields . . . . .	268
	Table 7: show security policies Output Fields . . . . .	271



# About the Documentation

- Documentation and Release Notes on page xv
- Supported Platforms on page xv
- Using the Examples in This Manual on page xvi
- Documentation Conventions on page xvii
- Documentation Feedback on page xix
- Requesting Technical Support on page xx

## Documentation and Release Notes

---

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

## Supported Platforms

---

For the features described in this document, the following platforms are supported:

- SRX300
- SRX320
- SRX340
- SRX345
- SRX550M
- SRX1500
- vSRX

## Using the Examples in This Manual

---

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

### Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

## Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {  
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]  
user@host# edit system scripts  
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]  
user@host# load merge relative /var/tmp/ex-script-snippet.conf  
load complete
```

For more information about the **load** command, see [CLI Explorer](#).

---

## Documentation Conventions

[Table 1 on page xviii](#) defines notice icons used in this guide.

Table 1: Notice Icons







Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xviii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b>  No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies guide names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS CLI User Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"><li>To configure a stub area, include the <b>stub</b> statement at the <b>[edit protocols ospf area area-id]</b> hierarchy level.</li><li>The console port is labeled <b>CONSOLE</b>.</li></ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub &lt;default-metric <i>metric</i>&gt;;</b>
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  <b>(<i>string1</i>   <i>string2</i>   <i>string3</i>)</b>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ <i>community-ids</i> ]</b>
Indentation and braces ( { } )	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options {   static {     route default {       nexthop <i>address</i>;       retain;     }   } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"><li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li><li>To cancel the configuration, click <b>Cancel</b>.</li></ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.

- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net). Include the document or topic name, URL or page number, and software version (if applicable).

## Requesting Technical Support

---

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.



## PART 1

# Overview

- [Understanding Unified Threat Management on page 3](#)
- [Managing UTM Licensing on page 7](#)
- [Configuring WELF Logging on page 9](#)
- [Configuring UTM for Chassis Cluster on page 13](#)



## CHAPTER 1

# Understanding Unified Threat Management

- [Unified Threat Management Overview on page 3](#)
- [Understanding UTM Custom Objects on page 4](#)

## Unified Threat Management Overview

---

Unified Threat Management (UTM) is a term used to describe the consolidation of several security features into one device, protecting against multiple threat types. The advantage of UTM is streamlined installation and management of these multiple security capabilities.

The security features provided as part of the UTM solution are:

- **Antispam Filtering**—E-mail spam consists of unwanted e-mail messages, usually sent by commercial, malicious, or fraudulent entities. The antispam feature examines transmitted e-mail messages to identify e-mail spam. When the device detects an e-mail message deemed to be spam, it either drops the message or tags the message header or subject field with a preprogrammed string. The antispam feature uses a constantly updated spam block list (SBL). Sophos updates and maintains the IP-based SBL. The antispam feature is a separately licensed subscription service.
- **Content Filtering**—Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type. Content filtering does not require a separate license.
- **Web Filtering**—Web filtering lets you manage Internet usage by preventing access to inappropriate Web content. There are three types of Web filtering solutions. In the case of the integrated Web filtering solution, the decision-making for blocking or permitting Web access is done on the device after it identifies the category for a URL either from user-defined categories or from a category server (Websense provides the CPA Server). The integrated Web filtering feature is a separately licensed subscription service. The redirect Web filtering solution intercepts HTTP requests and forwards the server URL to an external URL filtering server provided by Websense to determine whether to block or permit the requested Web access. Redirect Web filtering does not require a separate license. With Juniper Local Web Filtering, the decision-making for blocking or permitting Web access is done on the device after it identifies the category for a URL.

from user-defined categories stored on the device. With Local filtering, there is no additional Juniper license or remote category server required.

- **Sophos Antivirus**— Sophos antivirus is as an in-the-cloud antivirus solution. The virus pattern and malware database is located on external servers maintained by Sophos (Sophos Extensible List) servers, thus there is no need to download and maintain large pattern databases on the Juniper device. The Sophos antivirus scanner also uses a local internal cache to maintain query responses from the external list server to improve lookup performance.



**NOTE:** The `sessions-per-client limit` CLI command, which imposes a session throttle to prevent a malicious user from generating large amounts of traffic simultaneously, supports the antispam, content filtering, and antivirus UTM features. It does not support Web filtering.



**NOTE:** Starting with Junos OS Release 15.1X49-D60, on SRX1500 Services Gateways and vSRX instances, UTM policies, profiles, MIME patterns, filename extensions, and protocol-command numbers are increased to 500; custom URL patterns and custom URL categories are increased to 1000.

**Release History Table**

Release	Description
15.1X49-D60	Starting with Junos OS Release 15.1X49-D60, on SRX1500 Services Gateways and vSRX instances, UTM policies, profiles, MIME patterns, filename extensions, and protocol-command numbers are increased to 500; custom URL patterns and custom URL categories are increased to 1000.

**Related Documentation**

- [Understanding UTM Custom Objects on page 4](#)
- [Understanding UTM Licensing on page 7](#)
- [Updating UTM Licenses \(CLI Procedure\) on page 8](#)
- [Understanding WELF Logging for UTM Features on page 9](#)
- [Example: Configuring WELF Logging for UTM Features on page 10](#)

## Understanding UTM Custom Objects

Before you can configure most UTM features, you must first configure the custom objects for the feature in question. Custom objects are global parameters for UTM features. This means that configured custom objects can be applied to all UTM policies where applicable, rather than only to individual policies.

The following UTM features make use of certain custom objects:

- Anti-Virus (see *Full Antivirus Pattern Update Configuration Overview*)
- Web Filtering (see *Example: Configuring Integrated Web Filtering*)
- Anti-Spam (see [“Server-Based Antispam Filtering Configuration Overview” on page 22](#))
- Content Filtering (see [“Content Filtering Configuration Overview” on page 74](#))

**Related  
Documentation**

- [Unified Threat Management Overview on page 3](#)
- [Understanding UTM Licensing on page 7](#)
- [Updating UTM Licenses \(CLI Procedure\) on page 8](#)
- [Understanding WELF Logging for UTM Features on page 9](#)
- [Example: Configuring WELF Logging for UTM Features on page 10](#)



## CHAPTER 2

# Managing UTM Licensing

- [Understanding UTM Licensing on page 7](#)
- [Updating UTM Licenses \(CLI Procedure\) on page 8](#)

### Understanding UTM Licensing

The majority of UTM features function as a subscription service requiring a license. You can redeem this license once you have purchased your subscription license SKUs. You redeem your license by entering your authorization code and chassis serial number into the Customer Service License Management System (LMS) interface. Once your entitlement is generated, you can use the CLI from your device to send a license update request to the LMS server. The LMS server then sends your subscription license directly to the device.



**NOTE:** UTM requires 1 GB of memory.

**Table 3: UTM Feature Subscription Service License Requirements**

UTM Feature	Requires License
Antispam	Yes
Antivirus: sophos	Yes
Content Filtering	No
Web Filtering: integrated	Yes
Web Filtering: redirect	No
Web Filtering: local	No
Web Filtering: enhanced	Yes



**NOTE:** License enforcement is supported on all high-end SRX Series devices. Licensed features including anti-virus or Enhanced Web Filtering will not function until a license has been installed. The license must be installed after installing or upgrading to a new Junos OS Release version. Unlicensed features such as UTM blacklists and whitelists will continue to function without a license.

---

**Related  
Documentation**

- [Unified Threat Management Overview on page 3](#)
- [Understanding UTM Custom Objects on page 4](#)
- [Updating UTM Licenses \(CLI Procedure\) on page 8](#)
- [Understanding WELF Logging for UTM Features on page 9](#)
- [Example: Configuring WELF Logging for UTM Features on page 10](#)

---

## Updating UTM Licenses (CLI Procedure)

---

To apply your UTM subscription license to the device, use the following CLI command:

```
user@host> request system license update
```

After you install the license and reboot the device, the device reserves more memory for UTM features, and hence decreases the session capacity. Use the **set security forwarding-process application-services enable-utm-memory** command to manually reallocate the memory for UTM features. You must reboot the device for the configuration to take effect.

**Related  
Documentation**

- [Unified Threat Management Overview on page 3](#)
- [Understanding UTM Custom Objects on page 4](#)
- [Understanding UTM Licensing on page 7](#)
- [Understanding WELF Logging for UTM Features on page 9](#)
- [Example: Configuring WELF Logging for UTM Features on page 10](#)

## CHAPTER 3

# Configuring WELF Logging

- [Understanding WELF Logging for UTM Features on page 9](#)
- [Example: Configuring WELF Logging for UTM Features on page 10](#)

### Understanding WELF Logging for UTM Features

---

UTM features support the WELF standard. The WELF Reference defines the WebTrends industry standard log file exchange format. Any system logging to this format is compatible with Firewall Suite 2.0 and later, Firewall Reporting Center 1.0 and later, and Security Reporting Center 2.0 and later.

A WELF log file is composed of records. Each record is a single line in the file. Records are always in chronological order. The earliest record is the first record in the file; the most recent record is the last record in the file. WELF places no restrictions on log filenames or log file rotation policies.



**NOTE:** Each WELF record is composed of fields. The record identifier field (**id=**) must be the first field in a record. All other fields can appear in any order.

The following is a sample WELF record:

```
id=firewall time="2000-2-4 12:01:01" fw=192.168.0.238 pri=6 rule=3 proto=http  
src=192.168.0.23 dst=6.1.0.36 rg=www.example.com/index.html op=GET result=0  
rcvd=1426
```

The fields from the example WELF record include the following required elements (all other fields are optional):

- **id** (Record identifier)
- **time** (Date/time)
- **fw** (Firewall IP address or name)
- **pri** (Priority of the record)

#### Related Documentation

- [Unified Threat Management Overview on page 3](#)
- [Understanding UTM Custom Objects on page 4](#)

- [Understanding UTM Licensing on page 7](#)
- [Updating UTM Licenses \(CLI Procedure\) on page 8](#)
- [Example: Configuring WELF Logging for UTM Features on page 10](#)

## Example: Configuring WELF Logging for UTM Features

---

This example shows how to configure WELF logging for UTM features.

- [Requirements on page 10](#)
- [Overview on page 10](#)
- [Configuration on page 10](#)
- [Verification on page 11](#)

### Requirements

Before you begin, review the fields used to create a WELF log file and record. See [“Understanding WELF Logging for UTM Features” on page 9](#).

### Overview

A WELF log file is composed of records. Each record is a single line in the file. Records are always in chronological order. The earliest record is the first record in the file; the most recent record is the last record in the file. WELF places no restrictions on log filenames or log file rotation policies. In this example, the severity level is emergency and the name of the security log stream is **utm-welf**.

### Configuration

**CLI Quick Configuration** To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security log source-address 1.2.3.4 stream utm-welf
set security log source-address 1.2.3.4 stream utm-welf format welf
set security log source-address 1.2.3.4 stream utm-welf format welf category
content-security
set security log source-address 1.2.3.4 stream utm-welf format welf category
content-security severity emergency
set security log source-address 1.2.3.4 stream utm-welf format welf category
content-security severity emergency host 5.6.7.8
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [Using the CLI Editor in Configuration Mode in the CLI User Guide](#).

To configure WELF logging for UTM features:

1. Set the security log source IP address.  
**[edit security log]**

```
user@host# set source-address 1.2.3.4
```



**NOTE:** You must save the WELF logging messages to a dedicated WebTrends server.

2. Name the security log stream.

```
[edit security log]
user@host# set source-address 1.2.3.4 stream utm-welf
```

3. Set the format for the log messages.

```
[edit security log]
user@host# set source-address 1.2.3.4 stream utm-welf format welf
```

4. Set the category of log messages that are sent.

```
[edit security log]
user@host# set source-address 1.2.3.4 stream utm-welf format welf category
content-security
```

5. Set the severity level of log messages that are sent.

```
[edit security log]
user@host# set source-address 1.2.3.4 stream utm-welf format welf category
content-security severity emergency
```

6. Enter the host address of the dedicated WebTrends server to which the log messages are to be sent.

```
[edit security log]
user@host# set source-address 1.2.3.4 stream utm-welf format welf category
content-security severity emergency host 5.6.7.8
```

**Results** From configuration mode, confirm your configuration by entering the **show security log** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security log
stream utm-welf {
    severity emergency;
    format welf;
    category content-security;
    host {
        5.6.7.8;
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### Verifying the Security Log

**Purpose** Verify that the WELF log for UTM features is complete.

**Action** From operational mode, enter the **show security utm status** command to verify if the UTM service is running or not.

- Related Documentation**
- [Unified Threat Management Overview on page 3](#)
  - [Understanding UTM Custom Objects on page 4](#)
  - [Understanding UTM Licensing on page 7](#)
  - [Updating UTM Licenses \(CLI Procedure\) on page 8](#)

## CHAPTER 4

# Configuring UTM for Chassis Cluster

- [Understanding UTM Support for Active/Backup Chassis Cluster on page 13](#)
- [Understanding Chassis Cluster Support for UTM Modules on page 15](#)

## Understanding UTM Support for Active/Backup Chassis Cluster

---

A chassis cluster environment supports UTM with:

- Packet Forwarding Engine in active/backup chassis cluster configurations with the Packet Forwarding Engine and the Routing Engine being active in the same node (On SRX Series devices).



**NOTE:** UTM does not require a separate license for chassis cluster mode. The usual UTM license is sufficient and should be available on both of the nodes in the chassis cluster.

UTM supports stateless (that is, no state regarding UTM is synchronized between the cluster nodes) the Packet Forwarding Engine active/active chassis cluster configurations. All the UTM sessions anchored on the redundancy group being failed over will be aborted and new sessions are set up with the new primary redundancy group.

Stateful active/active cluster mode is not supported. Stateful objects like UTM sessions will not be synchronized; that is, no UTM module runtime objects (RTOs) are synchronized between the cluster nodes. You need to install UTM licenses in both the nodes independently.

UTM is supported in the following chassis cluster mode:

- **Active/backup mode**—In this mode, all the redundancy groups are active in one cluster node. All the transit traffic is processed by this single node.

The transit traffic includes:

- Traffic forwarded between interfaces for redundancy groups 1 and up that are part of the same node

- Traffic forwarded between RGO-controlled interfaces for redundancy groups 1 and up that are in the same node

UTM is supported for the following chassis cluster failover types:

- **Manual failover**—Supports manual failover through the **set chassis cluster failover** command. Both RGO and redundancy groups 1 and up can fail over using this command.
- **RGO automatic failover**—This failover is supported through control link failure, monitoring objects (IP address, interface monitoring), or preempt/priority configuration.
- **Redundancy groups 1 and up automatic failover**—This failover is supported through monitoring objects (IP address, interface monitoring) or preempt/priority configuration. This failover leads to active link changes and can result in active/active mode.
- **Failover through reboot**—A primary node can be changed to a secondary node by rebooting the node. All redundancy groups in the node that's is rebooted will no longer be primary nodes.
- **Failover through flowd restart**—Redundancy groups 1 and up will be changed to secondary nodes when the flowd restarts.

The following UTM features are supported in chassis cluster:

- Content filtering
- URL (Web) filtering
- Antispam filtering
- Sophos antivirus scanning

All the UTM configurations are either maintained in the Routing Engine or pushed to the Packet Forwarding Engine from the Routing Engine. The configuration synchronization between the two nodes is taken care of by the chassis cluster infrastructure. This holds true for all the UTM modules too. You can configure UTM either from the primary or secondary node, and the same configuration will be reflected in the other node once you commit the first configuration.

There is a dependency on ACL support on control links. The time taken to spawn the processes depends on the device. There will be a small delay for the Unified Threat Management daemon (utmd) to come up operationally, even though utmd daemon is running in the secondary Routing Engine, because there can be a startup delay for all the dependant daemons.

#### **Related Documentation**

- *Chassis Cluster Overview*
- *Preparing Your Equipment for Chassis Cluster Formation*
- *Understanding Chassis Cluster Redundancy Groups*
- *Understanding Chassis Cluster Redundant Ethernet Interfaces*
- [Unified Threat Management Overview on page 3](#)
- [Understanding Chassis Cluster Support for UTM Modules on page 15](#)

## Understanding Chassis Cluster Support for UTM Modules

---

- **Content filtering**—Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, and protocol command. The content filter controls file transfers across the gateway by checking traffic against configured filter lists.

In content filtering, the user configuration (mime-pattern/filename-extension/protocol-command/content-type) is pushed from the Routing Engine to the Packet Forwarding Engine real-time (PFE-RT). The filtering decision is entirely based on the user configuration and is done on the Packet Forwarding Engine real-time (PFE-RT) side. For the transit traffic, the configuration lookup (for the block/permit decision) and the entire UTM processing occurs in the Packet Forwarding Engine itself and does not go to the Routing Engine (that is, the complete UTM session resides in the Packet Forwarding Engine).

- **URL (Web) filtering**—Web filtering lookups takes place in the primary Routing Engine and both the Packet Forwarding Engines send the lookup request to the primary Routing Engine.
- **Antispam filtering**—Antispam filtering pushes the user configuration (whitelist and blacklist) from the Routing Engine to the PFE-RT.
- **Sophos Antivirus Scanning**—Sophos antivirus scanning is done on the Packet Forwarding Engine real-time (PFE-RT) of each node where the UTM traffic is anchored. The signature database files are downloaded by the primary Routing Engine (RE) and synchronized to its PFE-RT side. After it succeeds, the database files will be synchronized to the secondary RE and then to its PFE-RT. If configured, the primary Routing Engine performs the periodic signature database update and synchronizes it to the secondary Routing Engine and both PFE-RTs.

### Related Documentation

- *Chassis Cluster Overview*
- *Preparing Your Equipment for Chassis Cluster Formation*
- *Understanding Chassis Cluster Redundancy Groups*
- *Understanding Chassis Cluster Redundant Ethernet Interfaces*
- [Unified Threat Management Overview on page 3](#)
- [Understanding UTM Support for Active/Backup Chassis Cluster on page 13](#)



## PART 2

# Configuring Antispam Filtering

- [Understanding Antispam Filtering on page 19](#)
- [Configuring Server-Based Antispam Filtering on page 21](#)
- [Configuring Local List Antispam Filtering on page 29](#)



## CHAPTER 5

# Understanding Antispam Filtering

- [Antispam Filtering Overview on page 19](#)
- [Handling Spam Messages on page 19](#)

## Antispam Filtering Overview

---

Spam consists of unwanted e-mail messages, usually sent by commercial, malicious, or fraudulent entities. The antispam feature examines transmitted e-mail messages to identify spam. When the device detects a message deemed to be spam, it blocks the e-mail message or tags the e-mail message header or subject with a preprogrammed string.

Antispam filtering allows you to use both a third-party server-based spam block list (SBL) and to optionally create your own local whitelists (benign) and blacklists (malicious) for filtering against e-mail messages. The antispam feature is not meant to replace your antispam server, but to complement it.

### Related Documentation

- [Understanding Server-Based Antispam Filtering on page 21](#)
- [Server-Based Antispam Filtering Configuration Overview on page 22](#)
- [Understanding Local List Antispam Filtering on page 29](#)
- [Local List Antispam Filtering Configuration Overview on page 30](#)
- [Handling Spam Messages on page 19](#)

## Handling Spam Messages

---

There are two possible actions the device can take when spam is detected. It can perform a drop action or a tag action.

- [Blocking Detected Spam on page 19](#)
- [Tagging Detected Spam on page 20](#)

## Blocking Detected Spam

The device can block and drop detected spam at either the connection level or the e-mail level:

- Blocking spam at the connection level

When the SMTP sender is identified as a spam sender based on its IP address, the SMTP connection is rejected and dropped. An error message with a proper error code from the firewall is sent out on behalf of the SMTP server. An example of such an error message is:

554 Transaction failed due to anti spam setting

- Blocking spam at the e-mail level

When a particular e-mail sender is identified as spam sender based on its sender address, the e-mail is rejected and dropped. An error message with a proper error code from the firewall is sent back to the sender on behalf of the server. An example of such an error message is:

550 Requested action not taken: mailbox unavailable

## Tagging Detected Spam

The device can allow and tag the e-mail if the message sender is detected as a spammer. This tagging can occur at the connection level so that all the e-mails for the connection in question are tagged. Otherwise, you can tag only an individual e-mail. Two tagging methods are supported:

- Tag the subject: A user-defined string is added at the beginning of the subject of the e-mail.
- Tag the header: A user-defined string is added to the e-mail header.

### Related Documentation

- [Antispam Filtering Overview on page 19](#)
- [Server-Based Antispam Filtering Configuration Overview on page 22](#)
- [Local List Antispam Filtering Configuration Overview on page 30](#)

## CHAPTER 6

# Configuring Server-Based Antispam Filtering

- [Understanding Server-Based Antispam Filtering on page 21](#)
- [Server-Based Antispam Filtering Configuration Overview on page 22](#)
- [Example: Configuring Server-Based Antispam Filtering on page 23](#)

### Understanding Server-Based Antispam Filtering

Server-based antispam filtering requires Internet connectivity with the spam block list (SBL) server. Domain Name Service (DNS) is required to access the SBL server. The firewall performs SBL lookups through the DNS protocol. The lookups are against the IP address of the sender (or relaying agent) of the e-mail, adding the name of the SBL server as the authoritative domain. The DNS server then forwards each request to the SBL server, which returns a DNS response to the device. The device then interprets the DNS response to determine if the e-mail sender is a spammer.

IP addresses that are included in the block lists are generally considered to be invalid addresses for mail servers or easily compromised addresses. Criteria for listing an IP address as a spammer on the SBL can include:

- Running an SMTP open relay service
- Running open proxy servers (of various kinds)
- Being a zombie host possibly compromised by a virus, worm, Trojan, or spyware
- Using a dynamic IP range
- Being a confirmed spam source with a known IP address

By default, the device first checks incoming e-mail against local whitelists and blacklists. If there are no local lists, or if the sender is not found on local lists, the device proceeds to query the SBL server over the Internet. When both server-based spam filtering and local list spam filtering are enabled, checks are done in the following order:

1. The local whitelist is checked. If there is a match, no further checking is done. If there is no match...
2. The local blacklist is checked. If there is a match, no further checking is done. If there is no match...

3. The SBL server list is checked.

**NOTE:**

- SBL server matching stops when the antispam license key is expired.
- Server-based spam filtering supports only IP-based spam block list blacklist lookup. Sophos updates and maintains the IP-based spam block list. Server-based antispam filtering is a separately licensed subscription service. When your antispam license key expires, you can continue to use locally defined blacklists and whitelists.

**Related Documentation**

- [Antispam Filtering Overview on page 19](#)
- [Server-Based Antispam Filtering Configuration Overview on page 22](#)
- [Example: Configuring Server-Based Antispam Filtering on page 23](#)
- [Local List Antispam Filtering Configuration Overview on page 30](#)
- [Understanding Local List Antispam Filtering on page 29](#)
- [Handling Spam Messages on page 19](#)

## Server-Based Antispam Filtering Configuration Overview

For each UTM feature, configure feature parameters in the following order:

1. Configure UTM custom objects for the feature:

```
user@host# set security utm custom-objects
```

2. Configure the main feature parameters, using feature profiles.

```
user@host# set security utm feature-profile anti-spam
```

3. Configure a UTM policy for each protocol, and attach this policy to a profile.

```
user@host# set security utm utm-policy utmp1 anti-spam smtp-profile smtp1
```



**NOTE:** Antispam filtering is only supported for the SMTP protocol.

4. Attach the UTM policy to a security policy.

```
user@host# set security policies from-zone trust to-zone untrust policy p1 then permit
application-services utm-policy utmp1
```

**Related Documentation**

- [Antispam Filtering Overview on page 19](#)
- [Understanding Server-Based Antispam Filtering on page 21](#)
- [Example: Configuring Server-Based Antispam Filtering on page 23](#)
- [Understanding Local List Antispam Filtering on page 29](#)

- [Local List Antispam Filtering Configuration Overview on page 30](#)
- [Handling Spam Messages on page 19](#)

## Example: Configuring Server-Based Antispam Filtering

This example shows how to configure server-based antispam filtering.

- [Requirements on page 23](#)
- [Overview on page 23](#)
- [Configuration on page 23](#)
- [Verification on page 28](#)

### Requirements

Before you begin, review how to configure the feature parameters for each UTM feature. See “[Server-Based Antispam Filtering Configuration Overview](#)” on page 22.

### Overview

Server-based antispam filtering requires Internet connectivity with the spam block list (SBL) server. Domain Name Service (DNS) is required to access the SBL server.

### Configuration

#### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile anti-spam sbl profile sblprofile1 sbl-default-server
set security utm feature-profile anti-spam sbl profile sblprofile1 sbl-default-server
spam-action block
set security utm feature-profile anti-spam sbl profile sblprofile1 sbl-default-server
custom-tag-string ***spam***
set security utm utm-policy spampolicy1 anti-spam smtp-profile sblprofile1
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy1 match
source-address any
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy1 match
destination-address any
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy1 match
application junos-smtp
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy1 then permit
application-services utm-policy spampolicy1
```

**GUI Step-by-Step  
Procedure**

To configure server-based antispam filtering:

1. Configure a profile and enable/disable the SBL server lookup. Select **Configure>Security>UTM>Anti-Spam**.
  - a. In the Anti-Spam profiles configuration window, click **Add** to configure a profile for the SBL server, or click **Edit** to modify an existing item.
  - b. In the Profile name box, enter a unique name for the antispam profile that you are creating.
  - c. If you are using the default server, select **Yes** next to Default SBL server. If you are not using the default server, select **No**.



**NOTE:** The SBL server is predefined on the device. The device comes preconfigured with the name and address of the SBL server. If you do not select Yes, you are disabling server-based spam filtering. You should disable it only if you are using only local lists or if you do not have a license for server-based spam filtering.

- d. In the Custom tag string box, enter a custom string for identifying a message as spam. By default, the devices uses **\*\*\*SPAM\*\*\***.
  - e. From the antispam action list, select the action that the device should take when it detects spam. Options include Tag subject, Block email, and Tag header.
2. Configure a UTM policy for SMTP to which you attach the antispam profile.
  - a. Select **Configure>Security>Policy>UTM Policies**.
  - b. In the UTM policy configuration window, click **Add**.
  - c. In the policy configuration window, select the **Main** tab.
  - d. In the Policy name box, type a unique name for the UTM policy.
  - e. In the Session per client limit box, type a session per client limit. Valid values range from 0 to 2000.
  - f. From the Session per client over limit list, select the action that the device should take when the session per client limit for this UTM policy is exceeded. Options include Log and permit and Block.
  - g. Select the **Anti-Spam profiles** tab in the pop-up window.
  - h. From the SMTP profile list, select an antispam profile to attach to this UTM policy.

3. Attach the UTM policy to a security policy.
  - a. Select **Configure>Security>Policy>FW Policies**.
  - b. In the Security Policy window, click **Add** to configure a security policy with UTM or click **Edit** to modify an existing policy.
  - c. In the Policy tab, type a name in the **Policy Name** box.
  - d. Next to From Zone, select a zone from the list.
  - e. Next to To Zone, select a zone from the list.
  - f. Choose a source address.
  - g. Choose a destination address.
  - h. Choose an application by selecting **junos-smtp** (for antispam) in the Application Sets box and move it to the Matched box.
  - i. Next to Policy Action, select one of the following: **Permit**, **Deny**, or **Reject**.



**NOTE:** When you select Permit for Policy Action, several additional fields become available in the Applications Services tab, including UTM Policy.

- j. Select the **Application Services** tab.
- k. Next to UTM Policy, select the appropriate policy from the list. This attaches your UTM policy to the security policy.
- l. Click **OK** to check your configuration and save it as a candidate configuration.
- m. If the policy is saved successfully, you receive a confirmation, and you must click **OK** again. If the profile is not saved successfully, click **Details** in the pop-up window to discover why.



**NOTE:**

- You must activate your new policy to apply it.
- In SRX Series devices the confirmation window that notifies you that the policy is saved successfully disappears automatically.

- n. If you are done configuring the device, click **Commit Options>Commit**.

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure server-based antispam filtering:

1. Create a profile.

```
[edit security]
user@host# set utm feature-profile anti-spam sbl profile sblprofile1
```

2. Enable or disable the default SBL server lookup.

```
[edit security]
user@host# set utm feature-profile anti-spam sbl profile sblprofile1
sbl-default-server
```



**NOTE:** If you are using server-based antispam filtering, you should type `sbl-default-server` to enable the default SBL server. (The SBL server is predefined on the device. The device comes preconfigured with the name and address of the SBL server.) You should disable server-based antispam filtering using the `no-sbl-default-server` option only if you are using only local lists or if you do not have a license for server-based spam filtering.

3. Configure the action to be taken by the device when spam is detected (block, tag-header, or tag-subject).

```
[edit security]
user@host# set utm feature-profile anti-spam sbl profile sblprofile1sbl-default-server
spam-action block
```

4. Configure a custom string for identifying a message as spam.

```
[edit security]
user@host# set utm feature-profile anti-spam sbl profile sblprofile1
sbl-default-server custom-tag-string ***spam***
```

5. Attach the spam feature profile to the UTM policy.

```
[edit security]
user@host# set utm utm-policy spampolicy1 anti-spam smtp-profile sblprofile1
```

6. Configure a security policy for UTM to which to attach the UTM policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy
utmsecuritypolicy1 match source-address any
user@host# set security policies from-zone trust to-zone untrust policy
utmsecuritypolicy1 match destination-address any
user@host# set security policies from-zone trust to-zone untrust policy
utmsecuritypolicy1 match application junos-smtp
user@host# set security policies from-zone trust to-zone untrust policy
utmsecuritypolicy1 then permit application-services utm-policy spampolicy1
```



**NOTE:** The device comes preconfigured with a default antispam policy. The policy is called `junos-as-defaults`. It contains the following configuration parameters:

```
anti-spam {
  sbl {
    profile junos-as-defaults {
      sbl-default-server;
      spam-action block;
      custom-tag-string "****SPAM****";
    }
  }
}
```

**Results** From configuration mode, confirm your configuration by entering the **show security utm** and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security utm
feature-profile {
  anti-spam {
    sbl {
      profile sblprofile1 {
        sbl-default-server;
        spam-action block;
        custom-tag-string ***spam***;
      }
    }
  }
}
utm-policy spampolicy1 {
  anti-spam {
    smtp-profile sblprofile1;
  }
}
```

```
[edit]
user@host# show security policies
from-zone trust to-zone untrust {
  policy utmsecuritypolicy1 {
    match {
      source-address any;
      destination-address any;
      application junos-smtp;
    }
    then {
      permit {
        application-services {
          utm-policy spampolicy1;
        }
      }
    }
  }
}
```

```
}  
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### Verifying Antispam Statistics

---

**Purpose** Verify the antispam statistics.

**Action** From operational mode, enter the **show security utm anti-spam status** and **show security utm anti-spam statistics** commands.

The following information appears:

```
SBL Whitelist Server:  
SBL Blacklist Server:  
msgsecurity.example.net  
DNS Server:  
Primary : 1.2.3.4, Src Interface: ge-0/0/0  
Secondary: 2.3.4.5, Src Interface: ge-0/0/1  
Ternary : 0.0.0.0, Src Interface: fe-0/0/2  
  
Total connections: #  
Denied connections: #  
Total greetings: #  
Denied greetings: #  
Total e-mail scanned: #  
White list hit: #  
Black list hit: #  
Spam total: #  
Spam tagged: #  
Spam dropped: #  
DNS errors: #  
Timeout errors: #  
Return errors: #  
Invalid parameter errors: #  
Statistics start time:  
Statistics for the last 10 days.
```

- Related Documentation**
- [Antispam Filtering Overview on page 19](#)
  - [Understanding Server-Based Antispam Filtering on page 21](#)
  - [Server-Based Antispam Filtering Configuration Overview on page 22](#)
  - [Understanding Local List Antispam Filtering on page 29](#)
  - [Local List Antispam Filtering Configuration Overview on page 30](#)
  - [Handling Spam Messages on page 19](#)
  - [spam-action on page 228](#)

## CHAPTER 7

# Configuring Local List Antispam Filtering

- [Understanding Local List Antispam Filtering on page 29](#)
- [Local List Antispam Filtering Configuration Overview on page 30](#)
- [Example: Configuring Local List Antispam Filtering on page 30](#)

## Understanding Local List Antispam Filtering

---

When creating your own local whitelist and blacklist for antispam filtering, you can filter against domain names, e-mail addresses, and/or IP addresses. Pattern matching works a bit differently depending upon the type of matching in question. For example, pattern matching for domain names uses a longest suffix match algorithm. If the sender e-mail address has a domain name of aaa.bbb.ccc, the device tries to match "aaa.bbb.ccc" in the list. If no match is found, it tries to match "bbb.ccc", and then "ccc". IP address matching, however, does not allow for partial matches.

Antispam filtering uses local lists for matching in the following manner:

1. **Sender IP:** The sender IP is checked against the local whitelist, then the local blacklist, and then the SBL IP-based server (if enabled).
2. **Sender Domain:** The domain name is checked against the local whitelist and then against the local blacklist.
3. **Sender E-mail Address:** The sender e-mail address is checked against the local whitelist and then against the local blacklist.

By default, the device first checks incoming e-mail against the local whitelist and blacklist. If the sender is not found on either list, the device proceeds to query the SBL server over the Internet. When both server-based antispam filtering and local list antispam filtering are enabled, checks are done in the following order:

1. The local whitelist is checked. If there is a match, no further checking is done. If there is no match...
2. The local blacklist is checked. If there is a match, no further checking is done. If there is no match...
3. The SBL server list is checked.



**NOTE:** Local blacklist and whitelist matching continues after the antispam license key is expired.

**Related Documentation**

- [Antispam Filtering Overview on page 19](#)
- [Local List Antispam Filtering Configuration Overview on page 30](#)
- [Example: Configuring Local List Antispam Filtering on page 30](#)
- [Server-Based Antispam Filtering Configuration Overview on page 22](#)
- [Handling Spam Messages on page 19](#)

---

## Local List Antispam Filtering Configuration Overview

For each UTM feature, configure feature parameters in the following order:

1. Configure UTM custom objects for the feature:

```
user@host# set security utm custom-objects url-pattern url-pattern-name
```

2. Configure the main feature parameters, using feature profiles.

```
user@host# set security utm feature-profile anti-spam as-profile-name
```

3. Configure a UTM policy for each protocol, and attach this policy to a profile.

```
user@host# set security utm utm-policy utmp1 anti-spam smtp-profile smtp1
```

4. Attach the UTM policy to a security policy.

```
user@host# set security policies from-zone trust to-zone untrust policy p1 then permit  
application-services utm-policy utmp1
```

**Related Documentation**

- [Antispam Filtering Overview on page 19](#)
- [Understanding Local List Antispam Filtering on page 29](#)
- [Example: Configuring Local List Antispam Filtering on page 30](#)
- [Understanding Server-Based Antispam Filtering on page 21](#)
- [Handling Spam Messages on page 19](#)

---

## Example: Configuring Local List Antispam Filtering

This example shows how to configure local list antispam filtering.

- [Requirements on page 31](#)
- [Overview on page 31](#)
- [Configuration on page 31](#)
- [Verification on page 36](#)

## Requirements

Before you begin, review how to configure the feature parameters for each UTM feature. See [“Local List Antispam Filtering Configuration Overview” on page 30](#).

## Overview

Antispam filtering uses local lists for matching. When creating your own local whitelist and blacklist for antispam filtering, you can filter against domain names, e-mail addresses, and/or IP addresses.

## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm custom-objects url-pattern as-black value [150.61.8.134]
set security utm custom-objects url-pattern as-white value [150.1.2.3]
set security utm feature-profile anti-spam address-whitelist as-white
set security utm feature-profile anti-spam sbl profile localprofile1
set security utm feature-profile anti-spam sbl profile localprofile1 spam-action block
set security utm feature-profile anti-spam sbl profile localprofile1 custom-tag-string
  ***spam***
set security utm utm-policy spampolicy2 anti-spam smtp-profile localprofile1
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy2 match
  source-address any
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy2 match
  destination-address any
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy2 match
  application junos-smtp
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy2 then permit
  application-services utm-policy spampolicy2
```

### GUI Step-by-Step Procedure

To configure local list antispam filtering:

1. Create local whitelist and blacklist custom objects by configuring a URL pattern list.
  - a. Select **Configure>Security>UTM>Custom Objects**.
  - b. In the UTM custom objects configuration window, select the **URL Pattern List** tab.
  - c. Click **Add** to create URL pattern lists.
  - d. Next to URL Pattern Name, type a unique name.



**NOTE:** If you are creating a whitelist, it is helpful to indicate this in the list name. The same applies to a blacklist. The name you enter here becomes available in the Address Whitelist and Address Blacklist fields when you are configuring your antispam profiles.

- e. Next to URL Pattern Value, type the URL pattern for whitelist or blacklist antispam filtering.
2. Configure antispam filtering to use the whitelist and blacklist custom objects.
  - a. Select **Configure>Security>UTM>Global options**.
  - b. In the right pane, select the **Anti-Spam** tab.
  - c. Under Anti-Spam, select an Address Whitelist and/or an Address Blacklist from the list for local lists for spam filtering. (These lists are configured as custom objects.)
  - d. Click **OK**.
  - e. If the configuration item is saved successfully, you receive a confirmation, and you must click **OK** again. If it is not saved successfully, click **Details** in the pop-up window to discover why.
  - f. In the left pane under Security, select the **Anti-Spam** tab.
  - g. Click **Add** to configure an anti-spam profile. The profile configuration pop-up window appears.
  - h. In the Profile name box, enter a unique name.
  - i. If you are using the default server, select **Yes** beside Default SBL server. If you are not using the default server, select **No**.



**NOTE:** If you select No, you are disabling server-based spam filtering. You disable it only if you are using local lists or if you do not have a license for server-based spam filtering.

- j. In the Custom tag string box, type a custom string for identifying a message as spam. By default, the device uses **\*\*\*SPAM\*\*\***.
  - k. In the Actions list, select the action that the device should take when it detects spam. Options include Tag subject, Block email, and Tag header.
3. Configure a UTM policy for SMTP to which you attach the antispam profile.
    - a. Select **Configure>Security>Policy>UTM Policies**.
    - b. In the UTM policy configuration window, click **Add** to configure a UTM policy. The policy configuration pop-up window appears.
    - c. Select the **Main** tab.
    - d. In the Policy name box, type a unique name.
    - e. In the Session per client limit box, type a session per client limit. Valid values range from 0 through 2000.
    - f. From the Session per client over limit list, select the action that the device should take when the session per client limit for this UTM policy is exceeded. Options include Log and permit and Block.
    - g. Select the **Anti-Spam profiles** tab.
    - h. From the SMTP profile list, select the antispam profile that you are attaching to this UTM policy.
  4. Attach the UTM policy to a security policy.
    - a. Select **Configure>Security>Policy>FW Policies**.
    - b. In the Security Policy window, click **Add** to configure a security policy with UTM. The policy configuration pop-up window appears.
    - c. In the Policy tab, type a name in the Policy Name box.
    - d. Next to From Zone, select a zone from the list.
    - e. Next to To Zone, select a zone from the list.
    - f. Choose a source address.
    - g. Choose a destination address.
    - h. Choose an application by selecting **junos-smtp** (for antispam) in the Application Sets box and move it to the Matched box.
    - i. Next to Policy Action, select one of the following: **Permit, Deny, or Reject**.



**NOTE:** When you select Permit for policy action, several additional fields become available in the Applications Services tab, including UTM Policy.

- j. Select the **Application Services** tab.
- k. Next to UTM Policy, select the appropriate policy from the list. This attaches your UTM policy to the security policy.
- l. Click **OK** to check your configuration and save it as a candidate configuration.
- m. If the policy is saved successfully, you receive a confirmation, and you must click **OK** again. If the profile is not saved successfully, click **Details** in the pop-up window to discover why.



**NOTE:** You must activate your new policy to apply it.

- n. If you are done configuring the device, click **Commit Options>Commit**.

#### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration* in the *CLI User Guide*.

To configure local list antispam filtering:

1. Configure the local list spam blocking by first creating your global local spam lists.  

```
[edit security]
user@host# set utm custom-objects url-pattern as-black value [150.61.8.134]
user@host# set utm custom-objects url-pattern as-white value [150.1.2.3]
```

2. Configure the local list antispam feature profile by first attaching your custom-object blacklist or whitelist or both.

```
[edit security]
user@host# set utm feature-profile anti-spam address-whitelist as-white
```



**NOTE:** When both the whitelist and the blacklist are in use, the whitelist is checked first. If there is no match, then the blacklist is checked.

3. Configure a profile for your local list spam blocking.

```
[edit security]
user@host# set utm feature-profile anti-spam sbl profile localprofile1
```



**NOTE:** Although you are not using the SBL for local list spam blocking, you configure your profile from within that command similar to the server-based spam blocking procedure.

4. Configure the action to be taken by the device when spam is detected (block, tag-header, tag-subject).

```
[edit security]
user@host# set utm feature-profile anti-spam sbl profile localprofile1 spam-action
block
```

5. Configure a custom string for identifying a message as spam.

```
[edit security]
user@host# set utm feature-profile anti-spam sbl profile localprofile1
custom-tag-string ***spam***
```

6. Attach the spam feature profile to the UTM policy.

```
[edit security]
user@host# set utm utm-policy spampolicy2 anti-spam smtp-profile localprofile1
```

7. Configure a security policy for UTM, and attach the UTM policy to the security policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy
utmsecuritypolicy2 match source-address any
user@host# set security policies from-zone trust to-zone untrust policy
utmsecuritypolicy2 match destination-address any
user@host# set security policies from-zone trust to-zone untrust policy
utmsecuritypolicy2 match application junos-smtp
user@host# set security policies from-zone trust to-zone untrust policy
utmsecuritypolicy2 then permit application-services utm-policy spampolicy2
```

**Results** From configuration mode, confirm your configuration by entering the **show security utm** and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security utm
custom-objects {
  anti-spam {
    url-pattern patternwhite;
    address-whitelist as-white;
    sbl {
      profile localprofile1 {
        spam-action block;
        custom-tag-string ***spam***;
      }
    }
  }
}
utm-policy spampolicy2 {
  anti-spam {
    smtp-profile localprofile1;
  }
}
```

```
[edit]
user@host# show security policies
from-zone trust to-zone untrust {
  policy utmsecuritypolicy2 {
    match {
      source-address any;
      destination-address any;
      application junos-smtp;
    }
  }
}
```

```
    }
    then {
        permit {
            application-services {
                utm-policy spampolicy2;
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### Verifying Antispam Statistics

---

**Purpose** Verify the antispam statistics.

**Action** From operational mode, enter the **show security utm anti-spam status** and **show security utm anti-spam statistics** commands.

The following information appears:

```
SBL Whitelist Server:
SBL Blacklist Server:
msgsecurity.example.net
DNS Server:
Primary : 1.2.3.4, Src Interface: ge-0/0/0
Secondary: 2.3.4.5, Src Interface: ge-0/0/1
Ternary : 0.0.0.0, Src Interface: fe-0/0/2

Total connections: #
Denied connections: #
Total greetings: #
Denied greetings: #
Total e-mail scanned: #
White list hit: #
Black list hit: #
Spam total: #
Spam tagged: #
Spam dropped: #
DNS errors: #
Timeout errors: #
Return errors: #
Invalid parameter errors: #
Statistics start time:
Statistics for the last 10 days.
```

**Related Documentation**

- [Antispam Filtering Overview on page 19](#)
- [Understanding Local List Antispam Filtering on page 29](#)
- [Local List Antispam Filtering Configuration Overview on page 30](#)
- [Handling Spam Messages on page 19](#)

- [spam-action on page 228](#)



## CHAPTER 8

# Configuring Whitelists

- [Understanding MIME Whitelists on page 39](#)
- [Example: Configuring MIME Whitelists to Bypass Antivirus Scanning on page 40](#)
- [Understanding URL Whitelists on page 40](#)
- [Configuring URL Whitelists to Bypass Antivirus Scanning \(CLI Procedure\) on page 41](#)

### Understanding MIME Whitelists

---

The gateway device uses MIME (Multipurpose Internet Mail Extension) types to decide which traffic may bypass antivirus scanning. The MIME whitelist defines a list of MIME types and can contain one or many MIME entries.

A MIME entry is case-insensitive. An empty MIME is an invalid entry and should never appear in the MIME list. If the MIME entry ends with a / character, prefix matching takes place. Otherwise, exact matching occurs.

There are two types of MIME lists used to configure MIME type antivirus scan bypassing:

- **mime-whitelist list**—This is the comprehensive list for those MIME types that can bypass antivirus scanning.
- **exception list**—The exception list is a list for excluding some MIME types from the mime-whitelist list. This list is a subset of MIME types found in the mime-whitelist.

For example, if the mime-whitelist includes the entry, **video/** and the exception list includes the entry **video/x-shockwave-flash**, by using these two lists, you can bypass objects with “video/” MIME type but not bypass “video/x-shockwave-flash” MIME type.

You should note that there are limits for mime-whitelist entries as follows:

- The maximum number of MIME items in a MIME list is 50.
- The maximum length of each MIME entry is restricted to 40 bytes.
- The maximum length of a MIME list name string is restricted to 40 bytes.

#### Related Documentation

- [Full Antivirus Protection Overview](#)
- [Example: Configuring MIME Whitelists to Bypass Antivirus Scanning on page 40](#)
- [Understanding URL Whitelists on page 40](#)

- [Configuring URL Whitelists to Bypass Antivirus Scanning \(CLI Procedure\) on page 41](#)

## Example: Configuring MIME Whitelists to Bypass Antivirus Scanning

---

This example shows how to configure MIME whitelists to bypass antivirus scanning.

- [Requirements on page 40](#)
- [Overview on page 40](#)
- [Configuration on page 40](#)
- [Verification on page 40](#)

### Requirements

Before you begin, decide the type of MIME lists used to configure MIME type antivirus scan bypassing. See “[Understanding MIME Whitelists](#)” on page 39.

### Overview

In this example, you create MIME lists called avmime2 and ex-avmime2 and add patterns to them.

### Configuration

#### Step-by-Step Procedure

To configure MIME whitelists to bypass antivirus scanning:

1. Create MIME lists and add patterns to the lists.  

```
[edit]
user@host# set security utm custom-objects mime-pattern avmime2 value
[video/quicktime image/x-portable-anymap x-world/x-vrml]
user@host# set security utm custom-objects mime-pattern ex-avmime2 value
[video/quicktime-inappropriate]
```
2. If you are done configuring the device, commit the configuration.  

```
[edit]
user@host# commit
```

### Verification

To verify the configuration is working properly, enter the **show security utm** command.

#### Related Documentation

- [Full Antivirus Protection Overview](#)
- [Understanding URL Whitelists on page 40](#)
- [Configuring URL Whitelists to Bypass Antivirus Scanning \(CLI Procedure\) on page 41](#)

## Understanding URL Whitelists

---

A URL whitelist is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for scanning. Because antivirus

scanning is CPU and memory intensive action, if there are URLs or IP addresses that you are sure do not require scanning, you might want to create this custom list and add them to it.

- Related Documentation**
- [Full Antivirus Protection Overview](#)
  - [Understanding MIME Whitelists on page 39](#)
  - [Example: Configuring MIME Whitelists to Bypass Antivirus Scanning on page 40](#)
  - [Configuring URL Whitelists to Bypass Antivirus Scanning \(CLI Procedure\) on page 41](#)

---

## Configuring URL Whitelists to Bypass Antivirus Scanning (CLI Procedure)

---

To configure URL whitelists, use the following CLI configuration statements:

```
security utm custom-objects {  
  custom-url-category { ; set of list  
    name url-category-name; #mandatory  
    value url-pattern-name;  
  }  
}
```

- Related Documentation**
- [Full Antivirus Protection Overview](#)
  - [Understanding MIME Whitelists on page 39](#)
  - [Example: Configuring MIME Whitelists to Bypass Antivirus Scanning on page 40](#)
  - [Understanding URL Whitelists on page 40](#)



## PART 3

# Configuring and Managing Sophos Antivirus Protection

- [Configuring Sophos Antivirus Protection on page 45](#)



## CHAPTER 9

# Configuring Sophos Antivirus Protection

- [Sophos Antivirus Protection Overview on page 45](#)
- [Sophos Antivirus Features on page 46](#)
- [Understanding Sophos Antivirus Data File Update on page 47](#)
- [Sophos Antivirus Configuration Overview on page 48](#)
- [Example: Configuring Sophos Antivirus Custom Objects on page 48](#)
- [Example: Configuring Sophos Antivirus Feature Profile on page 52](#)
- [Example: Configuring Sophos Antivirus UTM Policies on page 58](#)
- [Example: Configuring Sophos Antivirus Firewall Security Policies on page 59](#)
- [Example: Configuring Sophos Antivirus Scanner with SSL Forward Proxy on page 61](#)
- [Managing Sophos Antivirus Data Files on page 67](#)

## Sophos Antivirus Protection Overview

---

Sophos antivirus is as an in-the-cloud antivirus solution. The virus pattern and malware database is located on external servers maintained by Sophos (Sophos Extensible List) servers, thus there is no need to download and maintain large pattern databases on the Juniper device. The Sophos antivirus scanner also uses a local internal cache to maintain query responses from the external list server to improve lookup performance.

Because a significant amount of traffic processed by Juniper Unified Threat Management (UTM) is HTTP based, Uniform Resource Identifier (URI) checking is used to effectively prevent malicious content from reaching the endpoint client or server. The following checks are performed for HTTP traffic: URI lookup, true file type detection, and file checksum lookup. The following application layer protocols are supported: HTTP, FTP, SMTP, POP3 and IMAP.



**NOTE:** Starting with Junos OS Release 12.3X48-D35, the UTM Sophos antivirus (SAV) single session throughput is increased for optimizing tcp-proxy forwarding.

**Release History Table**

Release	Description
12.3X48-D35	Starting with Junos OS Release 12.3X48-D35, the UTM Sophos antivirus (SAV) single session throughput is increased for optimizing tcp-proxy forwarding.

**Related Documentation**

- [Sophos Antivirus Features on page 46](#)
- [Sophos Antivirus Configuration Overview on page 48](#)
- [Understanding TCP Proxy](#)
- [Enabling TCP Proxy Session to Increase the Network Transmit Speed](#)

---

## Sophos Antivirus Features

Sophos antivirus has the following main features:

- **Sophos antivirus expanded MIME decoding support**—Sophos antivirus offers decoding support for HTTP, POP3, SMTP, and IMAP. MIME decoding support includes the following for each supported protocol:
  - Multipart and nested header decoding
  - Base64 decoding, printed quote decoding, and encoded word decoding in the subject field
- **Sophos antivirus supports HTTPS traffic**—Sophos antivirus over SSL forward proxy supports HTTPS traffic by intercepting HTTPS traffic passing through the SRX Series device. The security channel from the SRX Series device is divided as one SSL channel between the client and the SRX Series device and another SSL channel between the SRX Series device and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to UTM. UTM extracts the URL and the file checksum information from cleartext traffic. The Sophos antivirus scanner determines whether to block or permit the requests.

SSL forward proxy does not support client authentication. If client authentication is required by the server, UTM bypasses the traffic. UTM bypasses the HTTPS traffic under the following conditions:

- If SSL proxy does not parse the first handshake packet from the client, SSL forward proxy bypasses the traffic.
  - If the SSL proxy handshake with the client and server is incomplete because of compatibility issues, connection drops.
  - If the system resource is low, SSL forward proxy cannot handle the new connection and Sophos antivirus bypasses the traffic.
  - If HTTPS traffic hits the whitelist of SSL forward proxy, SSL forward proxy and Sophos antivirus bypass the traffic.
- **Sophos antivirus scan result handling**—With Sophos antivirus, the TCP traffic is closed gracefully when a virus is found and the data content is dropped.

The following fail mode options are supported: content-size, default, engine-not-ready, out-of-resource, timeout, and too-many-requests. You can set the following actions: block, log-and-permit, and permit.

- **Sophos Uniform Resource Identifier checking**—Sophos provides Uniform Resource Identifier (URI) checking, which is similar to antispam realtime blackhole list (RBL) lookups. URI checking is a way of analyzing URI content in HTTP traffic against the Sophos database to identify malware or malicious content. Because malware is predominantly static, a checksum mechanism is used to identify malware to improve performance. Files that are capable of using a checksum include .exe, .zip, .rar, .swf, .pdf, and .ole2 (doc and xls).



**NOTE:** If you have a Juniper Networks device protecting an internal network that has no HTTP traffic, or has web servers that are not accessible to the outside world, you might want to turn off URI checking. If the web servers are not accessible to the outside world, it is unlikely that they contain URI information that is in the Sophos URI database. URI checking is on by default.

#### Related Documentation

- [Sophos Antivirus Protection Overview on page 45](#)
- [Sophos Antivirus Configuration Overview on page 48](#)
- [Example: Configuring Sophos Antivirus Feature Profile on page 52](#)

## Understanding Sophos Antivirus Data File Update

Sophos antivirus uses a small set of data files that need to be updated periodically. These data files only contain information on guiding scanning logic and do not contain the full pattern database. The main pattern database, which includes protection against critical viruses, URI checks, malware, worms, Trojans, and spyware, is located on remote Sophos Extensible List servers maintained by Sophos.

The Sophos data files are updated over HTTP or HTTPS and can be updated manually or scheduled to update automatically. With Sophos antivirus:

- The signature database auto-update interval is once a day by default. This interval can be changed.
- There is no interruption in virus scanning capability during the data file update. If the update fails, the existing data files will continue to be used.
- By default, the URL for Sophos antivirus data file update is <http://update.juniper-updates.net/SAV/>.



**NOTE:** The Sophos antivirus scanning feature is a separately licensed subscription service. When your antivirus license key expires, functionality will no longer work because the pattern lookup database is located on remote Sophos servers. You have a 30-day grace period in which to update your license.

---

**Related  
Documentation**

- [Sophos Antivirus Protection Overview on page 45](#)
- [Managing Sophos Antivirus Data Files on page 67](#)
- [Sophos Antivirus Configuration Overview on page 48](#)

---

## Sophos Antivirus Configuration Overview

---

Sophos antivirus is part of the Unified Threat Management (UTM) feature set, so you first configure UTM options (custom objects), configure the Sophos Feature, then create a UTM policy and a security policy. The security policy controls all traffic that is forwarded by the device, and the UTM policy specifies which parameters to use to scan traffic. The UTM policy is also used to bind a set of protocols to one or more UTM feature profiles, including Sophos antivirus in this case.

You must complete the following tasks to configure Sophos antivirus:

1. Configure UTM custom objects and MIME lists. See [“Example: Configuring Sophos Antivirus Custom Objects” on page 48](#),
2. Configure the Sophos antivirus feature profile. See [“Example: Configuring Sophos Antivirus Feature Profile” on page 52](#).
3. Configure a UTM policy. See [“Example: Configuring Sophos Antivirus UTM Policies” on page 58](#)
4. Configure a security policy. See [“Example: Configuring Sophos Antivirus Firewall Security Policies” on page 59](#).

**Related  
Documentation**

- [Sophos Antivirus Protection Overview on page 45](#)

---

## Example: Configuring Sophos Antivirus Custom Objects

---

This example shows you how to create UTM global custom objects to be used with Sophos antivirus.

- [Requirements on page 49](#)
- [Overview on page 49](#)
- [Configuration on page 49](#)
- [Verification on page 51](#)

## Requirements

Before you begin, read about UTM custom objects. See [“Understanding UTM Custom Objects” on page 4](#).

## Overview

Configure MIME lists. This includes creating a MIME whitelist and a MIME exception list for antivirus scanning. In this example, you bypass scanning of QuickTime videos, unless if they contain the MIME type quicktime-inappropriate.



**WARNING:** When you configure the MIME whitelist feature, be aware that, because header information in HTTP traffic can be spoofed, you cannot always trust HTTP headers to be legitimate. When a Web browser is determining the appropriate action for a given file type, it detects the file type without checking the MIME header contents. However, the MIME whitelist feature does refer to the MIME encoding in the HTTP header. For these reasons, it is possible in certain cases for a malicious website to provide an invalid HTTP header. For example, a network administrator might inadvertently add a malicious website to a MIME whitelist, and, because the site is in the whitelist, it will not be blocked by Sophos even though Sophos has identified the site as malicious in its database. Internal hosts would then be able to reach this site and could become infected.

## Configuration

### GUI Step-by-Step Procedure

To configure a MIME list:

1. Click the **Configure** tab from the taskbar, and then select **Security>UTM>Custom Objects**.
2. Click the **MIME Pattern List** tab and then click **Add**.
3. In the MIME Pattern Name box, type **avmime2**.
4. In the MIME Pattern Value box, type **video/quicktime**, and click **Add**.
5. In the MIME Pattern Value box, type **image/x-portable-anympa**, and click **Add**.
6. In the MIME Pattern Value box, type **x-world/x-vrml**, and click **Add**.

To configure a MIME exception list:

1. Click the **Configure** tab from the taskbar, and then select **Security>UTM>Custom Objects**.
2. Click the **MIME Pattern List** tab and then select **Add**.
3. In the MIME Pattern Name box, type **exception-avmime2**.
4. In the MIME Pattern Value box, type **video/quicktime-inappropriate** and click **Add**.

Configure a URL pattern list (whitelist) of URLs or addresses that will be bypassed by antivirus scanning. After you create the URL pattern list, you will create a custom URL category list and add the pattern list to it.



**NOTE:** Because you use URL pattern lists to create custom URL category lists, you must configure URL pattern list custom objects before you configure custom URL category lists.

To configure a URL pattern whitelist:

1. Click the **Configure** tab from the taskbar, and then select **Security>UTM>Custom Objects**.
2. Click the **URL Pattern List** tab, and then click **Add**.
3. In the URL Pattern Name box, enter **urlist2**.
4. In the URL Pattern Value box, enter **http://example.net**. (You can also use the IP address of the server instead of the URL.)

Save your configuration:

1. Click **OK** to check your configuration and save it as a candidate configuration.
2. If you are done configuring the device, click **Actions>Commit**.



**NOTE:** URL pattern wildcard support—The wildcard rule is as follows: `\*\.[]\?*` and you must precede all wildcard URLs with `http://`. You can use “\*” only if it is at the beginning of the URL and is followed by a “.”. You can only use “?” at the end of the URL.

The following wildcard syntax is supported: `http://*.example.net`, `http://www.example.ne?`, `http://www.example.n??`. The following wildcard syntax is not supported: `*example.net`, `www.example.ne?`, `http://*example.net`, `http://*`.

#### Step-by-Step Procedure

To configure antivirus protection using the CLI, you must create your custom objects in the following order:

1. Create the MIME whitelist.

```
[edit security utm]
user@host# set custom-objects mime-pattern avmime2 value [video/quicktime
image/x-portable-anymap x-world/x-vrml]
```

Create the MIME exception list.

```
[edit security utm]
```

```
user@host# set custom-objects mime-pattern exception-avmime2 value
[video/quicktime-inappropriate]
```

2. Configure a URL pattern list (whitelist) of URLs or addresses that you want to bypass. After you create the URL pattern list, you create a custom URL category list and add the pattern list to it. Configure a URL pattern list custom object by creating the list name and adding values to it as follows.



**NOTE:** Because you use URL pattern lists to create custom URL category lists, you must configure URL pattern list custom objects before you configure custom URL category lists.

```
[edit security utm]
user@host# set custom-objects url-pattern urllist2 value [http://www.example.net
192.168.1.5]
```



**NOTE:** URL pattern wildcard support—The wildcard rule is as follows: `\*\.[]\?*` and you must precede all wildcard URLs with `http://`. You can only use “\*” if it is at the beginning of the URL and is followed by a “.”. You can only use “?” at the end of the URL.

The following wildcard syntax is supported: `http://*.example.net`, `http://www.example.ne?`, `http://www.example.n??`. The following wildcard syntax is not supported: `*example.net`, `www.example.ne?`, `http://*example.net`, `http://*`.

3. Configure a custom URL category list custom object by using the URL pattern list `urllist2` that you created earlier:

```
[edit security utm]
user@host# set custom-objects custom-url-category custurl2 value urllist2
```

## Verification

To verify the configuration, enter the **show security utm custom-objects** command.

### Related Documentation

- [Sophos Antivirus Protection Overview on page 45](#)
- [Sophos Antivirus Configuration Overview on page 48](#)
- [Example: Configuring Sophos Antivirus Feature Profile on page 52](#)
- [Understanding UTM Custom Objects on page 4](#)

## Example: Configuring Sophos Antivirus Feature Profile

---

This example shows you how to configure a Sophos antivirus profile that defines the parameters that will be used for virus scanning.

- [Requirements on page 52](#)
- [Overview on page 52](#)
- [Configuration on page 52](#)
- [Verification on page 57](#)

### Requirements

Before you begin:

- Install a Sophos antivirus license. See [Installation and Upgrade Guide](#).
- Configure custom objects for UTM. See [“Example: Configuring Sophos Antivirus Custom Objects” on page 48](#).

### Overview

The following configuration defines Sophos as the antivirus engine and sets parameters, such as the data file update interval, notification options for administrators, fallback options, and file size limits.

### Configuration

#### GUI Step-by-Step Procedure



**NOTE:** The following example shows you how to create a custom Sophos profile. If you want to use the Juniper Networks preconfigured profile, use the profile named `junos-sophos-av-defaults` in your UTM policy. See [“Example: Configuring Sophos Antivirus UTM Policies” on page 58](#).

1. Select and configure the engine type. Because you are configuring Sophos antivirus, you configure `sophos-engine`:
  - a. Click the **Configure** tab from the taskbar, and then select **Security>UTM>Anti-Virus**.
  - b. Click the **Global Options** tab and then click **Sophos**.
  - c. Click **OK** and commit your changes.
2. Return to the antivirus Global Options screen as you did in step 1, and set the following parameters:
  - a. In the MIME whitelist list, select **exception-avmime2**.
  - b. In the URL whitelist list, select **custurl2**.
  - c. In the Pattern update interval (sec) box, type **2880**.

- d. In the box, type the e-mail address that will receive SophosAdmin e-mail data file update notifications. For example - admin@ example.net.
  - e. In the Custom message subject box, type **Sophos Data File Updated**.
  - f. Click **OK** to check your configuration and save it as a candidate configuration.
3. Configure a profile for the sophos-engine and set parameters.
    - a. Click the **Configure** tab from the taskbar and then select **Security>UTM>Anti-Virus**. Click **Add**.
    - b. In the Add profile box, click the **Main** tab.
    - c. In the Profile name box, type **sophos-profl**.
    - d. In the Trickling timeout box, type **180**.



**WARNING:** When enabling the trickling option, it is important to understand that trickling might send part of the file to the client during the antivirus scan. It is possible that some of the content could be received by the client and the client might become infected before the file is fully scanned.

- e. URI checking is on by default. To turn it off, clear **yes** in the URI check box.
  - f. In the Content size Limit box, type **20000**.
  - g. In the Scan engine timeout box, type **1800**.
4. Configure fallback settings by clicking the **Fallback settings** tab. In this example, all fallback options are set to log and permit. Click **Log and permit** for the following items: Default action, Content size, Engine not ready, Timeout, Out of resource, Too many requests.
  5. Configure notification options by clicking the **Notification options** tab. You can configure notifications for both fallback blocking and fallback nonblocking actions and for virus detection.

To configure notifications for Fallback settings:

- a. For Notification type, click **Protocol**.
- b. For Notify mail sender, click **yes**.

- c. In the Custom message box, type **Fallback block action occurred**.
- d. In the Custom message subject box, type **\*\*\*Antivirus fallback Alert\*\*\***.
6. To configure notification options for virus detection, click the **Notification options cont...** tab.
  - a. For the Notification type option button, select **Protocol**.
  - b. For the Notify mail sender option button, select **yes**.
  - c. In the Custom message box, type **Virus has been detected**.
  - d. In the Custom message subject box, type **\*\*\*Virus detected\*\*\***.
7. Click **OK** to check your configuration and save it as a candidate configuration.
8. If you are done configuring the device, click **Actions>Commit**.

#### Step-by-Step Procedure

To configure the Sophos antivirus feature profile using the CLI:



**NOTE:** The following example shows you how to create a custom Sophos profile. If you want to use the Juniper Networks preconfigured profile, use the profile named `junos-sophos-av-defaults` in your UTM policy. See [“Example: Configuring Sophos Antivirus UTM Policies” on page 58](#).

1. Select and configure the engine type. Because you are configuring Sophos antivirus, you configure `sophos-engine`.
 

```
[edit]
user@host# set security utm feature-profile anti-virus type sophos-engine
```
2. Commit the configuration.
3. Select a time interval for updating the data files. The default antivirus pattern-update interval is 1440 minutes (every 24 hours). You can choose to leave this default, or you can change it. You can also force a manual update, if needed. To change the default from every 24 hours to every 48 hours:
 

```
[edit security utm feature-profile anti-virus]
user@host# set sophos-engine pattern-update interval 2880
```
4. Configure the network device with the proxy server details, to download the pattern update from a remote server:
 

```
[edit security utm feature-profile anti-virus]
user@host# set sophos-engine pattern-update proxy
```
5. In most circumstances, you will not need to change the URL to update the pattern database. If you do need to change this option, use the following command:
 

```
[edit security utm feature-profile anti-virus]
user@host# set sophos-engine pattern-update url
http://www.example.net/test-download
```

6. You can configure the device to notify a specified administrator when data files are updated. This is an e-mail notification with a custom message and a custom subject line.

```
[edit security utm feature-profile anti-virus]
user@host# set sophos-engine pattern-update email-notify admin-email
admin@example.net custom-message "Sophos antivirus data file was updated"
custom-message-subject "AV data file updated"
```

7. Configure a list of fallback options as block, log and permit, or permit. The default setting is log-and-permit. You can use the default settings, or you can change them.

Configure the content size action. In this example, if the content size is exceeded, the action taken is block.

First create the profile named sophos-profl.

```
[edit security utm feature-profile anti-virus]
user@host# edit sophos-engine profile sophos-profl
```

Configure the content size fallback-option to block.

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-profl]
user@host# set fallback-options content-size block
```

Configure the default fallback option to log-and-permit.

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-profl]
user@host# set fallback-options default log-and-permit
```

Configure log-and-permit if the antivirus engine is not ready.

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-profl]
user@host# set fallback-options engine-not-ready log-and-permit
```

Configure log-and-permit if the device is out of resources.

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-profl]
user@host# set fallback-options out-of-resources log-and-permit
```

Configure log-and-permit if a virus scan timeout occurs.

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-profl]
user@host# set fallback-options timeout log-and-permit
```

Configure log-and-permit if there are too many requests for the virus engine to handle.

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-profl]
user@host# set fallback-options too-many-requests log-and-permit
```

8. Configure notification options. You can configure notifications for fallback blocking, fallback nonblocking actions, and virus detection.

In this step, configure a custom message for the fallback blocking action and send a notification for protocol-only actions to the administrator and the sender.

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-profl]
user@host# set notification-options fallback-block custom-message ***Fallback
block action occurred*** custom-message-subject Antivirus Fallback Alert
notify-mail-sender type protocol-only allow email administrator-email
admin@example.net
```

9. Configure a notification for protocol-only virus detection, and send a notification.

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-prof1]
user@host# set notification-options virus-detection type protocol-only
               notify-mail-sender custom-message-subject ***Virus detected***
               custom-message Virus has been detected
```

10. Configure content size parameters.



**NOTE:** When you configure the content-size value, keep in mind that in certain cases, content size is available in the protocol headers, so the max-content-size fallback is applied before a scan request is sent. However, in many cases, content size is not provided in the protocol headers. In these cases, the TCP payload is sent to the antivirus scanner and accumulates until the end of the payload. If the accumulated payload exceeds the maximum content size value, then max-content-size fallback is applied. The default fallback action is log and permit, so you may want to change this option to block, in which case such a packet is dropped and a block message is sent to the client.

In this example, if the content size exceeds 20 MB, the packet is dropped.

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-prof1]
user@host# set scan-options content-size-limit 20000
```

11. URI checking is on by default. To turn off URI checking:

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-prof1]
user@host# set scan-options no-uri-check
```

12. Configure the timeout setting for the scanning operation to 1800 seconds.

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-prof1]
user@host# set scan-options timeout 1800
```

13. The Sophos Extensible List servers contain the virus and malware database for scanning operations. Set the response timeout for these servers to 3 seconds (the default is 2 seconds).

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-prof1]
user@host# set scan-options sxl-timeout 3
```

14. Configure the Sophos Extensible List server retry option to 2 retries (the default is 1).

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-prof1]
user@host# set scan-options sxl-retry 2
```

15. Configure the trickling setting to 180 seconds. If you use trickling, you can also set timeout parameters. Trickling applies only to HTTP. HTTP trickling is a mechanism used to prevent the HTTP client or server from timing out during a file transfer or during antivirus scanning.



**WARNING:** When you enable the trickling option, keep in mind that trickling might send part of a file to the client during its antivirus scan. It is therefore possible that some of the content could be received by the client before the file has been fully scanned.

```
[edit security utm feature-profile anti-virus]
user@host# set sophos-engine profile sophos-prof1 trickling timeout 180
```

16. Configure the antivirus module to use MIME bypass lists and exception lists. You can use your own custom object lists, or you can use the default list that ships with the device called junos-default-bypass-mime. In this example, you use the lists that you set up earlier.

```
[edit security utm feature-profile anti-virus]
user@host# set mime-whitelist list avmime2
[edit security utm feature-profile anti-virus]
user@host# set mime-whitelist list exception-avmime2
```

17. Configure the antivirus module to use URL bypass lists. If you are using a URL whitelist, this is a custom URL category you have previously configured as a custom object. URL whitelists are valid only for HTTP traffic. In this example you use the lists that you set up earlier.

```
[edit security utm feature-profile anti-virus]
user@host# set url-whitelist custurl2
```

## Verification

### Obtaining Information About the Current Antivirus Status

**Action** From operational mode, enter the **show security utm anti-virus status** command to view the antivirus status.

```
user@host>show security utm anti-virus status
```

- Meaning**
- Antivirus key expire date—The license key expiration date.
  - Update server—URL for the data file update server.
    - Interval—The time period, in minutes, when the device will update the data file from the update server.
    - Pattern update status—When the data file will be updated next, displayed in minutes.
    - Last result—Result of the last update. If you already have the latest version, this will display **already have latest database**.
  - Antivirus signature version—Version of the current data file.
  - Scan engine type—The antivirus engine type that is currently running.
  - Scan engine information—Result of the last action that occurred with the current scan engine.

- Related Documentation**
- [Sophos Antivirus Protection Overview on page 45](#)
  - [Sophos Antivirus Configuration Overview on page 48](#)

---

## Example: Configuring Sophos Antivirus UTM Policies

This example shows how to create a UTM policy for Sophos antivirus.

- [Requirements on page 58](#)
- [Overview on page 58](#)
- [Configuration on page 58](#)
- [Verification on page 59](#)

### Requirements

Before you create the UTM policy, create custom objects and the Sophos feature profile.

1. Configure UTM custom objects and MIME lists. See [“Example: Configuring Sophos Antivirus Custom Objects” on page 48](#).
2. Configure the Sophos antivirus feature profile. See [“Example: Configuring Sophos Antivirus Feature Profile” on page 52](#).

### Overview

After you have created an antivirus feature profile, you configure a UTM policy for an antivirus scanning protocol and attach this policy to a feature profile. In this example, HTTP will be scanned for viruses, as indicated by the **http-profile** statement. You can scan other protocols as well by creating different profiles or adding other protocols to the profile, such as: **imap-profile**, **pop3-profile**, and **smtp-profile**.

### Configuration

#### GUI Step-by-Step Procedure

To configure a UTM policy for Sophos antivirus:

1. Click the **Configure** tab from the taskbar, and then select **Security>Policy>UTM Policies**. Then click **Add**.
2. Click the **Main** tab. In the Policy name box, type **utmp3**.
3. Click the **Anti-Virus profiles** tab. In the HTTP profile list, select **sophos-profl**.
4. Click **OK** to check your configuration and save it as a candidate configuration.
5. If you are done configuring the device, select **Actions>Commit**.

#### Step-by-Step Procedure

To configure a UTM policy for Sophos antivirus:

1. Go to the edit security utm hierarchy.  
  
[edit]  
user@host# edit security utm

2. Create the UTM policy utmp3 and attach it to the http-profile sophos-profl.

```
[edit security utm]
user@host# set utm-policy utmp3 anti-virus http-profile sophos-profl
```



**NOTE:** You can use the default Sophos feature profile settings by replacing `sophos-profl` in the above statement with `junos-sophos-av-defaults`.

## Verification

To verify the configuration, enter the **show security utm utm-policy utmp3** command.

### Related Documentation

- [Sophos Antivirus Protection Overview on page 45](#)
- [Sophos Antivirus Configuration Overview on page 48](#)
- [Example: Configuring Sophos Antivirus Feature Profile on page 52](#)

## Example: Configuring Sophos Antivirus Firewall Security Policies

This example shows how to create a security policy for Sophos antivirus.

- [Requirements on page 59](#)
- [Overview on page 59](#)
- [Configuration on page 60](#)
- [Verification on page 61](#)

## Requirements

Before you create the security policy, create custom objects, the Sophos feature profile, and the UTM policy.

1. Configure UTM custom objects and MIME lists. See [“Example: Configuring Sophos Antivirus Custom Objects” on page 48](#).
2. Configure the Sophos antivirus feature profile. See [“Example: Configuring Sophos Antivirus Feature Profile” on page 52](#).
3. Configure a UTM policy. See [“Example: Configuring Sophos Antivirus UTM Policies” on page 58](#).

## Overview

Create a firewall security policy that will cause traffic from the untrust zone to the trust zone to be scanned by Sophos antivirus using the feature profile settings defined in [“Example: Configuring Sophos Antivirus Feature Profile” on page 52](#). Because the match application configuration is set to any, all application types will be scanned.

## Configuration

### GUI Step-by-Step Procedure

To configure a security policy for Sophos antivirus:

1. Configure the untrust to trust policy to match any source address or destination address, and select the applications to be scanned to **any**.
  - a. Click the **Configure** tab from the taskbar, and then select **Security>Policy>FW Policies**. Then select **Add**.
  - b. In the Policy Name box, type **p3**.
  - c. In the Policy Action box, select **permit**.
  - d. In the From Zone list, select **untrust**.
  - e. In the To Zone list, select **trust**.
  - f. In the Source Address and Destination Address boxes, make sure that Matched is set to **any**.
  - g. In the Applications boxes, select **any** from the Application/Sets list, and move it to the Matched list.
2. Attach the UTM policy named utmp3 to the firewall security policy. This will cause matched traffic to be scanned by the Sophos antivirus feature.
  - a. From the Edit Policy box, click the **Application Services** tab.
  - b. In the UTM Policy list, select **utmp3**.
3. Click **OK** to check your configuration and save it as a candidate configuration.
4. If you are done configuring the device, select **Actions>Commit**.

### Step-by-Step Procedure

To configure a security policy for Sophos antivirus:

1. Configure the untrust to trust policy to match any source-address.

```
[edit security]
user@host# set policies from-zone untrust to-zone trust policy p3 match
source-address any
```
2. Configure the untrust to trust policy to match any destination-address.

```
[edit security]
user@host# set policies from-zone untrust to-zone trust policy p3 match
destination-address any
```
3. Configure the untrust to trust policy to match any application type.

```
[edit security]
user@host# set policies from-zone untrust to-zone trust policy p3 match application
any
```
4. Attach the UTM policy named utmp3 to the firewall security policy. This will cause matched traffic to be scanned by the Sophos antivirus feature.

```
[edit security]
user@host# set policies from-zone untrust to-zone trust policy p3 then permit
application-services utm-policy utmp3
```

## Verification

To verify the configuration, enter the **show security policies** command.

### Related Documentation

- [Sophos Antivirus Protection Overview on page 45](#)
- [Sophos Antivirus Configuration Overview on page 48](#)
- [Example: Configuring Sophos Antivirus Feature Profile on page 52](#)

## Example: Configuring Sophos Antivirus Scanner with SSL Forward Proxy

This example shows how to configure Sophos antivirus over SSL forward proxy to support HTTPS traffic passing through SRX Series devices.

- [Requirements on page 61](#)
- [Overview on page 61](#)
- [Configuration on page 61](#)
- [Verification on page 64](#)

## Requirements

Before you begin, understand Sophos antivirus features. See “[Sophos Antivirus Features](#)” on page 46.

## Overview

In this example, you configure Sophos antivirus over SSL forward proxy to support HTTPS traffic. You load the PKI certificate, generate a self-signed CA certificate, configure a trusted CA list, configure an SSL proxy profile using the root certificate, and enable SSL forward proxy. To configure UTM over SSL forward proxy, first match the source/destination/application, set up the SSL proxy service, and perform scanning to determine whether to block or permit the requests.

## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **edit** hierarchy level, and then enter **commit** from configuration mode.

```
request security pki generate-key-pair certificate-id ssl-inspect-ca size 2048 type rsa
request security pki local-certificate generate-self-signed certificate-id ssl-inspect-ca
domain-name www.example.net subject
"CN=www.example.net,OU=IT,O=example,L=Sunnyvale,ST=CA,C=US" email
security-admin@example.net
set security pki ca-profile trusted-ca-example ca-identity trusted-ca-example
```

```
request security pki ca-certificate load ca-profile trusted-ca-example filename
trusted-ca-example.crt
set services ssl proxy profile ssl-inspect-profile root-ca ssl-inspect-ca
set services ssl proxy profile ssl-inspect-profile trusted-ca trusted-ca-example
set security policies from-zone untrust to-zone trust policy 1 then permit
application-services ssl-proxy profile-name ssl-inspect-profile
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration* in the *CLI User Guide*.

To configure Sophos Antivirus over SSL forward proxy:

1. Generate a self-signed CA certificate on the device.

```
user@host> request security pki generate-key-pair certificate-id ssl-inspect-ca size
2048 type rsa
user@host> request security pki local-certificate generate-self-signed certificate-id
ssl-inspect-ca domain-name www.example.net subject
"CN=www.example.net,OU=IT,O=example,L=Sunnyvale,ST=CA,C=US" email
security-admin@example.net
```

2. Configure a trusted CA list.

```
[edit]
user@host# set security pki ca-profile trusted-ca-example ca-identity
trusted-ca-example

user@host> request security pki ca-certificate load ca-profile trusted-ca-example
filename trusted-ca-example.crt
```

3. Configure an SSL proxy profile using a root certificate.

```
[edit]
user@host# set services ssl proxy profile ssl-inspect-profile root-ca ssl-inspect-ca
user@host# set services ssl proxy profile ssl-inspect-profile trusted-ca
trusted-ca-example
```

4. Enable SSL forward proxy.

```
[edit]
user@host# set security policies from-zone untrust to-zone trust policy 1 then permit
application-services ssl-proxy profile-name ssl-inspect-profile
```

---

## Results

From configuration mode, confirm your configuration by entering the **show security utm**, **show services**, and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security utm
  traceoptions {
    flag all;
  }
  application-proxy {
    traceoptions {
```

```

        flag sophos-anti-virus;
    }
}
feature-profile {
    anti-virus {
        type sophos-engine;
        traceoptions {
            flag all;
        }
    }
    sophos-engine {
        sxl-timeout 4;
        profile profile1 {
            fallback-options {
                default log-and-permit;
                content-size log-and-permit;
                engine-not-ready log-and-permit;
                timeout log-and-permit;
                out-of-resources log-and-permit;
                too-many-requests log-and-permit;
            }
            scan-options {
                uri-check;
            }
            notification-options {
                virus-detection {
                    type message;
                }
                fallback-block {
                    type message;
                }
            }
        }
    }
}
}
}
}
utm-policy policy1 {
    anti-virus {
        http-profile profile1;
    }
}
[edit]
user@host# show services
ssl {
    traceoptions {
        file ssl_trace size 1g;
        flag all;
    }
    proxy {
        profile ssl-p {
            root-ca haojue;
            actions {
                ignore-server-auth-failure;
            }
        }
    }
}
}

```

```
[edit]
user@host# show security policies
  from-zone trust to-zone untrust {
    policy trust_2_untrust {
      match {
        source-address any;
        destination-address any;
        application [ junos-http junos-https ];
      }
      then {
        permit {
          application-services {
            ssl-proxy {
              profile-name ssl-p;
            }
          }
          utm-policy policy1;
        }
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying the Security PKI Local Certificate on page 64](#)
- [Verifying UTM Antivirus Statistics on page 65](#)
- [Verifying UTM Antivirus Statistics Details on page 65](#)
- [Verifying UTM Antivirus Status on page 66](#)

---

### Verifying the Security PKI Local Certificate

**Purpose** Verify the security PKI local certificate.

**Action** From configuration mode, enter the **show security pki local-certificate** command.

```
user@host# show security pki local-certificate
Certificate identifier: SELF-SIGNED
  Issued to: abc, Issued by: CN = abc
  Validity:
    Not before: 02-20-2015 00:49 UTC
    Not after: 02-19-2020 00:49 UTC
  Public key algorithm: rsaEncryption(2048 bits)

Certificate identifier: ssl-inspect-ca
  Issued to: www.example.net, Issued by: CN = www.example.net, OU = IT, O =
example, L = Sunnyvale, ST = CA, C = US
  Validity:
    Not before: 01-28-2016 22:28 UTC
    Not after: 01-26-2021 22:28 UTC
  Public key algorithm: rsaEncryption(2048 bits)
```

**Meaning** The sample output confirms that the PKI local certificate ssl-inspect-ca is configured.

### Verifying UTM Antivirus Statistics

**Purpose** Verify UTM antivirus statistics.

**Action** From operational mode, enter the **show security utm anti-virus statistics** command.

```
user@host> show security utm anti-virus statistics
MIME-whitelist passed:          0
URL-whitelist passed:           0

Scan Requests:
  Total      Clean      Thread found  Fall back  Abort
    0         0         0             0         0

Fall back:
  log-and-permit  block  permit
Engine not ready: 0       0       0
Out of resources: 0       0       0
Timeout:          0       0       0
Maxmium content size: 0     0     0
Too many requests: 0     0     0
Others            0     0     0
```

**Meaning** The sample output shows the list of UTM antivirus statistics.

### Verifying UTM Antivirus Statistics Details

**Purpose** Verify UTM antivirus statistics details.

**Action** From operational mode, enter the **show security utm anti-virus statistics details** command.

```
user@host> show security utm anti-virus statistics details
HTTP
MIME-whitelist passed:          0
URL-whitelist passed:           0

URI request:
  Total  Clean  Threat-found  Need-further-inspection  Abort
    10     1         1             8             0

File request:
  Total  Clean  Threat-found  Fallback  Abort
    8     6         1         1         0

Fall back:
  log-and-permit  block  permit
Engine not ready: 0       0       0
Out of resources: 0       0       0
Timeout:          0       0       0
Maxmium content size: 1     0     0
Too many requests: 0     0     0
Others            0     0     0

FTP
Scan request:
  Total  Clean  Threat-found  Fallback  Abort
    10     8         1         1         0
```

Fall back:	log-and-permit	block	permit
Engine not ready:	0	0	0
Out of resources:	0	0	0
Timeout:	0	0	0
Maxmium content size:	1	0	0
Too many requests:	0	0	0
Others	0	0	0

## SMTP

Scan request:				
Total	Clean	Threat-found	Fallback	Abort
10	8	1	1	0

Fall back:	log-and-permit	block	permit
Engine not ready:	0	0	0
Out of resources:	0	0	0
Timeout:	0	0	0
Maxmium content size:	1	0	0
Too many requests:	0	0	0
Others	0	0	0

## POP3

Scan request:				
Total	Clean	Threat-found	Fallback	Abort
10	8	1	1	0

Fall back:	log-and-permit	block	permit
Engine not ready:	0	0	0
Out of resources:	0	0	0
Timeout:	0	0	0
Maxmium content size:	1	0	0
Too many requests:	0	0	0
Others	0	0	0

## IMAP

Scan request:				
Total	Clean	Threat-found	Fallback	Abort
10	8	1	1	0

Fall back:	log-and-permit	block	permit
Engine not ready:	0	0	0
Out of resources:	0	0	0
Timeout:	0	0	0
Maxmium content size:	1	0	0
Too many requests:	0	0	0
Others	0	0	0

**Meaning** The sample output shows the list of antivirus statistics details.

### Verifying UTM Antivirus Status

**Purpose** Verify UTM antivirus status.

**Action** From operational mode, enter the **show security utm anti-virus status** command to view the antivirus status.

```
user@host> show security utm anti-virus status
```

```

Anti-virus Key Expiry Date: 07/01/2010 00:00:00
  Update server: http://update.juniper-updates.net//
    Interval: 1440 minutes
    Auto update status: next update in 1440 minutes
    Last result: No error
Anti-virus data file info:
  Version:
Scan engine information:
  Last action result: No error(0x00000000)
  Engine type: sophos-engine

```

- Meaning**
- Antivirus key expire date—The license key expiration date.
  - Update server—URL for the data file update server.
  - Interval—The time period, in minutes, when the device updates the data file from the update server.
  - Auto update status—Displays the next automatic update of the data file in minutes.
  - Last result—Result of the last database update.
  - Antivirus signature version—Version of the current antivirus signature data file.
  - Scan engine type—The antivirus scan engine type that is currently running.
  - Scan engine information—Result of the last action that occurred with the current scan engine.

- Related Documentation**
- [Sophos Antivirus Features on page 46](#)

## Managing Sophos Antivirus Data Files

Before you begin:

- Install a Sophos antivirus license. See the *Installation and Upgrade Guide*.
- Configure Sophos as the antivirus feature for the device. See “[Example: Configuring Sophos Antivirus Feature Profile](#)” on page 52. To set the antivirus engine type, you run the **set security utm feature-profile anti-virus type sophos-engine** statement.

In this example, you configure the security device to update the data files automatically every 4320 minutes (every 3 days). The default data file update interval is 1440 minutes (every 24 hours).

To automatically update Sophos data files:

```

[edit security utm feature-profile anti-virus]
user@host# set sophos-engine pattern-update interval 4320

```



**NOTE:** The following commands are performed from CLI operational mode.

To manually update data files:

```
user@host> request security utm anti-virus sophos-engine pattern-update
```

To manually reload data files:

```
user@host> request security utm anti-virus sophos-engine pattern-reload
```

To manually delete data files:

```
user@host> request security utm anti-virus sophos-engine pattern-delete
```

To check the status of antivirus, which also shows the data files version:

```
user@host> show security utm anti-virus status
```

To check the status of the proxy server:

```
user@host> show security utm anti-virus status
```

**Related  
Documentation**

- [Sophos Antivirus Protection Overview on page 45](#)
- [Understanding Sophos Antivirus Data File Update on page 47](#)
- [Sophos Antivirus Configuration Overview on page 48](#)

## PART 4

# Configuring and Monitoring Content Filtering

- [Configuring Content Filtering on page 71](#)



## CHAPTER 10

# Configuring Content Filtering

- [Content Filtering Overview on page 71](#)
- [Understanding Content Filtering Protocol Support on page 72](#)
- [Specifying Content Filtering Protocols \(CLI Procedure\) on page 73](#)
- [Content Filtering Configuration Overview on page 74](#)
- [Example: Configuring Content Filtering Custom Objects on page 75](#)
- [Example: Configuring Content Filtering Feature Profiles on page 77](#)
- [Example: Configuring Content Filtering UTM Policies on page 80](#)
- [Example: Attaching Content Filtering UTM Policies to Security Policies on page 82](#)
- [Monitoring Content Filtering Configurations on page 84](#)

## Content Filtering Overview

---

Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, and protocol command. The content filter controls file transfers across the gateway by checking traffic against configured filter lists.

The content filter module evaluates traffic before all other UTM modules, except Web Filtering. Therefore, if traffic meets criteria configured in the content-filter, the content-filter acts first upon this traffic.

You can configure the following types of content filters:

- **MIME Pattern Filter** — MIME patterns are used to identify the type of traffic in HTTP and MAIL protocols. There are two lists of MIME patterns that are used by the content filter to determine the action to be taken. The block MIME list contains a list of MIME type traffic that is to be blocked by the content filter. The MIME exception list contains MIME patterns that are not to be blocked by the content filter and are generally subsets of items on the block list. Note that the exception list has a higher priority than the block list. If you have MIME entries that appear on both lists, those MIME types are not blocked by the content filter because the exception list takes priority. Therefore, when adding items to the exception list, it is to your advantage to be specific.
- **Block Extension List** — Because the name of a file is available during file transfers, using file extensions is a highly practical way to block or allow file transfers. The content filter list contains a list of file extensions to be blocked. All protocols support the use of the block extension list.

- Protocol Command Block and Permit Lists — Different protocols use different commands to communicate between servers and clients. By blocking or allowing certain commands, traffic can be controlled on the protocol command level.

The block and permit command lists are intended to be used in combination, with the permit list acting as an exception list to the block list.



**NOTE:** If a protocol command appears on both the permit list and the block list, that command is permitted.

Because not all harmful files or components can be controlled by the MIME type or by the file extension, you can also use the content filter module to block ActiveX, Java Applets, and other types of content. The following types of content blocking are supported only for HTTP:

- Block ActiveX
- Block Java applets
- Block cookies
- Block EXE files
- Block ZIP files

**Related  
Documentation**

- [Unified Threat Management Overview on page 3](#)
- [Understanding Content Filtering Protocol Support on page 72](#)
- [Content Filtering Configuration Overview on page 74](#)
- [Monitoring Content Filtering Configurations on page 84](#)

---

## Understanding Content Filtering Protocol Support

Each supported protocol may implement available content filters differently. Not all filtering capabilities are supported for each protocol.

This topic contains the following sections:

- [HTTP Support on page 72](#)
- [FTP Support on page 73](#)
- [E-Mail Support on page 73](#)

### HTTP Support

The HTTP protocol supports all content filtering features. With HTTP, the content filter remains in the gateway, checking every request and response between the HTTP client and server.

If an HTTP request is dropped due to content filtering, the client receives a response such as:

```
<custom drop message/user-configured drop
message>.<src_port><dst_ip>:<dst_port>Download request was dropped due to
<reason>
```

Therefore, a message may appear as follows:

```
Juniper Networks Firewall Content Filtering blocked request. 5.5.5.1:80->4.4.4.1:55247
Download request was dropped due to file extension block list
```

## FTP Support

The FTP protocol does not support all content filtering features. It supports only the following: Block Extension List and Protocol Command Block List.

When content filtering blocks an FTP request, the following response is sent through the control channel:

```
550 <src_ip>:<src_port>-<dst_ip>:<dst_port><custom drop message/user-configured
drop message> for Content Filtering file extension block list.>
```

Therefore, a message may appear as follows:

```
550 5.5.5.1:21->4.4.4.1:45237 Requested action not taken and the request is dropped for
Content Filtering file extension block list
```

## E-Mail Support

E-mail protocols (SMTP, IMAP, POP3) have limited content filtering support for the following features: Block Extension List, Protocol Command Block List, and MIME Pattern Filtering. Support is limited for e-mail protocols for the following reasons:

- The content filter scans only one level of an e-mail header. Therefore recursive e-mail headers and encrypted attachments are not scanned.
- If an entire e-mail is MIME encoded, the content filter can only scan for the MIME type.
- If any part of an e-mail is blocked due to content filtering, the original e-mail is dropped and replaced by a text file with an explanation for why the e-mail was blocked.

### Related Documentation

- [Unified Threat Management Overview on page 3](#)
- [Specifying Content Filtering Protocols \(CLI Procedure\) on page 73](#)
- [Content Filtering Configuration Overview on page 74](#)
- [Monitoring Content Filtering Configurations on page 84](#)

## Specifying Content Filtering Protocols (CLI Procedure)

To configure content filtering protocols, use the following CLI configuration statements:

```
content-filtering {
  profile name {
    permit-command cmd-list
```

```
    block-command cmd-list
    block-extension file-ext-list
    block-mime {
        list mime-list
        exception ex-mime-list
    }
    block-content-type {
        activex
        java-applet
        exe
        zip
        http-cookie
    }
    notification-options {
        type { message }
        notify-mail-sender
        custom-message msg
    }
}
traceoptions {
    flag {
        all
        basic
        detail
    }
}
}
```

**Related Documentation**

- [Unified Threat Management Overview on page 3](#)
- [Example: Configuring Content Filtering Custom Objects on page 75](#)
- [Example: Configuring Content Filtering Feature Profiles on page 77](#)
- [Example: Configuring Content Filtering UTM Policies on page 80](#)

---

## Content Filtering Configuration Overview

A content security filter blocks or allows certain type of traffic base on the mime type, file extension, protocol commands and embedded object type. The content filter controls file transfers across the gateway by checking traffic against configured filter lists. The content filtering module evaluates traffic before all other UTM modules, if traffic meets the criteria configured in the content filter, the content filter acts first upon this traffic. The following procedure lists the recommended order in which you should configure content filters:

1. Configure UTM custom objects for the feature. See [“Example: Configuring Content Filtering Custom Objects” on page 75](#).
2. Configure the main feature parameters using feature profiles. See [“Example: Configuring Content Filtering Feature Profiles” on page 77](#).
3. Configure a UTM policy for each protocol and attach this policy to a profile. See [“Example: Configuring Content Filtering UTM Policies” on page 80](#).

4. Attach the UTM policy to a security policy. See [“Example: Attaching Content Filtering UTM Policies to Security Policies” on page 82.](#)

**Related  
Documentation**

- [Unified Threat Management Overview on page 3](#)

## Example: Configuring Content Filtering Custom Objects

This example shows how to configure content filtering custom objects.

- [Requirements on page 75](#)
- [Overview on page 75](#)
- [Configuration on page 75](#)
- [Verification on page 77](#)

### Requirements

Before you begin:

1. Decide on the type of content filter you require. See [“Content Filtering Overview” on page 71.](#)
2. Understand the order in which content filtering parameters are configured. See [“Content Filtering Configuration Overview” on page 74.](#)

### Overview

In this example, you define custom objects that are used to create content filtering profiles. You perform the following tasks to define custom objects:

1. Create two protocol command lists called ftpprotocom1 and ftpprotocom2, and add user, pass, port, and type commands to it.
2. Create a filename extension list called extlist2, and add the .zip, .js, and .vbs extensions to it.
3. Define block-mime list call cfmime1 and add patterns to the list.

### Configuration

**CLI Quick  
Configuration**

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm custom-objects protocol-command ftpprotocom1 value [user pass port type]
set security utm custom-objects protocol-command ftpprotocom2 value [user pass port type]
set security utm custom-objects filename-extension extlist2 value [zip js vbs]
set security utm custom-objects mime-pattern cfmime1 value [video/quicktime image/x-portable-anymap x-world/x-vmrl]
```

```
set security utm custom-objects mime-pattern ex-cfmime1 value
[video/quicktime-inappropriate]
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration* in the *CLI User Guide*.

To configure content filtering custom objects:

1. Create two protocol command lists.

```
[edit security utm]
user@host# set custom-objects protocol-command ftpprotocom1
[edit security utm]
user@host# set custom-objects protocol-command ftpprotocom2
```

2. Add protocol commands to the list.

```
[edit security utm]
user@host# set custom-objects protocol-command ftpprotocom1 value [user pass
port type]
[edit security utm]
user@host# set custom-objects protocol-command ftpprotocom2 value [user pass
port type]
```

3. Create a filename extension list.

```
[edit security utm]
user@host# set custom-objects filename-extension extlist2
```

4. Add extensions to the list.

```
[edit security utm]
user@host# set custom-objects filename-extension extlist2 value [zip js vbs]
```

5. Create antivirus scanning lists.

```
[edit security utm]
user@host# set custom-objects mime-pattern cfmime1
user@host# set custom-objects mime-pattern ex-cfmime1
```

6. Add patterns to the lists.

```
[edit security utm]
user@host# set custom-objects mime-pattern cfmime1 value [video/quicktime
image/x-portable-anymap x-world/x-vrml]
user@host# set custom-objects mime-pattern ex-cfmime1 value
[video/quicktime-inappropriate]
```

**Results** From configuration mode, confirm your configuration by entering the **show security utm** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost#show security utm
custom-objects {
  mime-pattern {
    cfmime1 {
      value [ video/quicktime image/x-portable-anymap x-world/x-vrml ];
```

```

    }
    ex-cfmime1 {
        value video/quicktime-inappropriate;
    }
}
filename-extension {
    extlist2 {
        value [ zip js vbs ];
    }
}
protocol-command {
    ftpprotocom1 {
        value [ user pass port type ];
    }
}
protocol-command {
    ftpprotocom2 {
        value [ user pass port type ];
    }
}
}

```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### Verifying Content Filtering Custom Objects

<b>Purpose</b>	Verify the content filtering custom objects.
<b>Action</b>	From operational mode, enter the <b>show configuration security utm</b> command.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Unified Threat Management Overview on page 3</a></li> <li>• <a href="#">Content Filtering Overview on page 71</a></li> <li>• <a href="#">Content Filtering Configuration Overview on page 74</a></li> <li>• <a href="#">Example: Configuring Content Filtering Feature Profiles on page 77</a></li> <li>• <a href="#">Example: Configuring Content Filtering UTM Policies on page 80</a></li> <li>• <a href="#">Example: Attaching Content Filtering UTM Policies to Security Policies on page 82</a></li> </ul>

## Example: Configuring Content Filtering Feature Profiles

This example describes how to configure the content filtering feature profiles.

- [Requirements on page 78](#)
- [Overview on page 78](#)
- [Configuration on page 78](#)
- [Verification on page 80](#)

## Requirements

Before you begin:

1. Decide on the type of content filter you require. See [“Content Filtering Overview” on page 71](#).
2. Create custom objects. See [“Content Filtering Configuration Overview” on page 74](#).

## Overview

In this example, you configure a feature profile called `confilter1` and specify the following custom objects to be used for filtering content:

1. Apply the `ftpprotocom1` protocol command list custom object to `confilter1`.
2. Apply blocks to Java applets, executable files, and HTTP cookies.
3. Apply the extension list `extlist2` custom object to `confilter1` for blocking extensions.
4. Apply the MIME pattern list custom objects `cfmime1` and `ex-cfmime1` to the `confilter1` for blocking MIME types.
5. Apply the protocol permit command custom object `ftpprotocom2` to `confilter1`. (The permit protocol command list acts as an exception list for the block protocol command list.)



**NOTE:** Protocol command lists, both permit and block, are created by using the same custom object.

6. Configure a custom message to send a notification.

## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile content-filtering profile confilter1
set security utm feature-profile content-filtering profile confilter1 block-command
  ftpprotocom1
set security utm feature-profile content-filtering profile confilter1 block-content-type
  java-applet exe http-cookie
set security utm feature-profile content-filtering profile confilter1 block-extension extlist2
set security utm feature-profile content-filtering profile confilter1 block-mime list cfmime1
  exception ex-cfmime1
set security utm feature-profile content-filtering profile confilter1 permit-command
  ftpprotocom2
set security utm feature-profile content-filtering profile confilter1 notification-options
  custom-message "the action is not taken" notify-mail-sender type message
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration* in the *CLI User Guide*.

To configure a content filtering feature profiles:

1. Create a content filtering profile.

```
[edit security utm]
user@host# set feature-profile content-filtering profile confilter1
```

2. Apply a protocol command list custom object to the profile.

```
[edit security utm]
user@host# set feature-profile content-filtering profile confilter1 block-command
ftpprotocom1
```

3. Apply blocks to available content.

```
[edit security utm]
user@host# set feature-profile content-filtering profile confilter1 block-content-type
java-applet exe http-cookie
```

4. Apply an extension list custom object to the profile.

```
[edit security utm]
user@host# set feature-profile content-filtering profile confilter1 block-extension
extlist2
```

5. Apply pattern list custom objects to the profile.

```
[edit security utm]
user@host# set feature-profile content-filtering profile confilter1 block-mime list
cfmime1 exception ex-cfmime1
```

6. Apply the protocol permit command custom object to the profile.

```
[edit security utm]
user@host# set feature-profile content-filtering profile confilter1 permit-command
ftpprotocom2
```

7. Configure the notification options.

```
[edit security utm]
user@host# set feature-profile content-filtering profile confilter1m
notification-options custom-message "the action is not taken" notify-mail-sender
type message
```

**Results** From configuration mode, confirm your configuration by entering the **show security utm** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security utm
feature-profile {
  content-filtering {
    profile contentfilter1;
    profile confilter1 {
      permit-command ftpprotocom2;
      block-command ftpprotocom1;
    }
  }
}
```

```
block-extension extlist2;
block-mime {
  list cfmime1;
  exception ex-cfmime1;
}
block-content-type {
  java-applet;
  exe;
  http-cookie;
}
notification-options {
  type message;
  notify-mail-sender;
  custom-message " the action is not taken";
}
}
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

---

### Verifying the Configuration of Content Filtering Feature Profile

**Purpose** Verify the content filtering feature profile.

**Action** From operational mode, enter the **show configuration security utm** command.

**Related Documentation**

- [Unified Threat Management Overview on page 3](#)
- [Content Filtering Overview on page 71](#)
- [Content Filtering Configuration Overview on page 74](#)
- [Example: Configuring Content Filtering Custom Objects on page 75](#)
- [Example: Configuring Content Filtering UTM Policies on page 80](#)
- [Example: Attaching Content Filtering UTM Policies to Security Policies on page 82](#)

---

## Example: Configuring Content Filtering UTM Policies

This example describes how to create a content filtering UTM policy to attach to your feature profile.

- [Requirements on page 81](#)
- [Overview on page 81](#)
- [Configuration on page 81](#)
- [Verification on page 81](#)

## Requirements

Before you begin:

1. Decide on the type of content filter you require. See [“Content Filtering Overview” on page 71](#).
2. Configure UTM custom objects for each feature and define the content-filtering profile. See [“Content Filtering Configuration Overview” on page 74](#).

## Overview

You configure UTM policies to selectively enforce various UTM solutions on network traffic passing through a UTM-enabled device. Through feature profiles you associate custom objects to these policies and specify blocking or permitting certain types of traffic.

In this example, you configure a UTM policy called `utmp4`, and then assign the preconfigured feature profile `confilter1` to this policy.

## Configuration

### Step-by-Step Procedure

To configure a content filtering UTM policy:

You can configure different protocol applications in the UTM policy. The example only shows HTTP and not other protocols. Earlier you configured custom objects for FTP (`ftpprotocom1` and `ftpprotocom2`). Next you should add a content filter policy for FTP, for example:

```
set security utm utm-policy utmp4 content-filtering ftp upload-profile confilter1
```

```
set security utm utm-policy utmp4 content-filtering ftp download-profile confilter1
```

1. Create a UTM policy.  

```
[edit security utm]
user@host# set utm-policy utmp4
```
2. Attach the UTM policy to the profile.  

```
[edit security utm]
user@host# set utm-policy utmp4 content-filtering http-profile contentfilter1
```
3. If you are done configuring the device, commit the configuration.  

```
[edit]
user@host# commit
```

## Verification

To verify the configuration is working properly, enter the `show security utm` command.

### Related Documentation

- [Unified Threat Management Overview on page 3](#)
- [Content Filtering Overview on page 71](#)
- [Content Filtering Configuration Overview on page 74](#)

- [Example: Configuring Content Filtering Custom Objects on page 75](#)
- [Example: Configuring Content Filtering Feature Profiles on page 77](#)
- [Example: Attaching Content Filtering UTM Policies to Security Policies on page 82](#)

---

## Example: Attaching Content Filtering UTM Policies to Security Policies

---

This example shows how to create a security policy and attach the UTM policy to the security policy.

- [Requirements on page 82](#)
- [Overview on page 82](#)
- [Configuration on page 82](#)
- [Verification on page 83](#)

### Requirements

Before you begin:

1. Configure UTM custom objects, define the content filtering profile, and create a UTM policy. See "[Content Filtering Configuration Overview](#)" on page 74.
2. Enable and configure a security policy. See *Example: Configuring a Security Policy to Permit or Deny All Traffic*.

### Overview

By attaching content filtering UTM policies to security policies, you can filter traffic transiting from one security zone to another.

In this example, you create a security policy called p4 and specify that traffic from any source address to any destination address with an HTTP application matches the criteria. You then assign a UTM policy called utmp4 to the security policy p4. This UTM policy applies to any traffic that matches the criteria specified in the security policy p4.

### Configuration

#### CLI Quick Configuration

To quickly attach a content filtering UTM policy to a security policy, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
[edit]
set security policies from-zone trust to-zone untrust policy p4 match source-address any
set security policies from-zone trust to-zone untrust policy p4 match destination-address
  any
set security policies from-zone trust to-zone untrust policy p4 match application
  junos-http
set security from-zone trust to-zone untrust policy p4 then permit application-services
  utm-policy utmp4
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration* in the *CLI User Guide*.

To attach a UTM policy to a security policy:

1. Create a security policy.  

```
[edit]
user@host# edit security policies from-zone trust to-zone untrust policy p4
```
2. Specify the match conditions for the policy.  

```
[edit security policies from-zone trust to-zone untrust policy p4]
user@host# set match source-address any
user@host# set match destination-address any
user@host# set match application junos-http
```
3. Attach the UTM policy to the security policy.  

```
[edit security policies from-zone trust to-zone untrust policy p4]
user@host# set then permit application-services utm-policy utmp4
```

**Results** From configuration mode, confirm your configuration by entering the **show security policies** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
from-zone trust to-zone untrust {
  policy p4 {
    match {
      source-address any;
      destination-address any;
      application junos-http;
    }
    then {
      permit {
        application-services {
          utm-policy utmp4;
        }
      }
    }
  }
}
default-policy {
  permit-all;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### Verifying Attaching Content Filtering UTM Policies to Security Policies

**Purpose** Verify the attachment of the content filtering UTM policy to the security policy.

**Action** From operational mode, enter the **show security policy** command.

- Related Documentation**
- [Unified Threat Management Overview on page 3](#)
  - [Content Filtering Overview on page 71](#)
  - [Content Filtering Configuration Overview on page 74](#)
  - [Example: Configuring Content Filtering Custom Objects on page 75](#)
  - [Example: Configuring Content Filtering Feature Profiles on page 77](#)
  - [Example: Configuring Content Filtering UTM Policies on page 80](#)

---

## Monitoring Content Filtering Configurations

---

**Purpose** View content filtering statistics.

**Action** To view content filtering statistics in the CLI, enter the **user@host > show security utm content-filtering statistics** command.

The content filtering **show statistics** command displays the following information:

```
Base on command list: # Blocked
Base on mime list: # Blocked
Base on extension list: # Blocked
ActiveX plugin: # Blocked
Java applet: # Blocked
EXE files: # Blocked
ZIP files: # Blocked
HTTP cookie: # Blocked
```

To view content filtering statistics using J-Web:

1. Select **Clear Content filtering statistics**Monitor>Security>UTM>Content FilteringMonitor>Security>UTM>Content Filtering.

The following statistics become viewable in the right pane.

```
Base on command list: # Passed # Blocked
Base on mime list: # Passed # Blocked
Base on extension list: # Passed # Blocked
ActiveX plugin: # Passed # Blocked
Java applet: # Passed # Blocked
EXE files: # Passed # Blocked
ZIP files: # Passed # Blocked
HTTP cookie: # Passed # Blocked
```

2. You can click **Clear Content filtering statistics** to clear all current viewable statistics and begin collecting new statistics.

- Related Documentation**
- [Content Filtering Overview](#)
  - [Understanding Content Filtering Protocol Support](#)
  - [Content Filtering Configuration Overview](#)

- [Example: Attaching Content Filtering UTM Policies to Security Policies](#)



## PART 5

# Configuring Web Filtering

- [Configuring Web Filtering on page 89](#)



# Configuring Web Filtering

- [Web Filtering Overview on page 89](#)
- [Enhanced Web Filtering Overview on page 91](#)
- [Understanding Enhanced Web Filtering Process on page 92](#)
- [Example: Configuring Enhanced Web Filtering on page 97](#)
- [Understanding the Quarantine Action for Enhanced Web Filtering on page 105](#)
- [Example: Configuring Site Reputation Action for Enhanced Web Filtering on page 106](#)
- [Understanding Local Web Filtering on page 112](#)
- [Example: Configuring Local Web Filtering on page 114](#)
- [Understanding Redirect Web Filtering on page 120](#)
- [Example: Enhancing Security by Configuring Redirect Web Filtering Using Custom Objects on page 121](#)
- [Monitoring Web Filtering Configurations on page 129](#)

## Web Filtering Overview

---

Web filtering lets you manage Internet usage by preventing access to inappropriate Web content. There are three types of Web filtering solutions:

- **Redirect Web filtering**—The redirect Web filtering solution intercepts HTTP requests and sends them to an external URL filtering server, provided by Websense, to determine whether to block the requests.



**NOTE:** Redirect Web filtering does not require a license.

- **Local Web filtering**—The local Web filtering solution intercepts every HTTP request in a TCP connection. In this case, the decision making is done on the device after it looks up a URL to determine if it is in the whitelist or blacklist based on its user-defined category.



**NOTE:** Local Web filtering does not require a license or a remote category server.

- **Enhanced Web filtering**—The enhanced Web filtering solution intercepts the HTTP and the HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC). The TSC categorizes the URL into one of the 151 or more categories that are predefined and also provides site reputation information. The TSC further returns the URL category and the site reputation information to the device. The device determines if it can permit or block the request based on the information provided by the TSC.

You can bind either Web filtering profiles or antivirus profiles, or both, to a firewall policy. When both are bound to a firewall policy, Web filtering is applied first, then antivirus is applied. If a URL is blocked by Web filtering, the TCP connection is closed and no antivirus scanning is necessary. If a URL is permitted, the content of the transaction is then passed to the antivirus scanning process.



**NOTE:** Web filtering is applied by TCP port number.

---

UTM Web filtering supports HTTPS protocol. UTM Web filtering solution uses the IP address of the HTTPS packet to make blacklist, whitelist, permit, or block decisions.

During a block decision, the UTM Web filtering solution does not generate a block page because the clear text is not available for a HTTPS session. However, the solution terminates the session and sends resets to the client and the server for the blocked HTTPS sessions.

UTM Web filtering configuration for HTTP is also applicable for the HTTPS sessions.



**NOTE:** The `sessions-per-client limit` CLI command, which imposes a session throttle to prevent a malicious user from generating large amounts of traffic simultaneously, does not support Web filtering.

---

**Related  
Documentation**

- [Understanding Redirect Web Filtering on page 120](#)
- [Understanding Enhanced Web Filtering Process on page 92](#)
- [Understanding Local Web Filtering on page 112](#)
- [Monitoring Web Filtering Configurations on page 129](#)
- [web-filtering on page 255](#)

## Enhanced Web Filtering Overview

---

Enhanced Web Filtering (EWF) with Websense is an integrated URL filtering solution. When you enable the solution on the device, it intercepts the HTTP and the HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC). The TSC categorizes the URL into one of the 95 or more categories that are predefined and also provides site reputation information. The TSC further returns the URL category and the site reputation information to the device. The device determines if it can permit or block the request based on the information provided by the TSC.

EWF supports HTTPS traffic by intercepting HTTPS traffic passing through the SRX Series device. The security channel from the SRX Series device is divided as one SSL channel between the client and the SRX Series device and another SSL channel between the SRX Series device and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to the UTM. UTM extracts the URL from the HTTP request message.

Enhanced Web Filtering supports the following HTTP methods:

- GET
- POST
- OPTIONS
- HEAD
- PUT
- DELETE
- TRACE
- CONNECT

### **Related Documentation**

- [Web Filtering Overview on page 89](#)
- [Understanding Local Web Filtering on page 112](#)
- [Understanding Redirect Web Filtering on page 120](#)
- [Understanding Enhanced Web Filtering Process on page 92](#)
- [Example: Configuring Enhanced Web Filtering on page 97](#)

## Understanding Enhanced Web Filtering Process

---

Web filtering enables you to manage Internet access and prevent access to inappropriate Web content. This topic describes how the Enhanced Web Filtering (EWF) feature intercepts, scans, and acts upon HTTP or HTTPS traffic.

1. The device creates TCP socket connections to the Websense ThreatSeeker Cloud (TSC).
2. The device intercepts an HTTP or an HTTPS connection and extracts each URL( in the HTTP request) or IP (in the HTTPS request).
3. The device looks for the URL in the user-configured blacklist or whitelist.



**NOTE:** A blacklist or a whitelist action type is a user-defined category in which all the URLs or IP addresses are always blocked or permitted and optionally logged.

- If the URL is in the user-configured blacklist, the device blocks the URL.
  - If the URL is in the user-configured whitelist, the device permits the URL.
4. The device checks the user-defined categories and blocks or permits the URL based on the user-specified action for the category.
  5. The device looks for the URL in the URL filtering cache.
    - If the URL is not available in the URL filtering cache, the device sends the URL in HTTP format to the TSC with a request for categorization. The device uses one of the connections made available to the TSC to send the request.
    - The TSC responds to the device with the categorization and a reputation score.
  6. The device performs the following actions based on the identified category:
    - If the URL is permitted, the device forwards the HTTP request to the HTTP server.
    - If the URL is blocked, the device sends a deny page to the HTTP client and also sends a reset message to the HTTP server to close the connection
    - If the URL is quarantined, the device sends a redirect response to the HTTP client and the URL is redirected to the HTTP server.
    - If the category is not available, the device permits or blocks the URL based on the configured action for the reputation score.
    - If an action for the site reputation score is not configured, the device permits or blocks the URL based on the default action configured in the Web filtering profile.

## Functional Requirements for Enhanced Web Filtering

- **License key**—Two different valid license keys are required for the EWF. You need to install a new license to upgrade to the EWF solution.



**NOTE:** You can ignore the warning message "requires 'wf\_key\_websense\_ewf' license" because it is generated by routine EWF license validation check.

A grace period of 30 days, consistent with other UTM features, is provided for the EWF feature after the license key expires.



**NOTE:**

When the grace period for the EWF feature has passed (or if the feature has not been installed), Web filtering is disabled, all HTTP requests bypass Web filtering, and any connections to the TSC are disabled. When you install a valid license, the connections to the server are established again.

- A **debug** command provides the following information to each TCP connection available on the device:
  - Number of processed requests
  - Number of pending requests
  - Number of errors (dropped or timed-out requests)
- **TCP connection between a Web client and a Webserver**—An App-ID module is used to identify an HTTP connection. The EWF solution identifies an HTTP connection after the device receives the first SYN packet. If an HTTP request has to be blocked, EWF sends a block message from the device to the Web client. EWF further sends a TCP FIN request to the client and a TCP reset (RST) to the server to disable the connection. The device sends all the messages through the flow session. The messages follow the entire service chain.
- **HTTP request interception**—EWF intercepts the first HTTP request on the device and performs URL filtering on all methods defined in HTTP 1.0 and HTTP 1.1. The device holds the original request while waiting for a response from the TSC. If the first packet in the HTTP URL is fragmented or if the device cannot extract the URL for some reason, then the destination IP address is used for the categorization.



**NOTE:** For HTTP 1.1 persistent connections, the subsequent requests on that session are ignored by the EWF module.

If the device holds the original request for a long time, then the client will retransmit the request. The URL filtering code will detect the retransmitted packets. If the original HTTP request has already been forwarded, then EWF forwards the retransmitted

packet to the server. However, if EWF is in the middle of first-packet processing or makes the calculation to block the session, then the solution drops the retransmitted packet. A counter tracks the number of retransmitted packets received by the device.

If the TSC does not respond in time to the categorization request from the device, then the original client request is blocked or permitted as per the timeout fallback setting.

- **HTTPS request interception**— EWF intercepts HTTPS traffic passing through the SRX Series device. The security channel from the SRX Series device is divided as one SSL channel between the client and the SRX Series device and another SSL channel between the SRX Series device and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to the UTM. UTM extracts the URL from the HTTP request message.
- **Blocking message**—The blocking message sent to the Web client is user-configurable and is of the following types:
  - The Juniper Networks blocking message is the default message defined in the device that can be modified by the user. The default blocking message contains the reason why the request is blocked and the category name (if it is blocked because of a category).
  - Syslog message.

For example, if you have set the action for Enhanced\_Search\_Engines\_and\_Portals to block, and you try to access [www.example.com](http://www.example.com), the blocking message is of the following form: **Juniper Web Filtering:Juniper Web Filtering has been set to block this site.**

**CATEGORY: Enhanced\_Search\_Engines\_and\_Portals REASON: BY\_PRE\_DEFINED .**

However, the corresponding syslog message on the DUT is:

**WEBFILTER\_URL\_BLOCKED: WebFilter: ACTION="URL Blocked"**

**56.56.56.2(59418)->74.125.224.48(80)**

**CATEGORY="Enhanced\_Search\_Engines\_and\_Portals" REASON="by predefined category" PROFILE="web-ewf" URL=www.example.com OBJ=/ .**

- **Monitoring the Websense server**—The URL filtering module uses two methods to determine if the TSC is active: socket connections and heartbeat. EWF maintains persistent TCP sockets to the TSC. The server responds with a TCP ACK if it is enabled. EWF sends an application layer NOOP keepalive to the TSC. If the device does not receive responses to three consecutive NOOP keepalives in a specific period, it determines the socket to be inactive. The EWF module attempts to open a new connection to the TSC. If all sockets are inactive, the TSC is considered to be inactive. Therefore an error occurs. The error is displayed and logged. Subsequent requests and pending requests are either blocked or passed according to the server connectivity fallback setting until new connections to the TSC are opened again.
- **HTTP protocol communication with the TSC**—EWF uses the HTTP 1.1 protocol to communicate with the TSC. This ensures a persistent connection and transmission of multiple HTTP requests through the same connection. A single HTTP request or response is used for client or server communication. The TSC can handle queued requests; for optimal performance, an asynchronous request or response mechanism is used. The requests are sent over TCP, so TCP retransmission is used to ensure request or response delivery. TCP also ensures valid in-order, non-retransmitted HTTP stream data is sent to the HTTP client on the device.

- **Responses**—The responses adhere to the basic HTTP conventions. Successful responses include a 20x response code (typically 200). An error response includes a 4xx or 5xx code. Error responses in the 4xx series indicate issues in the custom code. Error responses in the 5xx series indicate issues with the service.

Error codes and meanings are as follows:

- 400—Bad request
- 403—Forbidden
- 404—Not found
- 408—Request canceled or null response
- 500—Internal server error

Errors in the 400 series indicate issues with the request. Errors in the 500 series indicate issues with the TSC service. Websense is notified of these errors automatically and responds accordingly.

You can configure the default fallback setting to determine whether to pass or block the request: **set security utm feature-profile web-filtering juniper-enhanced profile juniper-enhanced fallback-settings default ?**

The response also contains the site categorization and site reputation information.

- **Categories**—A category list is available on the device. This list consists of categories, each containing a category code, a name, and a parent ID. Categories can also be user-defined. Each category consists of a list of URLs or IP addresses. Categories are not updated dynamically and are tied to the Junos OS release because they have to be compiled into the Junos OS image. Any update in categories needs to be synchronized with the Junos OS release cycle.
- **Caching**—Successfully categorized responses are cached on the device. Uncategorized URLs are not cached. The size of the cache can be configured by the user.
- **Safe search (HTTP support only, not HTTPS)**—A safe-search solution is used to ensure that the embedded objects, such as images on the URLs received from the search engines, are safe and that no undesirable content is returned to the client.

A URL is provided to the TSC to provide categorization information. If it is a search URL, the TSC also returns a safe-search string. For instance, the safe-search string is **safe=active**. This safe-search string is appended to the URL, and a redirect response for redirecting the client's query with safe search is turned on. This ensures that no unsafe content is returned to the client. If the TSC indicates that it needs to be safe-searched, then you can perform the safe-search redirect.

For example, the client makes a request to the URL

[http://images.example.com/images?hl=en&source=imghp&biw=1183&bih=626&q=adult+movies&gbv=2&aq=f&aql=&oq=&gs\\_rfai=No category action is defined for this URL](http://images.example.com/images?hl=en&source=imghp&biw=1183&bih=626&q=adult+movies&gbv=2&aq=f&aql=&oq=&gs_rfai=No+category+action+is+defined+for+this+URL) . TSC returns safe-search string **safe=active**. The EWF code on the DUT generates a HTTP 302 response, with the redirect URL:

[http://images.example.com/images?hl=en&source=imghp&biw=1183&bih=626&q=adult+movies&gbv=2&aq=f&aql=&oq=&gs\\_rfai=&safe=active](http://images.example.com/images?hl=en&source=imghp&biw=1183&bih=626&q=adult+movies&gbv=2&aq=f&aql=&oq=&gs_rfai=&safe=active) . This response is returned to the client. The client now sends out a safe redirect request to this URL.



**NOTE:** Safe-search redirect supports HTTP only. You cannot extract the URL for HTTPS. Therefore it is not possible to generate a redirect response for HTTPS search URLs. Safe-search redirects can be disabled by using the CLI option `no-safe-search`.

- **Site reputation**—The TSC provides site reputation information. Based on these reputations, you can choose a block or a permit action. If the URL is not handled by a whitelist or a blacklist and does not fall in a user or predefined category, then the reputation can be used to perform URL filtering decision.

The reputation scores are as follows:

- 100-90—Site is considered very safe.
- 80-89—Site is considered moderately safe.
- 70-79—Site is considered fairly safe.
- 60-69—Site is considered suspicious.
- 0-59—Site is considered harmful.

The device maintains a log for URLs that are blocked or permitted based on site reputation scores.

- **Profiles**—A URL filtering profile is defined as a list of categories, with each profile having an action type (permit, log-and-permit, block, quarantine) associated with it. A predefined profile, *junos-wf-enhanced-default*, is provided to users if they choose not to define their own profile.

You can also define an action based on site reputations in a profile to specify the action when the incoming URL does not belong to any of the categories defined in the profile. If you do not configure the site reputation handling information, then you can define a default action. All URLs that do not have a defined category or defined reputation action in their profile will be blocked, permitted, logged-and-permitted, or quarantined depending on the block or permit handling for the default action explicitly defined in the profile. If you do not specify a default action, then the URLs will be permitted. For search engine requests, if there is no explicit user-defined configuration, and the URL request is without the safe search option, then EWF generates a redirect response and sends it to the client. The client will generate a new search request with the safe-search option enabled.

**NOTE:**

A URL filtering profile can contain the following items:

- Multiple user-defined and predefined categories, each with a permit or block action
- Multiple site reputation handling categories, each with a permit or block action
- One default action with a permit or block action

The order of search is blacklist, whitelist, user-defined category, predefined category, safe-search, site reputation, and default action.

**Related  
Documentation**

- [Web Filtering Overview on page 89](#)
- [Understanding Local Web Filtering on page 112](#)
- [Understanding Redirect Web Filtering on page 120](#)
- [Enhanced Web Filtering Overview on page 91](#)
- [Example: Configuring Enhanced Web Filtering on page 97](#)

## Example: Configuring Enhanced Web Filtering

- [Requirements on page 97](#)
- [Overview on page 97](#)
- [Configuration on page 98](#)
- [Verification on page 104](#)

### Requirements

Before you begin, you should be familiar with Web filtering and Enhanced Web Filtering (EWF). See [“Web Filtering Overview” on page 89](#) and [“Understanding Enhanced Web Filtering Process” on page 92](#).

### Overview

In this example, you configure custom objects and feature profiles.

In the first example configuration, you create a custom object called `urllist3` that contains the pattern `http://www.example.net 1.2.3.4`. The `urllist3` custom object is then added to the custom URL category `custurl3`.

In the second example configuration, you configure the Web filtering feature profile. You set the URL blacklist filtering category to `custblacklist`, set the whitelist filtering category to `custwhitelist`, and set the type of Web filtering engine to `juniper-enhanced`. Then you set the cache size parameters for Web filtering to 500 KB and the cache timeout parameters to 1800.

You name the EWF server as `rp.cloud.example.com` and enter 80 as the port number for communicating with it. (Default port is 80.) Then you create an EWF profile name called `junos-wf-enhanced-default`.

Next you select a category from the included whitelist and blacklist categories or select a custom URL category list you created for filtering against. Then you enter an action (permit, log and permit, block, or quarantine) to go with the filter. You do this as many times as necessary to compile your whitelists and blacklists and their accompanying actions. This example blocks URLs in the `Enhanced_Hacking` category. You also specify the action to be taken depending on the site reputation returned for the URL if there is no category match found.

Then you enter a custom message to be sent when HTTP requests are blocked. This example configures the device to send an `***access denied***` message. You select a default action (permit, log and permit, block, or quarantine) for this profile for requests that does not match to any explicitly configured action. This example sets the default action to block. You select fallback settings (block or log and permit) for this profile, in case errors occur in each configured category. This example sets fallback settings to block.

You can also define a redirect URL server so that instead of the device sending a block page with plain text html, the device will send an HTTP 302 redirect to this redirect server with some special variables embedded in the HTTP redirect location field. These special variables can be parsed by the redirect server and serve a special block page to the client with rich images and formatting. The CLI command hierarchy is as follows:

```
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default block-message type custom-redirect-url
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default block-message url http://10.10.121.18
```



**NOTE:** If you configure the `security utm feature-profile web-filtering juniper-enhanced profile junos-wf-enhanced-default block-message`, then the default block message configuration takes precedence over the `security utm feature-profile web-filtering juniper-enhanced profile junos-wf-enhanced-default custom-block-message` configuration.

Finally, you enter a timeout value in seconds. Once this limit is reached, fail mode settings are applied. The default is 15 seconds, and you can enter a value from 0 through 1800 seconds. This example sets the timeout value to 10. You also disable the safe-search functionality. By default, search requests have safe-search strings attached to them, and a redirect response is sent to ensure that all search requests are safe or strict.

## Configuration

- [Configuring Enhanced Web Filtering Custom Objects on page 99](#)
- [Configuring the Enhanced Web Filtering Feature Profiles on page 100](#)

### Configuring Enhanced Web Filtering Custom Objects

**CLI Quick Configuration** To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm custom-objects url-pattern urllist3 value http://www.example.net
set security utm custom-objects url-pattern urllist3 value 1.2.3.4
set security utm custom-objects url-pattern urllistblack value http://www.untrusted.com
set security utm custom-objects url-pattern urllistblack value 13.13.13.13
set security utm custom-objects url-pattern urllistwhite value http://www.trusted.com
set security utm custom-objects url-pattern urllistwhite value 7.7.7.7
set security utm custom-objects custom-url-category custurl3 value urllist3
set security utm custom-objects custom-url-category custblacklist value urllistblack
set security utm custom-objects custom-url-category custwhitelist value urllistwhite
```



**WARNING:** A custom category does not take precedence over a predefined category when it has the same name as one of the predefined categories. Do not use the same name for a custom category that you have used for a predefined category.

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration* in the *CLI User Guide*.

To configure integrated Web filtering:

1. Create custom objects and create the URL pattern list.  

```
[edit security utm]
user@host# set custom-objects url-pattern urllist3 value [http://www.example.net 1.2.3.4]
```
2. Configure the custom URL category list custom object using the URL pattern list.  

```
[edit security utm]
user@host# set custom-objects custom-url-category custurl3 value urllist3
```
3. Create a list of untrusted sites.  

```
[edit security utm]
user@host# set custom-objects url-pattern urllistblack value [http://www.untrusted.com 13.13.13.13]
```
4. Configure the custom URL category list custom object using the URL pattern list of untrusted sites.  

```
[edit security utm]
user@host# set custom-objects custom-url-category custblacklist value urllistblack
```
5. Create a list of trusted sites.  

```
[edit security utm]
```

```
user@host# set custom-objects url-pattern urllistwhite value  
[http://www.trusted.com 7.7.7.7]
```

6. Configure the custom URL category list custom object using the URL pattern list of trusted sites.

```
[edit security utm]  
user@host# set custom-objects custom-url-category custwhitelist value urllistwhite
```

**Results** From configuration mode, confirm your configuration by entering the **show security utm custom-objects** command. If the output does not display the intended configuration, repeat the instructions in this example to correct.

```
[edit]  
userhost#show security utm custom-objects  
url-pattern {  
  urllist3 {  
    value [ http://www.example.net ];  
  }  
  urllistblack {  
    value [ http://www.untrusted.com 13.13.13.13 ];  
  }  
  urllistwhite {  
    value [ http://www.trusted.com 7.7.7.7 ];  
  }  
}  
custom-url-category {  
  custurl3 {  
    value urllist3;  
  }  
  custblacklist {  
    value urllistblack;  
  }  
  custwhitelist {  
    value urllistwhite;  
  }  
}
```

If you are done configuring the device, enter **commit** from configuration mode.

---

### Configuring the Enhanced Web Filtering Feature Profiles

**CLI Quick Configuration** To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile web-filtering url-whitelist custwhitelist  
set security utm feature-profile web-filtering url-blacklist custblacklist  
set security utm feature-profile web-filtering juniper-enhanced cache size 500  
set security utm feature-profile web-filtering juniper-enhanced cache timeout 1800  
set security utm feature-profile web-filtering juniper-enhanced server host  
  rp.cloud.example.com  
set security utm feature-profile web-filtering juniper-enhanced server port 80  
set security utm feature-profile web-filtering http-reassemble
```

```

set security utm feature-profile web-filtering http-persist
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default category Enhanced_Hacking action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default site-reputation-action very-safe permit
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default site-reputation-action moderately-safe log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default site-reputation-action fairly-safe log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default site-reputation-action harmful block
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default site-reputation-action suspicious block
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default default block
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default custom-block-message "****access denied ****"
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default default block
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default fallback-settings server-connectivity block
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default fallback-settings timeout block
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default fallback-settings too-many-requests block
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default timeout 10
set security utm feature-profile web-filtering juniper-enhanced profile
  junos-wf-enhanced-default no-safe-search
set security utm utm-policy mypolicy web-filtering http-profile my_ewfprofile01
set security policies from-zone utm_clients to-zone mgmt policy 1 then permit
  application-services utm-policy mypolicy
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  quarantine-custom-message "***The requested webpage is blocked by your
  organization's access policy***".
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  quarantine-message type custom-redirect-url
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  quarantine-message url besgas.spglab.example.net

```

### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration* in the *CLI User Guide*.

To configure the EWF feature profiles:

1. Configure the Web filtering URL blacklist.  

```

[edit security utm feature-profile web-filtering]
user@host# set url-blacklist custblacklist

```
2. Configure the Web filtering URL whitelist.  

```

[edit security utm feature-profile web-filtering]
user@host# set url-whitelist custwhitelist

```
3. Specify the EWF engine, and set the cache size parameters.

- [edit security utm feature-profile web-filtering]  
user@host# set juniper-enhanced cache size 500
4. Set the cache timeout parameters.
- [edit security utm feature-profile web-filtering]  
user@host# set juniper-enhanced cache timeout 1800
5. Set the server name or IP address.
- [edit security utm feature-profile web-filtering]  
user@host# set juniper-enhanced server host rp.cloud.example.com
6. Enter the port number for communicating with the server.
- [edit security utm feature-profile web-filtering]  
user@host# set juniper-enhanced server port 80
7. Set HTTP fragment reassemble.
- [edit security utm feature-profile web-filtering]  
user@host# set security utm feature-profile web-filtering http-reassemble
8. Set HTTP requests in the same session.
- [edit security utm feature-profile web-filtering]  
user@host# set security utm feature-profile web-filtering http-persist
9. Create a profile name, and select a category from the included whitelist and blacklist categories.
- [edit security utm feature-profile web-filtering]  
user@host# set juniper-enhanced profile junos-wf-enhanced-default category  
Enhanced\_Hacking action log-and-permit
10. Specify the action to be taken depending on the site reputation returned for the URL if there is no category match found.
- [edit security utm feature-profile web-filtering]  
user@host#set juniper-enhanced profile junos-wf-enhanced-default  
site-reputation-action very-safe permit  
user@host#set juniper-enhanced profile junos-wf-enhanced-default  
site-reputation-action moderately-safe log-and-permit  
user@host#set juniper-enhanced profile junos-wf-enhanced-default  
site-reputation-action fairly-safe log-and-permit  
user@host#set juniper-enhanced profile junos-wf-enhanced-default  
site-reputation-action harmful block  
user@host#set juniper-enhanced profile junos-wf-enhanced-default  
site-reputation-action suspicious block
11. Enter a custom message to be sent when HTTP requests are blocked.
- [edit security utm feature-profile web-filtering]  
user@host# set juniper-enhanced profile junos-wf-enhanced-default  
custom-block-message "\*\*\*access denied \*\*\*"
12. Select a default action (permit, log and permit, block, or quarantine) for the profile, when no other explicitly configured action (blacklist, whitelist, custom category, predefined category actions, or site reputation actions) is matched .
- [edit security utm feature-profile web-filtering]  
user@host# set juniper-enhanced profile junos-wf-enhanced-default default block

13. Select fallback settings (block or log and permit) for this profile.

```
[edit security utm feature-profile web-filtering]
set juniper-enhanced profile junos-wf-enhanced-default fallback-settings default
block
user@host# set juniper-enhanced profile junos-wf-enhanced-default
fallback-settings server-connectivity block
user@host# set juniper-enhanced profile junos-wf-enhanced-default
fallback-settings timeout block
set juniper-enhanced profile junos-wf-enhanced-default fallback-settings
too-many-requests block
```

14. Enter a timeout value in seconds.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile junos-wf-enhanced-default timeout 10
```

15. Disable the safe-search option.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile junos-wf-enhanced-default no-safe-search
```

16. Configure a UTM policy for the Web-filtering HTTP protocol and attach this policy to a security profile to implement it.

```
[edit security utm]
user@host# set utm-policy mypolicy web-filtering http-profile my_ewfprofile01
```

17. Configure a security policy.

```
[edit security]
user@host# set policies from-zone utm_clients to-zone mgmt policy 1 then permit
application-services utm-policy mypolicy
```

**Results** From configuration mode, confirm your configuration by entering the **show security utm feature-profile** command. If the output does not display the intended configuration, repeat the instructions in this example to correct.

```
[edit]
user@host# show security utm
feature-profile {
web-filtering {
url-whitelist custwhitelist;
url-blacklist custblacklist;
http-reassemble;
http-persist;
type juniper-enhanced;
juniper-enhanced {
cache {
timeout 1800;
size 500;
}
server {
host rp.cloud.example.com;
port 80;
}
profile junos-wf-enhanced-default {
category {
```

```
Enhanced_Hacking {
    action log-and-permit;
}
Enhanced_Government {
    action quarantine;
}
}
site-reputation-action {
    very-safe permit;
    moderately-safe log-and-permit;
    fairly-safe log-and-permit;
    harmful block;
    suspicious block;
}
default block;
custom-block-message "***access denied ***";
fallback-settings {
    default block;
    server-connectivity block;
    timeout block;
    too-many-requests block;
}
timeout 10;
no-safe-search;
}
utm-policy mypolicy {
    web-filtering {
        http-profile my_ewfprofile01;
    }
}
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying the Status of the Web Filtering Server on page 104](#)
- [Verifying the Increase in Web Filtering Statistics on page 104](#)

---

### Verifying the Status of the Web Filtering Server

**Purpose** Verify the Web filtering server status.

**Action** From the top of the configuration in configuration mode, enter the **show security utm web-filtering status** command.

---

### Verifying the Increase in Web Filtering Statistics

**Purpose** Verify the increase in Web filtering statistics.

- Action** From the top of the configuration in configuration mode, enter the **show security utm web-filtering statistics** command.
- Related Documentation**
- [Web Filtering Overview on page 89](#)
  - [Understanding Redirect Web Filtering on page 120](#)
  - [Enhanced Web Filtering Overview on page 91](#)
  - [Understanding Enhanced Web Filtering Process on page 92](#)

## Understanding the Quarantine Action for Enhanced Web Filtering

UTM Enhanced Web Filtering supports block, log-and-permit, and permit actions for HTTP/HTTPS requests. In addition to this, UTM Enhanced Web Filtering now supports the quarantine action which allows or denies access to the blocked site based on the user's response to the message.

The following sequence explains how the HTTP or HTTPS request is intercepted, redirected, and acted upon by the quarantine action:

- The HTTP client requests URL access.
- The device intercepts the HTTP request and sends the extracted URL to the Websense Thread Seeker Cloud (TSC).
- The TSC returns the URL category and the site reputation information to the device.
- If the action configured for the category is quarantine, the device logs the quarantine action and sends a redirect response to HTTP client.
- The URL is sent to the HTTP server for redirecting.
- The device shows a warning message stating that the access to the URL is blocked according to the organization's security policies and prompts the user to respond.
- If the user response is "No," the session is terminated. If the user response is "Yes," the user is allowed access to the site and such access is logged and reported to the administrator.



**NOTE:** On all branch SRX Series devices, the quarantine action is supported only for UTM Enhanced Web Filtering or Juniper enhanced type of Web filtering.

### Quarantine Message

The quarantine message sent to the HTTP client is user-configurable and is of the following types:

- Default message

The default quarantine message is displayed when a user attempts to access a quarantined website and it contains the following information:

- URL name
- Quarantine reason
- Category (if available)
- Site-reputation (if available)

For example, if you have set the action for `Enhanced_Search_Engines_and_Portals` to quarantine, and you try to access `www.search.example.com`, the quarantine message is as follows:

**\*\*\*The requested webpage is blocked by your organization's access policy\*\*\***

- Syslog message.

The syslog message will be logged by the system when the user access the web page that has already been quarantined and marked as block or permit.

The corresponding syslog message on the device under test is:

```
Jan 25 15:10:40 rodian utmd[3871]: WEBFILTER_URL_BLOCKED: WebFilter:
ACTION="URL Blocked" 99.99.99.4(60525)->74.125.224.114(80)
CATEGORY="Enhanced_Search_Engines_and_Portals" REASON="by predefined
category(quarantine)" PROFILE="ewf-test-profile" URL=www.search.example.com
OBJ=/  

```

#### Related Documentation

- [Web Filtering Overview on page 89](#)
- [Understanding Integrated Web Filtering](#)
- [Understanding Local Web Filtering on page 112](#)
- [Understanding Redirect Web Filtering on page 120](#)
- [Understanding Enhanced Web Filtering Process on page 92](#)
- [Example: Configuring Enhanced Web Filtering on page 97](#)
- [Example: Configuring Site Reputation Action for Enhanced Web Filtering on page 106](#)

---

## Example: Configuring Site Reputation Action for Enhanced Web Filtering

This example shows how to configure the site reputation action for both categorized and uncategorized URLs.

- [Requirements on page 107](#)
- [Overview on page 107](#)
- [Configuration on page 107](#)
- [Verification on page 110](#)

## Requirements

Before you begin, you should be familiar with Web Filtering and Enhanced Web Filtering. See [“Web Filtering Overview” on page 89](#) and [“Understanding Enhanced Web Filtering Process” on page 92](#).

## Overview

In this example, you configure Web Filtering profiles to URLs according to defined categories using the site reputation action. You set the URL whitelist filtering category to url-cat-white and the type of Web Filtering engine to juniper-enhanced. Then you set the cache size parameters for Web Filtering and the cache timeout parameters to 1.

Then you create a juniper-enhanced profile called profile ewf-test-profile, set the URL whitelist category to cust-cat-quarantine, and set the reputation action to quarantine.

You enter a custom message to be sent when HTTP requests are quarantined. In this example, the following message is sent: **\*\*\*The requested webpage is blocked by your organization's access policy\*\*\***.

You block URLs in the Enhanced\_News\_and\_Media category and permit URLs in the Enhanced\_Education category. Then you quarantine the URLs in the Enhanced\_Streaming\_Media category and configure the device to send the following message: **\*\*\*The requested webpage is blocked by your organization's access policy\*\*\***.

In this example, you set the default action to permit. You select fallback settings (block or log and permit) for this profile in case errors occur in each configured category. Finally, you set the fallback settings to block.

## Configuration

### Configuring Site Reputation Action

**CLI Quick Configuration** To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile web-filtering set url-whitelist url-cat-white
set security utm feature-profile web-filtering juniper-enhanced cache size
set security utm feature-profile web-filtering juniper-enhanced cache timeout 1
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
category cust-cat-quarantine action quarantine
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
category Enhanced_News_and_Media action block
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
category Enhanced_Education action permit
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
category Enhanced_Education reputation-action harmful block
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
category Enhanced_Streaming_Media action quarantine
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
default permit
```

```

set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
default quarantine-message "**** The requested webpage is blocked by your
organization's access policy****".
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
fallback-settings server-connectivity block
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
fallback-settings timeout block

```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration* in the *CLI User Guide*.

To configure the site reputation action:

1. Configure the Web Filtering URL whitelist.  

```

[edit security utm feature-profile web-filtering]
user@host# set url-whitelist custwhitelist

```
2. Specify the Enhanced Web Filtering engine, and set the cache size parameters.  

```

[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced cache size

```
3. Set the cache timeout parameters.  

```

[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced cache timeout 1

```
4. Create a profile name, and select a category from the whitelist categories.  

```

[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile category
cust-cat-quarantine action quarantine

```
5. Create a profile name, and select a category from the whitelist categories.  

```

[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile category
Enhanced_News_and_Media action block
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile category
Enhanced_Education action permit
user@host# set juniper-enhanced profile ewf-test-profile category
Enhanced_Education action harmful block
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile category
Enhanced_Streaming_Media action quarantine

```
6. Enter a warning message to be sent when HTTP requests are quarantined.  

```

[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile
quarantine-custom-message "****The requested webpage is blocked by your
organization's access policy ****"

```
7. Select a default action (permit, log and permit, block, or quarantine) for the profile, when no other explicitly configured action (blacklist, whitelist, custom category, predefined category or site reputation ) is matched .

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile default permit
```

8. Select fallback settings (block or log and permit) for this profile.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile fallback-settings
server-connectivity block
user@host# set juniper-enhanced profile ewf-test-profile fallback-settings timeout
block
```

**Results** From configuration mode, confirm your configuration by entering the **show security utm** command. If the output does not display the intended configuration, repeat the instructions in this example to correct.

```
[edit]
user@host# show security utm
feature-profile{
web-filtering {
url-whitelist url-cat-white;
type juniper-enhanced;
traceoptions;
flag all;
}
juniper-enhanced {
cache {
timeout 1
}
profile ewf-test-profile {
category {
cust-cat-quarantine {
action quarantine;
}
Enhanced_News_and_Media {
action block;
reputation-action;
}
Enhanced_Education {
action permit;
reputation-action;
{
harmful block;
}
}
Enhanced_Streaming_Media {
action quarantine;
}
}
default permit;
quarantine-custom-message "***The requested webpage is blocked by your
organization's access policy***".
fallback-settings {
server-connectivity block;
timeout block;
}
}
```

```
}  
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

Confirm that the configuration is working properly.

- [Verifying the Status of UTM Service on page 110](#)
- [Verifying the Status of UTM Session on page 110](#)
- [Verifying the Status of UTM Web Filtering on page 110](#)
- [Verifying the Statistics of UTM Web Filtering on page 111](#)

---

### Verifying the Status of UTM Service

**Purpose** Verify the UTM service status.

**Action** From operational mode, enter the **show security utm status** command.

## Sample Output

```
user@host>show security utm status  
UTM service status: Running
```

---

### Verifying the Status of UTM Session

**Purpose** Verify the UTM session status.

**Action** From operational mode, enter the **show security utm session** command.

## Sample Output

```
user@host>show security utm session  
UTM session info:  
Maximum sessions:           4000  
Total allocated sessions:    0  
Total freed sessions:        0  
Active sessions:             0
```

---

### Verifying the Status of UTM Web Filtering

**Purpose** Verify the UTM Web filtering status.

**Action** From operational mode, enter the **show security utm web-filtering status** command.

## Sample Output

```
user@host>show security utm web-filtering status  
UTM web-filtering status:  
Server status: Juniper Enhanced using Websense server UP
```

### Verifying the Statistics of UTM Web Filtering

- Purpose** Verify the Web filtering statistics for connections including whitelist and blacklist hits and custom category hits.
- Action** From operational mode, enter the **show security utm web-filtering statistics** command.

### Sample Output

```

user@host>show security utm web-filtering statistics
UTM web-filtering statistics:
  Total requests:                2594
  white list hit:                 0
  Black list hit:                 0
  Queries to server:             2407
  Server reply permit:           1829
  Server reply block:             0
  Server reply quarantine:        517
  Server reply quarantine block:  0
  Server reply quarantine permit: 8
  Custom category permit:         0
  Custom category block:          0
  Custom category quarantine:     0
  Custom category quarantine block: 0
  Custom category quarantine permit: 0
  Site reputation permit:         0
  Site reputation block:          0
  Site reputation quarantine:     0
  Site reputation quarantine block: 0
  Site reputation quarantine permit: 0
  Site reputation by Category    0
  Site reputation by Global      0
  Cache hit permit:              41
  Cache hit block:                0
  Cache hit quarantine:          144
  Cache hit quarantine block:     0
  Cache hit quarantine permit:    1
  Safe-search redirect:          0
  Web-filtering sessions in total: 16000
  Web-filtering sessions in use:  0
  Fallback:                      log-and-permit      block
    Default                      0              0
    Timeout                      0              0
    Connectivity                  0              1
    Too-many-requests             0              0

```

- Related Documentation**
- [Web Filtering Overview on page 89](#)
  - [Understanding Redirect Web Filtering on page 120](#)
  - [Enhanced Web Filtering Overview on page 91](#)
  - [Understanding Enhanced Web Filtering Process on page 92](#)
  - [Example: Configuring Enhanced Web Filtering on page 97](#)
  - [Understanding the Quarantine Action for Enhanced Web Filtering on page 105](#)
  - [web-filtering on page 255](#)

## Understanding Local Web Filtering

---

With local Web filtering, the firewall intercepts every HTTP request in a TCP connection and extracts the URL. The decision making is done on the device after it looks up a URL to determine if it is in the whitelist or blacklist based on its user-defined category. If the URL is in the url-blacklist, the request is blocked; if it's in the url-whitelist, the request is permitted. If the URL is not in either list, the defined default action will occur (block, log-and-permit, or permit). You can permit or block access to a requested site by binding a Web filtering profile to a firewall policy. Local Web filtering provides basic Web filtering without requiring an additional license or external category server.

This topic contains the following sections:

- [User-Defined URL Categories on page 112](#)
- [Local Web Filtering Process on page 112](#)
- [Local Web Filtering Profiles on page 113](#)
- [Profile Matching Precedence on page 113](#)

### User-Defined URL Categories

When defining your own URL categories, you can group URLs and create categories specific to your needs. Each category can have a maximum of 20 URLs. When you create a category, you can add either the URL or the IP address of a site. When you add a URL to a user-defined category, the device performs DNS lookup, resolves the hostname into IP addresses, and caches this information. When a user tries to access a site with the IP address of the site, the device checks the cached list of IP addresses and tries to resolve the hostname. Many sites have dynamic IP addresses, meaning that their IP addresses change periodically. A user attempting to access a site can type an IP address that is not in the cached list on the device. Therefore, if you know the IP addresses of sites you are adding to a category, enter both the URL and the IP address(es) of the site.

You define your own categories using URL pattern list and custom URL category list custom objects. Once defined, you assign your categories to the global user-defined url-blacklist (block) or url-whitelist (permit) categories.



**NOTE:** Web filtering is performed on all the methods defined in HTTP1.0 and HTTP 1.1.

---

### Local Web Filtering Process

This is a general description of how Web traffic is intercepted and acted upon by the Web filtering module.

1. The device intercepts a TCP connection.
2. The device intercepts each HTTP request in the TCP connection.

3. The device extracts each URL in the HTTP request and checks its URL against the user-defined whitelist and blacklist.
4. If the URL is found in the blacklist, the request is not permitted and a deny page is sent to the http client. If the URL is found in the whitelist, the request is permitted.
5. If the URL is not found in the whitelist or blacklist, the configured default fallback action is applied. If no fallback action is defined, then the request is permitted.

## Local Web Filtering Profiles

You configure Web filtering profiles that permit or block URLs according to defined custom categories. A Web filtering profile consists of a group of URL categories assigned one of the following actions:

- **Blacklist** — The device always blocks access to the websites in this list. Only user-defined categories are used with local Web filtering.
- **Whitelist** — The device always allows access to the websites in this list. Only user-defined categories are used with local Web filtering.

A Web filtering profile can contain one blacklist or one whitelist with multiple user-defined categories each with a permit or block action. You can define a default fallback action when the incoming URL does not belong to any of the categories defined in the profile. If the action for the default category is block, the incoming URL is blocked if it does not match any of the categories explicitly defined in the profile. If an action for the default action is not specified, the default action of permit is applied to the incoming URL not matching any category.

## Profile Matching Precedence

When a profile employs several categories for URL matching, those categories are checked for matches in the following order:

1. If present, the global blacklist is checked first. If a match is made, the URL is blocked. If no match is found...
2. The global whitelist is checked next. If a match is made, the URL is permitted. If no match is found...
3. User-defined categories are checked next. If a match is made, the URL is blocked or permitted as specified.

### Related Documentation

- [Web Filtering Overview on page 89](#)
- [Understanding Redirect Web Filtering on page 120](#)
- [Example: Configuring Local Web Filtering on page 114](#)

## Example: Configuring Local Web Filtering

---

This example shows how to configure local Web filtering.

- [Requirements on page 114](#)
- [Overview on page 114](#)
- [Configuration on page 114](#)
- [Verification on page 119](#)

### Requirements

Before you begin, learn more about Web filtering. See [“Web Filtering Overview” on page 89](#).

### Overview

In this example you configure local Web filtering custom objects, local Web filtering feature profiles, and local Web filtering UTM policies. You also attach local Web filtering UTM policies to security policies.

In the first example configuration you create custom objects called `urllist5` and `urllist6` that contains the patterns `http://www.example.net 1.2.3.4` and `http://www.example.com 1.2.3.4` respectively. The `urllist5` and `urllist6` custom objects are then added to the custom URL category `custurl5` and `custurl6`.

In the second example configuration, you configure the Web filtering feature profile. You set the URL blacklist filtering category to `custurl4` and URL whitelist filtering category to `custurl3`. You set the type of Web filtering engine to `juniper-local`.

Then you create a `juniper-local` profile name called `localprofile1`. You select a default action (permit, log and permit, block) for this profile for requests that experience errors. This example sets the default action to permit.

Then you enter a custom message to be sent when HTTP requests are blocked. This example configures the device to send an `***Access to this site is not permitted***` message. You select fallback settings (block or log and permit) for this profile, in case errors occur in each configured category. This example sets fallback settings to block.

In the third example configuration, you create UTM policy `utmp5` and attach it to profile `localprofile1`.

In the final example configuration, you attach the UTM policy `utmp5` to the security policy `p5`.

### Configuration

- [Configuring Local Web Filtering Custom Objects on page 115](#)
- [Configuring the Local Web Filtering Feature Profiles on page 116](#)
- [Configuring Local Web Filtering UTM Policies on page 117](#)
- [Attaching Local Web Filtering UTM Policies to Security Policies on page 118](#)

### Configuring Local Web Filtering Custom Objects

**CLI Quick Configuration** To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm custom-objects url-pattern urllist5 value http://www.example.net
set security utm custom-objects url-pattern urllist5 value 1.2.3.4
set security utm custom-objects url-pattern urllist6 value http://www.example.com
set security utm custom-objects url-pattern urllist6 value 1.2.3.4
set security utm custom-objects custom-url-category custurl5 value urllist5
set security utm custom-objects custom-url-category custurl6 value urllist6
```

**Step-by-Step Procedure** To configure local Web filtering using the CLI:

1. Create custom objects and URL pattern lists.

```
[edit]
user@host# set security utm custom-objects url-pattern urllist5 value
[http://www.example.net 1.2.3.4]
user@host# set security utm custom-objects url-pattern urllist6 value
[http://www.example.com 1.2.3.4]
```

2. Configure the custom URL category list custom object using the URL pattern list.

```
[edit]
user@host# set security utm custom-objects custom-url-category custurl5 value
urllist5
user@host# set security utm custom-objects custom-url-category custurl6 value
urllist6
```

**Results** From configuration mode, confirm your configuration by entering the **show security utm custom-objects** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost#show security utm custom-objects
url-pattern {
  urllist5 {
    value [ http://www.example.net 1.2.3.4 ];
  }
  urllist6 {
    value [ http://www.example.com 1.2.3.4 ];
  }
}
custom-url-category {
  custurl5 {
    value urllist5;
  }
  custurl6 {
    value urllist6;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

### Configuring the Local Web Filtering Feature Profiles

#### CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile web-filtering url-whitelist custurl3
set security utm feature-profile web-filtering url-blacklist custurl4
set security utm feature-profile web-filtering type juniper-local
set security utm feature-profile web-filtering juniper-local profile localprofile1 default permit
set security utm feature-profile web-filtering juniper-local profile localprofile1 custom-block-message "Access to this site is not permitted."
set security utm feature-profile web-filtering juniper-local profile localprofile1 fallback-settings default block
set security utm feature-profile web-filtering juniper-local profile localprofile1 fallback-settings too-many-requests block
set security utm feature-profile content-filtering profile contentfilter1
```

#### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration* in the *CLI User Guide*.

To configure local Web filtering feature profiles:

1. Configure the Web filtering feature profiles.  

```
[edit security utm feature-profile web-filtering]
user@host# set url-whitelist custurl3
user@host# set url-blacklist custurl4
```
2. Select the Web filtering engine.  

```
[edit security utm feature-profile web-filtering]
user@host# set type juniper-local
```
3. Select a default action (permit, log and permit, block) for this profile for requests that experience errors.  

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-local profile localprofile1 default permit
```
4. Enter a custom message to be sent when HTTP requests are blocked.  

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-local profile localprofile1 custom-block-message "Access to this site is not permitted"
```
5. Select fallback settings (block or log and permit) for this profile.  

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-local profile localprofile1 fallback-settings default block
set security utm feature-profile web-filtering juniper-local profile localprofile1 fallback-settings too-many-requests block
```

**Results** From configuration mode, confirm your configuration by entering the **show security utm feature-profile** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost#show security utm feature-profile
web-filtering {
  url-whitelist custurl3;
  url-blacklist custurl4;
  type juniper-local;
  juniper-local {
    profile localprofile1 {
      default permit;
      custom-block-message "Access to this site is not permitted.";
      fallback-settings {
        default block;
        too-many-requests block;
      }
    }
  }
}
content-filtering {
  profile contentfilter1;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

### Configuring Local Web Filtering UTM Policies

**CLI Quick Configuration** To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
et security utm utm-policy utmp5 web-filtering http-profile localprofile1
```

**Step-by-Step Procedure** To configure a UTM policy:

1. Create the UTM policy referencing a profile.

```
[edit]
user@host# set security utm utm-policy utmp5 web-filtering http-profile localprofile1
```

**Results** From configuration mode, confirm your configuration by entering the **show security utm** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this show command output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
userhost#show security utm
utm-policy utmp5 {
```

```

web-filtering {
  http-profile localprofile1;
}

```

If you are done configuring the device, enter **commit** from configuration mode.

### Attaching Local Web Filtering UTM Policies to Security Policies

**CLI Quick Configuration** To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```

set security policies from-zone trust to-zone untrust policy p5 match source-address any
set security policies from-zone trust to-zone untrust policy p5 match destination-address any
set security policies from-zone trust to-zone untrust policy p5 match application junos-http
set security policies from-zone trust to-zone untrust policy p5 then permit
application-services utm-policy utmp5

```

**Step-by-Step Procedure** To attach a UTM policy to a security policy:

1. Create and configure the security policy.
 

```

[edit security policies from-zone trust to-zone untrust policy p5]
user@host# set match source-address any
user@host# set match destination-address any
user@host# set match application junos-http

```
2. Attach the UTM policy to the security policy.
 

```

[edit security policies from-zone trust to-zone untrust policy p5]
user@host# set then permit application-services utm-policy utmp5

```

**Results** From configuration mode, confirm your configuration by entering the **show security policies** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
userhost#show security policies
from-zone trust to-zone untrust {
  policy p5 {
    match {
      source-address any;
      destination-address any;
      application junos-http;
    }
    then {
      permit {
        application-services {
          utm-policy utmp5;
        }
      }
    }
  }
}

```

```
}
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying the Configuration of Local Web Filtering Custom Objects on page 119](#)
- [Verifying the Configuration of Local Web Filtering Feature Profiles on page 119](#)
- [Verifying the Configuration of Local Web Filtering UTM Policies on page 119](#)
- [Verifying the Attachment of Local Web Filtering UTM Policies to Security Policies on page 119](#)

### Verifying the Configuration of Local Web Filtering Custom Objects

**Purpose** Verify the configuration of local Web filtering custom objects.

**Action** From operational mode, enter the **show security utm custom-objects** command.

### Verifying the Configuration of Local Web Filtering Feature Profiles

**Purpose** Verify the configuration of local Web filtering feature profiles.

**Action** From operational mode, enter the **show security utm feature-profile** command.

### Verifying the Configuration of Local Web Filtering UTM Policies

**Purpose** Verify the configuration of local Web filtering UTM policies.

**Action** From operational mode, enter the **show security utm** command.

### Verifying the Attachment of Local Web Filtering UTM Policies to Security Policies

**Purpose** Verify the attachment of local Web filtering UTM policies to security policies.

**Action** From operational mode, enter the **show security policies** command.

- Related Documentation**
- [Understanding Local Web Filtering on page 112](#)
  - [Monitoring Web Filtering Configurations on page 129](#)
  - [web-filtering on page 255](#)

## Understanding Redirect Web Filtering

---

With redirect Web filtering, the Web filtering module intercepts an HTTP request. The URL in the request is then sent to the external Websense server, which makes a permit or a deny decision. If access is permitted to the URL in question, the original HTTP request and all the subsequent requests are sent to the intended HTTP server. But if access is denied to the URL in question, a blocking message is sent to the client.

This is a general description of how Web traffic is intercepted, redirected, and acted upon by the Web filtering module:

1. A Web client establishes a TCP connection with the webserver.
2. The Web client then sends an HTTP request.
3. The device intercepts the requests and extract URL. The URL is checked against Global Web filtering whitelists and blacklists. If no match is made, the Websense server configuration parameters are utilized. Otherwise go to step 6.
4. The URL is sent to the Websense server for checking,
5. The Websense server returns a response indicating whether or not the URL is to be permitted or blocked.
6. If access is allowed, then the original HTTP request is sent to the webserver. If access is denied, the device sends a blocking message to the client and tears down the TCP connection.



**NOTE:** Web filtering is performed on all the methods defined in HTTP1.0 and HTTP 1.1. However, redirect Web filtering uses destination IP as URL when it is checking HTTPS traffic.

---



**NOTE:** Decision making from real-time options provides a higher level of accuracy, therefore caching for redirect Web filtering is not supported.

---



**NOTE:** Redirect Web filtering does not require a subscription license.

---

### Related Documentation

- [Web Filtering Overview on page 89](#)
- [Understanding Local Web Filtering on page 112](#)
- [Example: Enhancing Security by Configuring Redirect Web Filtering Using Custom Objects on page 121](#)

## Example: Enhancing Security by Configuring Redirect Web Filtering Using Custom Objects

---

This example shows how to manage Internet usage by configuring redirect Web filtering using custom objects and preventing access to inappropriate Web content.

- [Requirements on page 121](#)
- [Overview on page 121](#)
- [Configuration on page 122](#)
- [Verification on page 127](#)

### Requirements

Before you begin, learn more about Web filtering. See [“Web Filtering Overview” on page 89](#).

### Overview

The benefit of using Web filtering is that it extracts the URLs from HTTP request messages and performs filtering according to the requirements. The advantage of configuring redirect Web filtering is that it extracts the URLs from the HTTP requests and sends them to an external URL filtering server to determine whether to allow or deny access.

In this example you configure redirect Web filtering custom objects, redirect Web filtering feature profiles, and redirect Web filtering UTM policies. You also attach redirect Web filtering UTM policies to security policies.

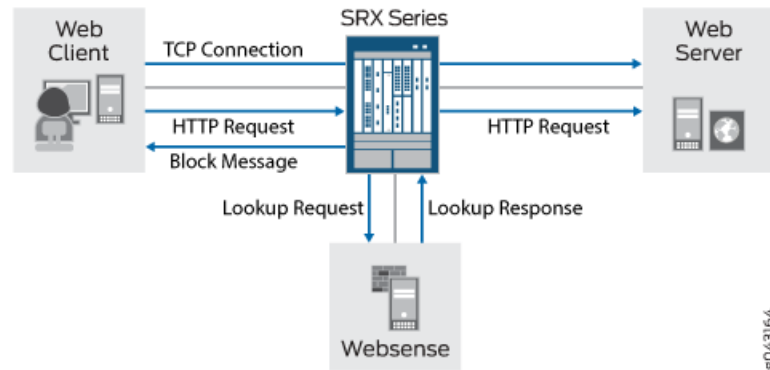
The default websense-redirect server port number is 15868.

You select fallback settings (block or log and permit) for this profile, in case errors occur in each configured category. This example sets fallback settings to block the profile. You enter the number of sockets used for communicating between the client and the server. The default is 32 for SRX Series devices.

Finally, you enter a timeout value in seconds. Once this limit is reached, fail mode settings are applied. The default is 15 seconds, and you can enter a value from 1 to 1800 seconds. This example sets the timeout value to 10.

Figure 1 on page 122 shows the overall architecture for the Websense redirect feature.

Figure 1: Websense Redirect Architecture



## Configuration

- [Configuring Redirect Web Filtering Custom Objects on page 122](#)
- [Configuring the Redirect Web Filtering Feature Profiles on page 124](#)
- [Configuring Redirect Web Filtering UTM Policies and Attaching the Redirect Web Filtering UTM Policies to Security Policies on page 125](#)

### Configuring Redirect Web Filtering Custom Objects

#### CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```

set security utm custom-objects url-pattern urllist4 value 1.2.3.4
set security utm custom-objects url-pattern urllistblack value http://www.untrusted.com
set security utm custom-objects url-pattern urllistblack value 13.13.13
set security utm custom-objects url-pattern urllistwhite value http://www.trusted.com
set security utm custom-objects url-pattern urllistwhite value 7.7.7.7
set security utm custom-objects custom-url-category custurl4 value urllist4
set security utm custom-objects custom-url-category custblacklist value urllistblack
set security utm custom-objects custom-url-category custwhitelist value urllistwhite
  
```

#### Step-by-Step Procedure

To configure redirect Web filtering custom objects:

1. Create custom objects and create the URL pattern list.
 

```

[edit security utm]
user@host# set custom-objects url-pattern urllist4 value [http://www.example.net 1.2.3.4]
      
```
2. Configure the custom URL category list custom object using the URL pattern list.
 

```

[edit security utm]
user@host# set custom-objects custom-url-category custurl4 value urllist4
      
```

3. Create a list of untrusted sites

```
[edit security utm]
user@host# set custom-objects url-pattern urllistblack value
[http://www.untrusted.com 13.13.13.13]
```

4. Configure the custom URL category list custom object using the URL pattern list of untrusted sites.

```
[edit security utm]
user@host# set custom-objects custom-url-category custblacklist value urllistblack
```

5. Create a list of trusted sites.

```
[edit security utm]
user@host# set custom-objects url-pattern urllistwhite value
[http://www.trusted.com 7.7.7.7]
```

6. Configure the custom URL category list custom object using the URL pattern list of trusted sites.

```
[edit security utm]
user@host# set custom-objects custom-url-category custwhitelist value urllistwhite
```

**Results** From configuration mode, confirm your configuration by entering the **show security utm custom-objects** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost# show security utm custom-objects
url-pattern {
  urllist4 {
    value [ http://www.example.net 1.2.3.4 ];
  }
  urllistblack {
    value [ http://www.untrusted.com 13.13.13.13 ];
  }
  urllistwhite {
    value [ http://www.trusted.com 7.7.7.7 ];
  }
}
custom-url-category {
  custurl4 {
    value urllist4;
  }
  custblacklist {
    value urllistblack;
  }
  custwhitelist {
    value urllistwhite;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Configuring the Redirect Web Filtering Feature Profiles

**CLI Quick Configuration** To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile web-filtering url-whitelist custwhitelist
set security utm feature-profile web-filtering url-blacklist custblacklist
set security utm feature-profile web-filtering type websense-redirect
set security utm feature-profile web-filtering websense-redirect profile websenseprofile1
  server host Websenseserver
set security utm feature-profile web-filtering websense-redirect profile websenseprofile1
  server port 15868
set security utm feature-profile web-filtering websense-redirect profile websenseprofile1
  fallback-settings server-connectivity block
set security utm feature-profile web-filtering websense-redirect profile websenseprofile1
  fallback-settings timeout block
set security utm feature-profile web-filtering websense-redirect profile websenseprofile1
  fallback-settings too-many-requests block
set security utm feature-profile web-filtering websense-redirect profile websenseprofile1
  timeout 10
set security utm feature-profile web-filtering websense-redirect profile websenseprofile1
  sockets 1
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure redirect Web filtering feature profiles:

1. Configure the Web filtering URL Black List.  

```
[edit security utm feature-profile web-filtering]
user@host# set url-blacklist custblacklist
```
2. Configure the Web filtering URL White List.  

```
[edit security utm feature-profile web-filtering]
user@host# set url-whitelist custwhitelist
```
3. Specify the Web filtering type, create a profile name, and set the server name or IP address.  

```
[edit security utm feature-profile web-filtering]
user@host# set websense-redirect profile websenseprofile1 server host
Websenseserver
```
4. Enter the port number for communicating with the server.  

```
[edit security utm feature-profile web-filtering]
user@host# set websense-redirect profile websenseprofile1 server port 15868
```
5. Select fallback settings (block or log and permit) for this profile.  

```
[edit security utm feature-profile web-filtering]
user@host# set websense-redirect profile websenseprofile1 fallback-settings default
block
```

```

user@host# set websense-redirect profile websenseprofile1 fallback-settings
server-connectivity block
user@host# set websense-redirect profile websenseprofile1 fallback-settings
timeout block
user@host# set websense-redirect profile websenseprofile1 fallback-settings
too-many-requests block

```

6. Enter the number of sockets used for communicating between the client and the server.

```

[edit security utm feature-profile web-filtering]
user@host# set websense-redirect profile websenseprofile1 sockets 1

```

7. Enter a timeout value, in seconds.

```

[edit security utm feature-profile web-filtering]
user@host# set .websense-redirect profile websenseprofile1 timeout 10

```

**Results** From configuration mode, confirm your configuration by entering the **show security utm feature-profile** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
userhost# show security utm feature-profile
web-filtering {
  url-whitelist custwhitelist;
  url-blacklist custblacklist;
  type websense-redirect {
    profile websenseprofile1 {
      server {
        host Websenseserver;
        port 15868;
      }
      fallback-settings {
        server-connectivity block;
        timeout block;
        too-many-requests block;
      }
      timeout 10;
      sockets 1;
    }
  }
}
content-filtering {
  profile contentfilter1;
}

```

If you are done configuring the device, enter **commit** from configuration mode.

### Configuring Redirect Web Filtering UTM Policies and Attaching the Redirect Web Filtering UTM Policies to Security Policies

#### CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm utm-policy utmp6 web-filtering http-profile websenseprofile1
set security policies from-zone trust to-zone untrust policy p6 match source-address any
set security policies from-zone trust to-zone untrust policy p6 match destination-address
  any
set security policies from-zone trust to-zone untrust policy p6 match application junos-http
set security policies from-zone trust to-zone untrust policy p6 then permit
  application-services utm-policy utmp6
```

**Step-by-Step  
Procedure**

To configure a UTM policy and attach it to a security policy:

1. Create the UTM policy referencing a profile.  

```
[edit security utm]
user@host# set utm-policy utmp6 web-filtering http-profile websenseprofile1
```
2. Create and configure the security policy.  

```
[edit security policies from-zone trust to-zone untrust policy p6]
user@host# set match source-address any
user@host# set match destination-address any
user@host# set match application junos-http
```
3. Attach the UTM policy to the security policy.  

```
[edit security policies from-zone trust to-zone untrust policy p6]
user@host# set then permit application-services utm-policy utmp6
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost# show security utm
utm-policy utmp6 {
  web-filtering {
    http-profile websenseprofile1;
  }
}
```

From configuration mode, confirm your configuration by entering the **show security policies** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost# show security policies
from-zone trust to-zone untrust {
  policy p6 {
    match {
      source-address any;
      destination-address any;
      application junos-http;
    }
    then {
      permit {
        application-services {
          utm-policy utmp6;
        }
      }
    }
  }
}
```

```

    }
  }
}

```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying the Configuration of Redirect Web Filtering Custom Objects on page 127](#)
- [Verifying the Configuration of Redirect Web Filtering Feature Profiles on page 127](#)
- [Verifying the Attachment of Redirect Web Filtering UTM Policies to Security Policies on page 128](#)

### Verifying the Configuration of Redirect Web Filtering Custom Objects

<b>Purpose</b>	Verify the configuration of redirect Web filtering custom objects.
<b>Action</b>	<p>From the top of the configuration in configuration mode, enter the <b>show security utm custom-objects</b> command.</p> <pre> [edit] userhost# show security utm custom-objects url-pattern {   urllist4 {     value [ http://www.example.net 1.2.3.4 ];   }   urllistblack {     value [ http://www.untrusted.com 13.13.13.13 ];   }   urllistwhite {     value [ http://www.trusted.com 7.7.7.7 ];   } } custom-url-category {   custurl4 {     value urllist4;   }   custblacklist {     value urllistblack;   }   custwhitelist {     value urllistwhite;   } } </pre>
<b>Meaning</b>	The sample output shows the list of custom objects created.

### Verifying the Configuration of Redirect Web Filtering Feature Profiles

<b>Purpose</b>	Verify the configuration of redirect Web filtering feature profiles.
----------------	--

**Action** From the top of the configuration in configuration mode, enter the **show security utm feature-profile** command.

```
[edit]
userhost# show security utm feature-profile
web-filtering {
  url-whitelist custwhitelist;
  url-blacklist custblacklist;
  type websense-redirect {
    profile websenseprofile1 {
      server {
        host Websenseserver;
        port 15868;
      }
      fallback-settings {
        server-connectivity block;
        timeout block;
        too-many-requests block;
      }
      timeout 10;
      sockets 1;
    }
  }
}
content-filtering {
  profile contentfilter1;
}
```

**Meaning** The sample output shows the feature profile configured for a Websense redirect server.

---

### Verifying the Attachment of Redirect Web Filtering UTM Policies to Security Policies

---

**Purpose** Verify the attachment of the newly created redirect Web filtering UTM policies to the security policies.

**Action** From the top of the configuration in configuration mode, enter the **show security utm** and **show security policies** commands.

```
[edit]
userhost# show security utm
utm-policy utmp6 {
  web-filtering {
    http-profile websenseprofile1;
  }
}

[edit]
userhost# show security policies
from-zone trust to-zone untrust {
  policy p6 {
    match {
      source-address any;
      destination-address any;
```

```

        application junos-http;
    }
    then {
        permit {
            application-services {
                utm-policy utmp6;
            }
        }
    }
}

```

**Meaning** The sample output shows the security policies to which the newly created redirect Web filtering UTM policies are attached.

- Related Documentation**
- [Web Filtering Overview on page 89](#)
  - [Understanding Local Web Filtering on page 112](#)
  - [web-filtering on page 255](#)
  - [Understanding Redirect Web Filtering on page 120](#)

## Monitoring Web Filtering Configurations

**Purpose** View Web-filtering statistics.

**Action** To view Web-filtering statistics using the CLI, enter the following commands:

```

user@host> show security utm web-filtering status
user@host> show security utm web-filtering statistics

```

To view Web-filtering statistics using J-Web:

1. Select **Clear Web Filtering Statistics**.

The following information is displayed in the right pane.

```

Total Requests: #
White List Hit: #
Black List Hit: #
Queries to Server: #
Server Reply Permit: #
Server Reply Block: #
Custom Category Permit: #
Custom Category Block: #
Cache Hit Permit: #
Cache Hit Block: #
Web Filtering Session Total: #
Web Filtering Session Inuse: #
Fall Back: Log-and-Permit Block
Default # #
Timeout # #
Server-Connectivity # #
Too-Many-Requests # #

```

2. You can click the **Clear Web Filtering Statistics** button to clear all current viewable statistics and begin collecting new statistics.

**Related  
Documentation**

- [Web Filtering Overview](#)
- [Example: Configuring Local Web Filtering](#)

## PART 6

# Configuration Statements and Operational Commands

- Configuration Statements on page 133
- Operational Commands on page 257



## CHAPTER 12

# Configuration Statements

- [action \(Security UTM Web Filtering\) on page 138](#)
- [address-blacklist on page 138](#)
- [address-whitelist on page 138](#)
- [admin-email on page 139](#)
- [administrator-email \(Security Fallback Block\) on page 139](#)
- [administrator-email \(Security Virus Detection\) on page 139](#)
- [allow-email \(Security Fallback Block\) on page 140](#)
- [allow-email \(Security Virus Detection\) on page 140](#)
- [application \(Security Policies\) on page 141](#)
- [application-proxy \(Security UTM\) on page 142](#)
- [anti-spam \(Security Feature Profile\) on page 142](#)
- [anti-spam \(Security UTM Policy\) on page 143](#)
- [anti-virus \(Security Feature Profile\) on page 144](#)
- [anti-virus \(Security UTM Policy\) on page 146](#)
- [block-command on page 146](#)
- [block-content-type on page 147](#)
- [block-extension on page 147](#)
- [block-message \(Security UTM\) on page 148](#)
- [block-mime on page 148](#)
- [cache on page 149](#)
- [category \(Security Logging\) on page 150](#)
- [category \(Security Web Filtering\) on page 151](#)
- [content-filtering \(Security Feature Profile\) on page 157](#)
- [content-filtering \(Security UTM Policy\) on page 158](#)
- [content-size \(Security Antivirus Sophos Engine\) on page 159](#)
- [content-size-limit on page 160](#)
- [custom-block-message on page 160](#)
- [custom-message \(Security Content Filtering\) on page 160](#)

- [custom-message \(Security Email Notify\) on page 161](#)
- [custom-message \(Security Fallback Block\) on page 161](#)
- [custom-message \(Security Fallback Non-Block\) on page 161](#)
- [custom-message \(Security Virus Detection\) on page 162](#)
- [custom-message-subject \(Security Email Notify\) on page 162](#)
- [custom-message-subject \(Security Fallback Block\) on page 162](#)
- [custom-message-subject \(Security Fallback Non-Block\) on page 163](#)
- [custom-message-subject \(Security Virus Detection\) on page 163](#)
- [custom-objects on page 164](#)
- [custom-tag-string on page 164](#)
- [custom-url-category on page 165](#)
- [default \(Security Antivirus Sophos Engine\) on page 166](#)
- [default \(Security UTM\) on page 166](#)
- [default \(Security Web Filtering\) on page 167](#)
- [display-host \(Security Fallback Block\) on page 167](#)
- [display-host \(Security Virus Detection\) on page 168](#)
- [download-profile \(Security Antivirus FTP\) on page 168](#)
- [download-profile \(Security Content Filtering FTP\) on page 168](#)
- [email-notify on page 169](#)
- [engine-not-ready \(Security Antivirus Sophos Engine\) on page 169](#)
- [exception \(Security Antivirus Mime Whitelist\) on page 170](#)
- [exception \(Security Content Filtering\) on page 170](#)
- [fallback-block \(Security Antivirus\) on page 171](#)
- [fallback-non-block \(Security Antivirus\) on page 171](#)
- [fallback-options \(Security Antivirus Sophos Engine\) on page 172](#)
- [fallback-settings \(Security Web Filtering\) on page 172](#)
- [fallback-settings \(Security Web Filtering Juniper Local\) on page 173](#)
- [fallback-settings \(Security Web Filtering Websense Redirect\) on page 173](#)
- [feature-profile on page 174](#)
- [filename-extension on page 177](#)
- [flag \(SMTP\) on page 178](#)
- [format \(Security Log Stream\) on page 179](#)
- [from-zone \(Security Policies\) on page 180](#)
- [ftp \(UTM Policy Anti-Virus\) on page 182](#)
- [ftp \(UTM Policy Content Filtering\) on page 183](#)
- [host \(Security Web Filtering\) on page 183](#)
- [http-profile \(Security Antivirus\) on page 184](#)

- [http-profile \(Security Content Filtering\)](#) on page 184
- [http-profile \(Security Web Filtering\)](#) on page 184
- [imap-profile \(Security UTM Policy Antivirus\)](#) on page 185
- [imap-profile \(Security UTM Policy Content Filtering\)](#) on page 185
- [interval \(Security Antivirus\)](#) on page 186
- [ipc](#) on page 187
- [juniper-local](#) on page 188
- [limit \(UTM Policy\)](#) on page 188
- [list \(Security Antivirus Mime Whitelist\)](#) on page 189
- [list \(Security Content Filtering Block Mime\)](#) on page 189
- [log \(Security\)](#) on page 190
- [mime-pattern](#) on page 193
- [mime-whitelist](#) on page 194
- [no-autoupdate](#) on page 195
- [no-notify-mail-recipient](#) on page 195
- [no-notify-mail-sender \(Security Content Filtering Notification Options\)](#) on page 196
- [no-notify-mail-sender \(Security Fallback Block\)](#) on page 196
- [no-notify-mail-sender \(Security Virus Detection\)](#) on page 197
- [no-sbl-default-server](#) on page 197
- [notification-options \(Security Antivirus\)](#) on page 198
- [notification-options \(Security Content Filtering\)](#) on page 199
- [notify-mail-recipient](#) on page 199
- [notify-mail-sender \(Security Content Filtering Notification Options\)](#) on page 200
- [notify-mail-sender \(Security Fallback Block\)](#) on page 200
- [notify-mail-sender \(Security Virus Detection\)](#) on page 201
- [no-uri-check](#) on page 201
- [out-of-resources \(Security Antivirus Sophos Engine\)](#) on page 202
- [over-limit](#) on page 202
- [packet-filter](#) on page 203
- [password \(Security Antivirus\)](#) on page 204
- [pattern-update \(Security Antivirus\)](#) on page 204
- [permit-command](#) on page 205
- [policies](#) on page 206
- [pop3-profile \(Security UTM Policy Antivirus\)](#) on page 210
- [pop3-profile \(Security UTM Policy Content Filtering\)](#) on page 210
- [port \(Security Antivirus\)](#) on page 211
- [port \(Security Web Filtering Server\)](#) on page 211

- [primary-server](#) on page 212
- [profile \(Security Antispam SBL\)](#) on page 212
- [profile \(Security Content Filtering\)](#) on page 213
- [profile \(Security Sophos Engine Antivirus\)](#) on page 214
- [profile \(Security Web Filtering Juniper Enhanced\)](#) on page 215
- [profile \(Security Web Filtering Juniper Local\)](#) on page 216
- [profile \(Security Web Filtering Websense Redirect\)](#) on page 217
- [protocol-command](#) on page 218
- [proxy \(Security Antivirus\)](#) on page 218
- [quarantine-message \(Security UTM\)](#) on page 219
- [sbl](#) on page 219
- [sbl-default-server](#) on page 220
- [scan-options \(Security Antivirus Sophos Engine\)](#) on page 220
- [secondary-server](#) on page 221
- [server \(Security Antivirus\)](#) on page 221
- [server \(Security Web Filtering\)](#) on page 222
- [server-connectivity](#) on page 222
- [sessions-per-client](#) on page 223
- [site-reputation-action](#) on page 224
- [size \(Security Web Filtering Cache\)](#) on page 224
- [smtp-profile \(Security UTM Policy Antispam\)](#) on page 225
- [smtp-profile \(Security UTM Policy Antivirus\)](#) on page 225
- [smtp-profile \(Security UTM Policy Content Filtering\)](#) on page 225
- [sockets](#) on page 226
- [sophos-engine](#) on page 227
- [spam-action](#) on page 228
- [sxl-retry](#) on page 229
- [sxl-timeout](#) on page 229
- [timeout \(Security Antivirus Fallback Options Sophos Engine\)](#) on page 230
- [timeout \(Security Antivirus Scan Options\)](#) on page 230
- [timeout \(Security Web Filtering\)](#) on page 231
- [timeout \(Security Web Filtering Cache\)](#) on page 231
- [timeout \(Security Web Filtering Fallback Settings\)](#) on page 232
- [too-many-requests \(Security Antivirus Fallback Options Sophos Engine\)](#) on page 232
- [too-many-requests \(Security Web Filtering Fallback Settings\)](#) on page 233
- [to-zone \(Security Policies\)](#) on page 234
- [traceoptions \(Security Antispam\)](#) on page 236

- [traceoptions \(Security Antivirus\) on page 237](#)
- [traceoptions \(Security Application Proxy\) on page 238](#)
- [traceoptions \(Security Content Filtering\) on page 239](#)
- [traceoptions \(Security UTM\) on page 239](#)
- [traceoptions \(Security Web Filtering\) on page 240](#)
- [traceoptions \(SMTP\) on page 241](#)
- [traffic-options on page 241](#)
- [trickling on page 242](#)
- [type \(Security Antivirus Feature Profile\) on page 242](#)
- [type \(Security Content Filtering Notification Options\) on page 243](#)
- [type \(Security Fallback Block\) on page 243](#)
- [type \(Security Virus Detection\) on page 244](#)
- [upload-profile \(Security Antivirus FTP\) on page 244](#)
- [upload-profile \(Security Content Filtering FTP\) on page 244](#)
- [uri-check on page 245](#)
- [url \(Security Antivirus\) on page 245](#)
- [url-blacklist on page 245](#)
- [url-pattern on page 246](#)
- [url-whitelist \(Security Antivirus\) on page 246](#)
- [url-whitelist \(Security Web Filtering\) on page 247](#)
- [username \(Security Antivirus\) on page 247](#)
- [utm on page 248](#)
- [utm-policy on page 253](#)
- [utm-policy \(Application Services\) on page 254](#)
- [virus-detection \(Security Antivirus\) on page 254](#)
- [web-filtering on page 255](#)
- [websense-redirect on page 256](#)

## action (Security UTM Web Filtering)

---

<b>Syntax</b>	action (block   log-and-permit   permit   quarantine);
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> category <i>customurl-last-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Statement introduced in Junos OS Release 11.4 for UTM Enhanced Web Filtering.
<b>Description</b>	Enter an action to go with the customurl-list filter.
<b>Options</b>	<ul style="list-style-type: none"><li>• block—Log the error and deny the traffic.</li><li>• log-and-permit—Log the error and permit the traffic.</li><li>• permit—Permit the traffic.</li><li>• quarantine—Show the warning message and permit/block the traffic based on user input.</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## address-blacklist

---

<b>Syntax</b>	address-blacklist <i>list-name</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-spam]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Enter an address blacklist (or whitelist) custom object for local list spam filtering.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## address-whitelist

---

<b>Syntax</b>	address-whitelist <i>list-name</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-spam]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Enter an address-whitelist (or blacklist) custom-object for local list spam filtering.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## admin-email

---

<b>Syntax</b>	admin-email <i>email-address</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine pattern-update email-notify]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	You can configure the device to notify a specified administrator when patterns are updated. This is an e-mail notification with a custom message and a custom subject line.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## administrator-email (Security Fallback Block)

---

<b>Syntax</b>	administrator-email <i>email-address</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options fallback-block]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	Configure the administrator e-mail address that will be notified when a fallback-block occurs. This is an e-mail notification with a custom message and a custom subject line.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## administrator-email (Security Virus Detection)

---

<b>Syntax</b>	administrator-email <i>email address</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile name</i> notification-options virus-detection]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 .
<b>Description</b>	Configure the administrator e-mail address that will be notified when a virus is detected by Sophos antivirus. This is an e-mail notification with a custom message and a custom subject line.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## allow-email (Security Fallback Block)

---


<b>Syntax</b>	allow-email;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options fallback-block]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	Enable e-mail notification to notify a specified administrator when a fallback-block occurs.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## allow-email (Security Virus Detection)

---

<b>Syntax</b>	allow-email;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus profile notification-options virus-detect]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 .
<b>Description</b>	Enable e-mail notification to notify a specified administrator when a virus is detected.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## application (Security Policies)

<b>Syntax</b>	<pre> application {     [application];     any; } </pre>
<b>Hierarchy Level</b>	<p>[edit security policies from-zone <i>zone-name</i> to-zone <i>zone-name</i> policy <i>policy-name</i> match]</p> <p>[edit security policies global policy <i>policy-name</i> match]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5.
<b>Description</b>	Specify the IP or remote procedure call (RPC) application or set of applications to be used as match criteria.
<b>Options</b>	<p><b><i>application-name-or-set</i></b>—Name of the predefined or custom application or application set used as match criteria.</p> <p><b><i>any</i></b>—Any predefined or custom applications or application sets.</p>
<div style="display: flex; align-items: center;">  <div> <p><b>NOTE:</b> A custom application that does not use a well-known destination port for the application will not be included in the <i>any</i> option, and must be named explicitly.</p> </div> </div>	
<b>Required Privilege Level</b>	<p><b>security</b>—To view this statement in the configuration.</p> <p><b>security-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Security Policies Overview</i></li> </ul>

## application-proxy (Security UTM)

---

<b>Syntax</b>	<pre>application-proxy {   traceoptions {     flag <i>flag</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit security utm]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Configure trace options for the application proxy.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## anti-spam (Security Feature Profile)

---

<b>Syntax</b>	<pre>anti-spam {   address-blacklist <i>list-name</i>;   address-whitelist <i>list-name</i>;   sbl {     profile <i>profile-name</i> {       custom-tag-string [<i>string</i>];       (sbl-default-server   no-sbl-default-server);       spam-action (block   tag-header   tag-subject);     }   }   traceoptions flag <i>flag</i>; }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure UTM antispam features.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

---

## anti-spam (Security UTM Policy)

---

<b>Syntax</b>	anti-spam { smtp-profile <i>profile-name</i> ; }
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the antispam SMTP protocol and attach this policy to a security profile to implement it.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## anti-virus (Security Feature Profile)

```

Syntax  anti-virus {
        mime-whitelist {
            exception listname;
            list listname {
                exception listname;
            }
        }
        sophos-engine {
            pattern-update {
                email-notify {
                    admin-email email-address;
                    custom-message message;
                    custom-message-subject message-subject;
                }
                interval value;
                no-autoupdate;
                proxy {
                    password password-string;
                    port port-number;
                    server address-or-url;
                    username name;
                }
                url url;
            }
        }
        profile <name> {
            fallback-options {
                content-size (block | log-and-permit | permit);
                default (block | log-and-permit | permit);
                engine-not-ready (block | log-and-permit | permit);
                out-of-resources (block | log-and-permit | permit);
                timeout (block | log-and-permit | permit);
                too-many-requests (block | log-and-permit | permit);
            }
            notification-options {
                fallback-block {
                    administrator-email email-address;
                    allow-email;
                    custom-message message;
                    custom-message-subject message-subject;
                    display-host;
                    (notify-mail-sender | no-notify-mail-sender);
                    type (message | protocol-only);
                }
                fallback-non-block {
                    custom-message message;
                    custom-message-subject message-subject;
                    (notify-mail-recipient | no-notify-mail-recipient);
                }
            }
            virus-detection {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-sender | no-notify-mail-sender);
            }
        }
    }

```

```

        type (message | protocol-only);
    }
}
scan-options {
    content-size-limit value;
    (no-uri-check | uri-check);
    timeout value;
}
trickling {
    timeout value;
}
}
sxl-retry value;
sxl-timeout seconds;
}
traceoptions flag flag;
url-whitelist listname;
}

```

<b>Hierarchy Level</b>	[edit security utm feature-profile]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure UTM antivirus full features.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## anti-virus (Security UTM Policy)

---

<b>Syntax</b>	<pre>anti-virus {   ftp {     download-profile <i>profile-name</i>;     upload-profile <i>profile-name</i>;   }   http-profile <i>profile-name</i>;   imap-profile <i>profile-name</i>;   pop3-profile <i>profile-name</i>;   smtp-profile <i>profile-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the antivirus protocols and attach this policy to a security profile to implement it.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## block-command

---

<b>Syntax</b>	<pre>block-command <i>protocol-command-list</i>;</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile content-filtering profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Apply protocol block command custom-objects to the content-filtering profile.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## block-content-type

<b>Syntax</b>	block-content-type (activex   exe   http-cookie   java-applet   zip);
<b>Hierarchy Level</b>	[edit security utm feature-profile content-filtering profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Apply blocks to other available content such as exe, http-cookie, java-applet. This is for HTTP only.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>activex</b>—Block ActiveX.</li> <li>• <b>exe</b>—Block EXE files.</li> <li>• <b>http-cookie</b>—Block cookies.</li> <li>• <b>java-applet</b>—Block Java applets.</li> <li>• <b>zip</b>—Block ZIP files.</li> </ul>
<b>Required Privilege</b>	security—To view this statement in the configuration.
<b>Level</b>	security-control—To add this statement to the configuration.

## block-extension

<b>Syntax</b>	block-extension <i>extension-list</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile content-filtering profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Apply block extensions to the content-filtering profile.
<b>Required Privilege</b>	security—To view this statement in the configuration.
<b>Level</b>	security-control—To add this statement to the configuration.

## block-message (Security UTM)

---

<b>Syntax</b>	<pre>block-message {     type {         custom-redirect-url;     }     url <i>url</i>; }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	Configure Juniper enhanced block message settings.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>type</b>—Specify the following type of the block message:<ul style="list-style-type: none"><li>• <b>custom-redirect-url</b>—Specify Custom redirect URL server.</li></ul></li><li>• <b>url <i>url</i></b>—Specify an URL of the block message.</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## block-mime

---

<b>Syntax</b>	<pre>block-mime {     exception <i>list-name</i>;     list <i>list-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile content-filtering profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Apply MIME pattern list custom-objects to the content-filtering profile for blocking MIME types.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

---

## cache

---

<b>Syntax</b>	cache { size <i>value</i> ; timeout <i>value</i> ; }
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering juniper-enhanced]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	Set the cache parameters for Enhanced Web Filtering.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## category (Security Logging)

<b>Syntax</b>	category (all   content-security   fw-auth   screen   alg   nat   flow   sctp   gtp   ipsec   idp   rtlog   pst-ds-lite   appqos   secintel)
<b>Hierarchy Level</b>	[edit security log stream <i>stream-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0. Statement modified in Junos OS Release 15.1X49-D40.
<b>Description</b>	Set the category of logging to <b>all</b> or <b>content-security</b> . Note that for the WELF format, the category must be set to <b>content-security</b> .



**NOTE:** On SRX5600 and SRX5800 devices, if the stream configuration does not specify a destination port, the default destination port will be the system log port. If you specify a destination port in the stream configuration, then that port will be used instead.

<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>all</b>—All events are logged.</li> <li>• <b>content-security</b>—Only content security events are logged.</li> <li>• <b>fw-auth</b>—Firewall authentication events are logged.</li> <li>• <b>screen</b>—Screen events are logged.</li> <li>• <b>alg</b>—Application Layer Gateway (ALG) events are logged.</li> <li>• <b>nat</b>—Network Address Translation (NAT) events are logged.</li> <li>• <b>flow</b>—Flow events are logged.</li> <li>• <b>sctp</b>—Stream Control Transmission Protocol (SCTP) events are logged.</li> <li>• <b>gtp</b>—GTP events are logged.</li> <li>• <b>ipsec</b>—IPsec events are logged.</li> <li>• <b>idp</b>—Intrusion Detection and Prevention (IDP) events are logged.</li> <li>• <b>rtlog</b>—RTLOG system log events are logged.</li> <li>• <b>pst-ds-lite</b>—PST dual-stack lite (DS-Lite) events are logged.</li> <li>• <b>appqos</b>—Application quality of service (AppQoS) events are logged.</li> <li>• <b>secintel</b>—Juniper Networks Security Intelligence (SecIntel) events are logged.</li> </ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>AppSecure Services Feature Guide for Security Devices</i></li> <li>• <i>Logical Systems Feature Guide for Security Devices</i></li> </ul>

## category (Security Web Filtering)

---

<b>Syntax</b>	<code>category <i>customurl-list name</i> {     action (block   log-and-permit   permit   quarantine); }</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering. Support for new categories and category name updates by Websense added in Junos OS Release 12.1X47-D15 and 12.3X48-D10.
<b>Description</b>	Select a custom URL category list you created (custom objects) for filtering against.

Table 4: List of Categories Predefined by Websense

Category ID	Category Name	Parent ID
1	Adult Material	0
2	Business and Economy	0
3	Education	0
4	Government	0
5	News and Media	0
6	Religion	0
7	Society and Lifestyles	0
8	Special Events	0
9	Information Technology	0
10	Abortion	0
11	Advocacy Groups	0
12	Entertainment	0
13	Gambling	0
14	Games	0
15	Illegal or Questionable	0
16	Job Search	0
17	Shopping	0
18	Sports	0
19	Tasteless	0
20	Travel	0
21	Vehicles	0
22	Violence	0
23	Weapons	0
24	Drugs	0

Table 4: List of Categories Predefined by Websense (*continued*)

Category ID	Category Name	Parent ID
25	Militancy and Extremist	0
26	Intolerance	0
27	Health	0
28	Website Translation	9
29	Advertisements	110
64	User-Defined	0
65	Nudity	1
66	Adult Content	1
67	Sex	1
68	Financial Data and Services	2
69	Cultural Institutions	3
70	Media File Download	12
72	Military	4
73	Political Organizations	4
74	General Email	91
75	Proxy Avoidance	9
76	Search Engines and Portals	9
78	Web Hosting	9
79	Web Chat	91
80	Hacking	9
81	Alternative Journals	5
82	Non-Traditional Religions	6
83	Traditional Religions	6
84	Restaurants and Dining	7

Table 4: List of Categories Predefined by Websense (*continued*)

Category ID	Category Name	Parent ID
85	Gay or Lesbian or Bisexual Interest	7
86	Personals and Dating	7
87	Alcohol and Tobacco	7
88	Prescribed Medications	24
89	Nutrition	24
90	Abused Drugs	24
91	Internet Communication	0
92	Pro-Choice	10
93	Pro-Life	10
94	Sex Education	1
95	Lingerie and Swimsuit	1
96	Online Brokerage and Trading	110
97	Educational Institutions	3
98	Instant Messaging	110
99	Application and Software Download	110
100	Pay-to-Surf	110
101	Internet Auctions	17
102	Real Estate	17
103	Hobbies	7
107	Sport Hunting and Gun Clubs	18
108	Internet Telephony	116
109	Streaming Media	116
110	Productivity	0
111	Marijuana	24

Table 4: List of Categories Predefined by Websense (*continued*)

Category ID	Category Name	Parent ID
112	Message Boards and Forums	110
113	Personal Network Storage and Backup	116
114	Internet Radio and TV	116
115	Peer-to-Peer File Sharing	116
116	Bandwidth	0
117	Social Networking and Personal Sites	7
118	Educational Materials	3
121	Reference Materials	3
122	Social Organizations	0
123	Service and Philanthropic Organizations	122
124	Social and Affiliation Organizations	122
125	Professional and Worker Organizations	122
126	Security	0
128	Malicious Web Sites	126
138	Computer Security	9
146	Miscellaneous	0
147	Web Infrastructure	146
148	Web Images	146
149	Private IP Addresses	146
150	Content Delivery Networks	146
151	Dynamic Content	146
152	Network Errors	146
153	Uncategorized	146
154	Spyware	126

Table 4: List of Categories Predefined by Websense (*continued*)

Category ID	Category Name	Parent ID
156	File Download Servers	146
164	Phishing and Other Frauds	126
166	Keyloggers	126
167	Potentially Unwanted Software	126
172	Bot Networks	126
191	Extended Protection	0
192	Elevated Exposure	191
193	Emerging Exploits	191
194	Suspicious Content	191
195	Organizational Email	91
196	Text and media messaging	91
200	Web and Email Spam	9
220	Compromised Websites	0
221	Newly Registered Websites	0
222	Collaboration Office	0
223	Office Mail	222
224	Office Drive	222
225	Office Documents	222
226	Office Apps	222
227	Web Analytics	9
228	Web and Email Marketing	9
1529	Classifieds Posting	0
1530	Blog Posting	0
1531	Blog Commenting	0

**Options** The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege** security—To view this statement in the configuration.  
**Level** security-control—To add this statement to the configuration.

## content-filtering (Security Feature Profile)

**Syntax**

```
content-filtering {
  profile profile-name {
    block-command protocol-command-list;
    block-content-type (activex | exe | http-cookie | java-applet | zip);
    block-extension extension-list;
    block-mime {
      exception list-name;
      list list-name;
    }
    notification-options {
      custom-message message;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
    permit-command protocol-command-list;
  }
  traceoptions flag flag;
}
```

**Hierarchy Level** [edit security utm feature-profile]

**Release Information** Statement introduced in Junos OS Release 9.5 .

**Description** Configure UTM content-filtering features.

**Options** The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege** security—To view this statement in the configuration.  
**Level** security-control—To add this statement to the configuration.

## content-filtering (Security UTM Policy)

---

**Syntax**    content-filtering {  
              ftp {  
                  download-profile *profile-name*;  
                  upload-profile *profile-name*;  
              }  
              http-profile *profile-name*;  
              imap-profile *profile-name*;  
              pop3-profile *profile-name*;  
              smtp-profile *profile-name*;  
          }

**Hierarchy Level**    [edit security utm utm-policy *policy-name*]

**Release Information**    Statement introduced in Junos OS Release 9.5 .

**Description**    Configure a UTM policy for the content-filtering protocols and attach this policy to a security profile to implement it.

**Options**    The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege**    security—To view this statement in the configuration.  
**Level**    security-control—To add this statement to the configuration.

## content-size (Security Antivirus Sophos Engine)

<b>Syntax</b>	content-size (block   log-and-permit   permit);
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> fallback-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 .
<b>Description</b>	If the content size exceeds a set limit, the content is either passed or blocked.



**NOTE:** When you configure the content-size value, keep in mind that in certain cases, content size is available in the protocol headers, so the max-content-size fallback is applied before a scan request is sent. However, in many cases, content size is not provided in the protocol headers. In these cases, the TCP payload is sent to the antivirus scanner and accumulates until the end of the payload. If the accumulated payload exceeds the maximum content size value, then max-content-size fallback is applied. You might want to set the fallback action to block, in which case such a packet is dropped and a block message is sent to the client.

<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>block</b>—Log the error and deny the traffic</li> <li>• <b>log-and-permit</b>—Log the error and permit the traffic</li> <li>• <b>permit</b>—Permit the traffic</li> </ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Sophos Antivirus Configuration Overview on page 48</a></li> </ul>

## content-size-limit

---

<b>Syntax</b>	content-size-limit <i>value</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> scan-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	<p>The content size check occurs before the scan request is sent. The content size refers to accumulated TCP payload size.</p> <p>Range: 20 through 20,000</p>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## custom-block-message

---

<b>Syntax</b>	custom-block-message <i>value</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	Enter a custom message to be sent when HTTP requests are blocked.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## custom-message (Security Content Filtering)

---

<b>Syntax</b>	custom-message <i>message</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile content-filtering profile <i>profile-name</i> notification-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Custom message notifications are generally used when content is blocked by the content filter.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Content Filtering Overview on page 71</a></li></ul>

## custom-message (Security Email Notify)

---

<b>Syntax</b>	custom-message <i>message</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine pattern-update email-notify]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
<b>Description</b>	You can configure the device to notify a specified administrator when patterns are updated. This is an e-mail notification with a custom message.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## custom-message (Security Fallback Block)

---

<b>Syntax</b>	custom-message <i>message</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options fallback-block]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## custom-message (Security Fallback Non-Block)

---

<b>Syntax</b>	custom-message <i>message</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options fallback-non-block]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## custom-message (Security Virus Detection)

---

<b>Syntax</b>	custom-message <i>message</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options virus-detection]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## custom-message-subject (Security Email Notify)

---

<b>Syntax</b>	custom-message-subject <i>message-subject</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine pattern-update email-notify]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
<b>Description</b>	You can configure the device to notify a specified administrator when patterns are updated. This is an e-mail notification with a custom message and a custom subject line.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## custom-message-subject (Security Fallback Block)

---

<b>Syntax</b>	custom-message-subject <i>message-subject</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options fallback-block]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. As part of a custom message, you can customize the message subject line.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## custom-message-subject (Security Fallback Non-Block)

---

<b>Syntax</b>	custom-message-subject <i>message-subject</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options fallback-non-block]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. As part of a custom message, you can customize the message subject line.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## custom-message-subject (Security Virus Detection)

---

<b>Syntax</b>	custom-message-subject <i>message-subject</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options virus-detection]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. As part of a custom message, you can customize the message subject line.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## custom-objects

<b>Syntax</b>	<pre> custom-objects {   custom-url-category <i>object-name</i> {     value [<i>value</i>];   }   filename-extension <i>object-name</i> {     value [<i>value</i>];   }   mime-pattern <i>object-name</i> {     value [<i>value</i>];   }   protocol-command <i>object-name</i> {     value [<i>value</i>];   }   url-pattern <i>object-name</i> {     value [<i>value</i>];   } } </pre>
<b>Hierarchy Level</b>	[edit security utm]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Configure custom objects before configuring UTM feature-profile features.



**WARNING:** Custom category does not take precedence over predefined categories when it has the same name as one of the predefined categories. We do not recommend having a custom category name be the same as the predefined category name.

<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## custom-tag-string

<b>Syntax</b>	custom-tag-string [ <i>string</i> ];
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-spam sbl profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Configure a custom string for identifying a message as spam.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## custom-url-category

---

<b>Syntax</b>	<code>custom-url-category <i>object-name</i> {     value [<i>value</i>]; }</code>
<b>Hierarchy Level</b>	[edit security utm custom-objects]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Use URL pattern lists to create Custom URL category lists. These are lists of patterns that bypass scanning.



**WARNING:** Custom category does not take precedence over predefined categories when it has the same name as one of the predefined categories. We do not recommend having a custom category name be the same as the predefined category name.

<b>Options</b>	<ul style="list-style-type: none"> <li>• <b><i>object-name</i></b>—Name of the URL category-list object.</li> <li>• <b><i>value value</i></b>—Value of the URL category-list object. You can configure multiple values separated by spaces and enclosed in square brackets.</li> </ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Understanding UTM Custom Objects on page 4</a></li> </ul>

## default (Security Antivirus Sophos Engine)

---

<b>Syntax</b>	default (block   log-and-permit   permit);
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> fallback-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 .
<b>Description</b>	All errors other than those specifically listed fall into this category. This could include either unhandled system exceptions (internal errors) or other unknown errors.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>block</b>—Log the error and deny the traffic</li><li>• <b>log-and-permit</b>—Log the error and permit the traffic</li><li>• <b>permit</b>—Permit the traffic</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## default (Security UTM)

---

<b>Syntax</b>	default (block  log-and-permit   permit);
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4 .
<b>Description</b>	Specify the default action to take for a URL.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>block</b>—Log the error and deny the traffic.</li><li>• <b>log-and-permit</b>—Log the error and permit the traffic.</li><li>• <b>permit</b>—Permit the traffic.</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## default (Security Web Filtering)

<b>Syntax</b>	default (block   log-and-permit   permit   quarantine);
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering websense-redirect profile <i>profile-name</i> fallback-settings] [edit security utm feature-profile web-filtering juniper-local profile <i>profile-name</i> fallback-settings] [edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> fallback-settings]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	Specify an action for the profile, for requests that experience internal errors in the Web-filtering module.
<b>Options</b>	<ul style="list-style-type: none"> <li>• block—Log the error and deny the traffic.</li> <li>• log-and-permit—Log the error and permit the traffic.</li> <li>• permit —Permit the traffic.</li> <li>• quarantine—Show the warning message and permit/block the traffic based on user input.</li> </ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## display-host (Security Fallback Block)

<b>Syntax</b>	display-host;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options fallback-block]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	Display the computer host name in the notification e-mail sent to the administrator when a fallback-block notification occurs.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## display-host (Security Virus Detection)

---

<b>Syntax</b>	display-host;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus profile <i>profile name</i> notification-options virus-detection]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 .
<b>Description</b>	Display the computer host name in the notification e-mail sent to the administrator when a virus is detected by Sophos antivirus.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## download-profile (Security Antivirus FTP)

---

<b>Syntax</b>	download-profile <i>profile-name</i> ;
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> anti-virus ftp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the antivirus FTP (download) protocol and attach this policy to a security profile to implement it.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## download-profile (Security Content Filtering FTP)

---

<b>Syntax</b>	download-profile <i>profile-name</i> ;
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> content-filtering ftp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the content-filtering FTP (download) protocol and attach this policy to a security profile to implement it.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Content Filtering Overview on page 71</a></li></ul>

## email-notify

<b>Syntax</b>	email-notify { admin-email <i>email-address</i> ; custom-message <i>message</i> ; custom-message-subject <i>message-subject</i> ; }
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine pattern-update]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	You can configure the device to notify a specified administrator when patterns are updated. This is an e-mail notification with a custom message and a custom subject line.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## engine-not-ready (Security Antivirus Sophos Engine)

<b>Syntax</b>	default (block   log-and-permit   permit);
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> fallback-options]
<b>Release Information</b>	Statement introduced in Release 11.1 .
<b>Description</b>	The scan engine is initializing itself, for example, loading the signature database. During this phase, it is not ready to scan a file. A file could either pass or be blocked according to this setting.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>block</b>—Log the error and deny the traffic</li> <li>• <b>log-and-permit</b>—Log the error and permit the traffic</li> <li>• <b>permit</b>—Permit the traffic</li> </ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Sophos Antivirus Configuration Overview on page 48</a></li> </ul>

## exception (Security Antivirus Mime Whitelist)

---

<b>Syntax</b>	<code>exception <i>listname</i>;</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus mime-whitelist] [edit security utm feature-profile anti-virus mime-whitelist list <i>listname</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Configure the antivirus scanner to use an exception list to the MIME bypass list (custom objects). To use the exception list, you first create a whitelist custom-object list with the <b>list</b> statement. The system will first look at any existing whitelist mime pattern. If it matches an item, it will then continue to look for any exceptions to the whitelist and will then scan any item in the exception list.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## exception (Security Content Filtering)

---

<b>Syntax</b>	<code>exception <i>list-name</i>;</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile content-filtering profile <i>profile-name</i> block-mime]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure the content filter to use an exception list to the MIME block list (custom objects).
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Content Filtering Overview on page 71</a></li></ul>

## fallback-block (Security Antivirus)

<b>Syntax</b>	<pre> fallback-block {   administrator-email <i>email-address</i>;   allow-email;   custom-message <i>message</i>;   custom-message-subject <i>message-subject</i>;   display-host;   (notify-mail-sender   no-notify-mail-sender);   type (message   protocol-only); }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	Configure notifications for fallback blocking actions. Fallback options tell the system how to handle the errors returned by either the scan engine or the scan manager.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## fallback-non-block (Security Antivirus)

<b>Syntax</b>	<pre> fallback-non-block {   custom-message <i>message</i>;   custom-message-subject <i>message-subject</i>;   (notify-mail-recipient   no-notify-mail-recipient); }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	Configure notifications for fallback nonblocking actions.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## fallback-options (Security Antivirus Sophos Engine)

---

<b>Syntax</b>	<pre>fallback-options {   content-size (block   log-and-permit   permit);   default (block   log-and-permit   permit);   engine-not-ready (block   log-and-permit   permit);   out-of-resources (block   log-and-permit   permit);   timeout (block   log-and-permit   permit);   too-many-requests (block   log-and-permit   permit); }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 .
<b>Description</b>	Configure fallback options to instruct the system how to handle errors.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Sophos Antivirus Configuration Overview on page 48</a></li></ul>

## fallback-settings (Security Web Filtering)

---

<b>Syntax</b>	<pre>fallback-settings {   default (block   log-and-permit);   server-connectivity (block   log-and-permit);   timeout (block   log-and-permit);   too-many-requests (block   log-and-permit); }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	Fallback settings tell the system how to handle errors.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## fallback-settings (Security Web Filtering Juniper Local)

<b>Syntax</b>	<pre>fallback-settings {   default (block   log-and-permit);   server-connectivity (block   log-and-permit);   timeout (block   log-and-permit);   too-many-requests (block   log-and-permit); }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering juniper-local profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0 .
<b>Description</b>	Fallback settings tell the system how to handle errors.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Web Filtering Overview on page 89</a></li> </ul>

## fallback-settings (Security Web Filtering Websense Redirect)

<b>Syntax</b>	<pre>fallback-settings {   default (block   log-and-permit);   server-connectivity (block   log-and-permit);   timeout (block   log-and-permit);   too-many-requests (block   log-and-permit); }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering websense-redirect profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Fallback settings tell the system how to handle errors.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Understanding Redirect Web Filtering on page 120</a></li> </ul>

## feature-profile

---

```
Syntax feature-profile {
  anti-spam {
    address-blacklist list-name;
    address-whitelist list-name;
    sbl {
      profile profile-name {
        custom-tag-string [string];
        (sbl-default-server | no-sbl-default-server);
        spam-action (block | tag-header | tag-subject);
      }
    }
    traceoptions flag flag;
  }
  anti-virus {
    mime-whitelist {
      exception listname;
      list listname {
        exception listname;
      }
    }
    sophos-engine {
      pattern-update {
        email-notify {
          admin-email email-address;
          custom-message message;
          custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
          password password-string;
          port port-number;
          server address-or-url;
          username name;
        }
        url url;
      }
      profile <name> {
        fallback-options {
          content-size (block | log-and-permit | permit);
          default (block | log-and-permit | permit);
          engine-not-ready (block | log-and-permit | permit);
          out-of-resources (block | log-and-permit | permit);
          timeout (block | log-and-permit | permit);
          too-many-requests (block | log-and-permit | permit);
        }
        notification-options {
          fallback-block {
            administrator-email email-address;
            allow-email;
            custom-message message;
            custom-message-subject message-subject;
          }
        }
      }
    }
  }
}
```

```

        display-host;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
    }
    fallback-non-block {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-recipient | no-notify-mail-recipient);
    }
    virus-detection {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
    }
}
scan-options {
    content-size-limit value;
    (no-uri-check | uri-check);
    timeout value;
}
trickling {
    timeout value;
}
}
sxl-retry value;
sxl-timeout seconds;
}
traceoptions flag flag;
url-whitelist listname;
}
content-filtering {
    profile profile-name {
        block-command protocol-command-list;
        block-content-type (activex | exe | http-cookie | java-applet | zip);
        block-extension extension-list;
        block-mime {
            exception list-name;
            list list-name;
        }
        notification-options {
            custom-message message;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
        permit-command protocol-command-list;
    }
    traceoptions flag flag;
}
web-filtering {
    url-whitelist custwhitelist;
    url-blacklist custblacklist;
    http-reassemble;
    type juniper-enhanced;
    juniper-enhanced {
        cache {

```

```

        timeout 1800;
        size 500;
    }
    server {
        host rp.cloud.threatseeker.com;
        port 80;
    }
    profile junos-wf-enhanced-default {
        category {
            Enhanced_Hacking {
                action log-and-permit;
            }
            Enhanced_Government {
                action quarantine;
            }
        }
        site-reputation-action {
            very-safe permit;
            moderately-safe log-and-permit;
            fairly-safe log-and-permit;
            harmful block;
            suspicious block;
        }
        default block;
        custom-block-message "****access denied ****";
        fallback-settings {
            default block;
            server-connectivity block;
            timeout block;
            too-many-requests block;
        }
        timeout 10;
        no-safe-search;
    }
    utm-policy mypolicy {
        web-filtering {
            http-profile my_ewfprofile01;
        }
    }
}

```

<b>Hierarchy Level</b>	[edit security utm]
<b>Release Information</b>	Statement introduced in Release 9.5 .
<b>Description</b>	Configure UTM features, antivirus, antispam, content-filtering, and web-filtering by creating feature profiles.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## filename-extension

---

<b>Syntax</b>	filename-extension <i>object-name</i> { value [ <i>value</i> ]; }
<b>Hierarchy Level</b>	[edit security utm custom-objects]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	When scanning content, you can use a file extension list to define a set of file extensions that are used in file extension scan mode (scan-by-extension).
<b>Options</b>	<ul style="list-style-type: none"><li>• <b><i>object-name</i></b>—Name of the extension-list object.</li><li>• <b><i>value value</i></b>—Value of the extension-list object. You can configure multiple values separated by spaces and enclosed in square brackets.</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## flag (SMTP)

---

<b>Syntax</b>	<pre>flag {     all;     configuration;     IPC;     protocol-exchange;     send-request; }</pre>
<b>Hierarchy Level</b>	[edit smtp traceoptions]
<b>Release Information</b>	Statement added in Junos OS Release 10.0.
<b>Description</b>	Set flag for the SMTP traceoptions.
<b>Options</b>	<p>The following flag options are supported:</p> <ul style="list-style-type: none"><li>• <b>IPC</b>—Trace interprocess communication.</li><li>• <b>all</b>—Trace everything.</li><li>• <b>configuration</b>—Trace configuration event.</li><li>• <b>protocol-exchange</b>—Trace SMTP protocol exchanges.</li><li>• <b>send-request</b>—Trace send mail request event.</li></ul>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">smtp-profile (Security UTM Policy Antispam) on page 225</a></li></ul>

## format (Security Log Stream)

---

<b>Syntax</b>	format (binary   sd-syslog   syslog   welf)
<b>Hierarchy Level</b>	[edit security log stream <i>stream-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0 . Updated in Junos OS Release 12.1 .
<b>Description</b>	Set the format for remote security message logging to <b>binary</b> , <b>syslog</b> (system log), <b>sd-syslog</b> (structured system log), or <b>welf</b> . Note that for the WELF format, the category must be set to <b>content-security</b> (see <a href="#">category (Security Logging)</a> ).
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>binary</b>—Binary encoded text to conserve resources.</li> <li>• <b>sd-syslog</b>—Structured system log file.</li> <li>• <b>syslog</b>—Traditional system log file.</li> <li>• <b>welf</b>—Web Trends Extended Log Format.</li> </ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>AppSecure Services Feature Guide for Security Devices</i></li> <li>• <i>Logical Systems Feature Guide for Security Devices</i></li> </ul>

## from-zone (Security Policies)

---

```
Syntax  from-zone zone-name to-zone zone-name {  
        policy policy-name {  
            description description;  
            match {  
                application {  
                    [application];  
                    any;  
                }  
                destination-address {  
                    [address];  
                    any;  
                    any-ipv4;  
                    any-ipv6;  
                }  
                source-address {  
                    [address];  
                    any;  
                    any-ipv4;  
                    any-ipv6;  
                }  
                source-identity {  
                    [role-name];  
                    any;  
                    authenticated-user;  
                    unauthenticated-user;  
                    unknown-user;  
                }  
                source-end-user-profile {  
                    profile-name;  
                }  
            }  
            scheduler-name scheduler-name;  
            then {  
                count {  
                    alarm {  
                        per-minute-threshold number;  
                        per-second-threshold number;  
                    }  
                }  
                deny;  
                log {  
                    session-close;  
                    session-init;  
                }  
                permit {  
                    application-services {  
                        application-firewall {  
                            rule-set rule-set-name;  
                        }  
                    }  
                    application-traffic-control {  
                        rule-set rule-set-name;  
                    }  
                }  
            }  
        }  
    }
```

```

    gprs-gtp-profile profile-name;
    gprs-sctp-profile profile-name;
    idp;
    redirect-wx | reverse-redirect-wx;
    ssl-proxy {
        profile-name profile-name;
    }
    uac-policy {
        captive-portal captive-portal;
    }
    utm-policy policy-name;
}
destination-address {
    drop-translated;
    drop-untranslated;
}
firewall-authentication {
    pass-through {
        access-profile profile-name;
        client-match user-or-group-name;
        ssl-termination-profile profile-name;
        web-redirect;
        web-redirect-to-https;
    }
    user-firewall {
        access-profile profile-name;
        domain domain-name;
        ssl-termination-profile profile-name;
    }
    web-authentication {
        client-match user-or-group-name;
    }
}
services-offload;
tcp-options {
    initial-tcp-mss mss-value;
    reverse-tcp-mss mss-value;
    sequence-check-required;
    sequence-check-required;
    syn-check-required;
}
tunnel {
    ipsec-group-vpn group-vpn;
    ipsec-vpn vpn-name;
    pair-policy pair-policy;
}
}
reject;
}
}

```

Hierarchy Level [edit security policies]

<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. Support for the <b>services-offload</b> option added in Junos OS Release 11.4. Support for the <b>source-identity</b> option added in Junos OS Release 12.1. Support for the <b>description</b> option added in Junos OS Release 12.1. Support for the <b>ssl-termination-profile</b> and <b>web-redirect-to-https</b> options added in Junos OS Release 12.1X44-D10. Support for the <b>user-firewall</b> option added in Junos OS Release 12.1X45-D10. Support for the <b>initial-tcp-mss</b> and <b>reverse-tcp-mss</b> options added in Junos OS Release 12.3X48-D20.
<b>Description</b>	Specify a source zone and destination zone to be associated with the security policy.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>from-zone <i>zone-name</i></b>—Name of the source zone.</li><li>• <b>to-zone <i>zone-name</i></b>—Name of the destination zone.</li></ul> <p>The remaining statements are explained separately. See <a href="#">CLI Explorer</a>.</p>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Security Policies Overview</i></li><li>• <i>Understanding Security Policy Rules</i></li><li>• <i>Understanding Security Policy Elements</i></li></ul>

---

## ftp (UTM Policy Anti-Virus)

---

<b>Syntax</b>	<pre>ftp {   download-profile <i>profile-name</i>;   upload-profile <i>profile-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> anti-virus]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the antivirus FTP protocol and attach this policy to a security profile to implement it.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Security Policies Overview</i></li><li>• <i>Understanding Security Policy Rules</i></li><li>• <i>Understanding Security Policy Elements</i></li></ul>

## ftp (UTM Policy Content Filtering)

<b>Syntax</b>	ftp { download-profile <i>profile-name</i> ; upload-profile <i>profile-name</i> ; }
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> content-filtering]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the content-filtering FTP protocol and attach this policy to a security profile to implement it.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Security Policies Overview</i></li> <li>• <i>Understanding Security Policy Rules</i></li> <li>• <i>Understanding Security Policy Elements</i></li> </ul>

## host (Security Web Filtering)

<b>Syntax</b>	host <i>host-name</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering websense-redirect profile <i>profile-name</i> server] [edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> server]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	Set server host parameters by entering the server name or IP address.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## http-profile (Security Antivirus)

---

<b>Syntax</b>	http-profile <i>profile-name</i> ;
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> anti-virus]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the antivirus HTTP protocol and attach this policy to a security profile to implement it.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## http-profile (Security Content Filtering)

---

<b>Syntax</b>	http-profile <i>profile-name</i> ;
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> content-filtering]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the content-filtering HTTP protocol and attach this policy to a security profile to implement it.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Content Filtering Overview on page 71</a></li></ul>

## http-profile (Security Web Filtering)

---

<b>Syntax</b>	http-profile <i>profile-name</i> ;
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> web-filtering]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Configure a UTM policy for the Web-filtering HTTP protocol and attach this policy to a security profile to implement it.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Web Filtering Overview on page 89</a></li></ul>

## imap-profile (Security UTM Policy Antivirus)

---

<b>Syntax</b>	imap-profile <i>profile-name</i> ;
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> anti-virus]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the antivirus IMAP protocol and attach this policy to a security profile to implement it.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.


## imap-profile (Security UTM Policy Content Filtering)

---

<b>Syntax</b>	imap-profile <i>profile-name</i> ;
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> content-filtering]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the content-filtering IMAP protocol and attach this policy to a security profile to implement it.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Content Filtering Overview on page 71</a></li> </ul>

## interval (Security Antivirus)

---

<b>Syntax</b>	interval <i>value</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine pattern-update]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	Set the pattern data files auto-update interval. You can choose to leave the default interval value or you can change it by using this command. You can also force a manual update, if necessary.
<div> <b>NOTE:</b> The data files used with Sophos are not typical virus pattern files; they are small files that help guide virus scanning logic. The full virus pattern database is stored on an external Sophos server called the Sophos Extensible List (SXL) server.</div>	
<b>Options</b>	<p><b>value</b>—Pattern data files auto-update interval in minutes.</p> <p><b>Range:</b> 10 through 10,080 minutes (10 minutes through 7 days)</p> <p><b>Default:</b> For Sophos engine, 1440 minutes (every 24 hours)</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>

---

## ipc

---

<b>Syntax</b>	<pre>ipc {     traceoptions flag <i>flag</i>; }</pre>
<b>Hierarchy Level</b>	[edit security utm]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Configure trace options for IPC.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>flag</b>—Trace operation to perform. To specify more than one trace operation, include multiple <b>flag</b> statements.</li><li>• <b>all</b>—Enable trace for all IPC trace options.</li><li>• <b>basic</b>—Trace basic IPC related information.</li><li>• <b>connection-manager</b>—Trace IPC connection manager information.</li><li>• <b>connection-status</b>—Trace IPC connection status information.</li><li>• <b>detail</b>—Trace IPC related detailed information.</li><li>• <b>pfe</b>—Trace communication with PFE.</li><li>• <b>utm-realtime</b>—Trace IPC realtime-thread information.</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## juniper-local

---

<b>Syntax</b>	<pre>juniper-local {   profile <i>profile-name</i> {     custom-block-message <i>value</i>;     default (block   log-and-permit   permit);     fallback-settings {       default (block   log-and-permit);       server-connectivity (block   log-and-permit);       timeout (block   log-and-permit);       too-many-requests (block   log-and-permit);     }     timeout <i>value</i>;   } }</pre>
<b>Hierarchy Level</b>	[set security utm feature-profile web-filtering]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0 .
<b>Description</b>	Configure the UTM Web-filtering local feature.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## limit (UTM Policy)

---

<b>Syntax</b>	<pre>limit <i>value</i>;</pre>
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> traffic-options sessions-per-client]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle to limit sessions.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## list (Security Antivirus Mime Whitelist)

---

<b>Syntax</b>	<code>list <i>listname</i> {     exception <i>listname</i>; }</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus mime-whitelist]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure the antivirus scanner to use MIME bypass lists (custom objects). If you want to have exceptions to the whitelist, create a mime-pattern list with the <b>exception</b> statement in addition to the <b>list</b> statement.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## list (Security Content Filtering Block Mime)

---

<b>Syntax</b>	<code>list <i>list-name</i>;</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile content-filtering profile <i>profile-name</i> block-mime]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure the content filter to use MIME block lists (custom objects).
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Content Filtering Overview on page 71</a></li> </ul>

## log (Security)

```

Syntax  log {
        cache {
            exclude exclude-name {
                destination-address destination-address;
                destination-port destination-port;
                event-id event-id;
                failure;
                interface-name interface-name;
                policy-name policy-name;
                process process-name;
                protocol protocol;
                source-address source-address;
                source-port source-port;
                success;
                user-name user-name;
            }
            limit value;
        }
        disable;
        event-rate rate;
        facility-override;
        file {
            files max-file-number;
            name file-name;
            path binary-log-file-path;
            size maximum-file-size;
        }
        format (binary | sd-syslog | syslog);
        max-database-record
        mode (event | stream);
        rate-cap <rate-cap-value;rate-limit> (0.5000 logs per second);
        (source-address source-address | source-interface interface-name);
        stream stream-name {
            category (all | content-security | fw-auth | screen | alg | nat | flow | sctp | gtp | ipsec | idp
                | rtlog |pst-ds-lite | appqos |secintel);
            file {
                name file-name;
                size file-size;
                rotation max-rotation-number;
            }
            filter
            threat-attack
            format (binary | sd-syslog | syslog | welf);
            host {
                ip-address;
                port port-number;
            }
            rate-limit (1..65535 logs per second)
            severity (alert | critical | debug | emergency | error | info | notice | warning);
        }
        traceoptions {
            file {

```

```

    filename;
    files number;
    match regular-expression;
    size maximum-file-size (10240..1073741824);
    world-readable
    no-world-readable
  }
  flag (all | configuration | hpl | report | source);
  no-remote-trace (file | flag);
}
transport {
  protocol (udp | tcp | tls);
  tls-profile tls-profile-name;
  tcp-connections tcp-connections;
}
utc-timestamp;
}

```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** You can set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server). You can also specify all the other parameters for security logging.

- Options**
- **disable**—Disable the security logging for the device.
  - **event-rate** *rate*—Limits the rate (0 through 1500) at which logs will be streamed per second.
  - **rate-cap** *rate-cap-value*—Works with event mode only. Limits the rate (0 through 5000) at which data plane logs will be generated per second.
  - **stream**—Every stream can configure file or host.
  - **file-name**—Specify the file name.
  - **file-size**—Specify the file size.
    - SRX1500 - The default value is 25M and the range is 10M through 50M.
    - SRX4100 and SRX4200 - The default value is 25M and the range is 10M through 50M.
    - vSRX - The default value is 2M and the range is 1M through 3M.
  - **rotation**—Configure the max file number for rotation. The default value is 10 and the range is 2 through 19.
  - **max-database-record**—The following are the disk usage range limit for database:
    - SRX1500: 0 through 15,000,000
    - SRX4100 and SRX4200: 0 through 15,000,000
    - vSRX: 0 through 10,000,000



**NOTE:** Be sure there is enough free space in `/var/log/hostlogs/`, otherwise logs may be dropped when written into database.

---

- **source-address** *source-address*—Specify a source IP address or IP address used when exporting security logs, which is mandatory to configure **stream host**.
- **source-interface** *interface-name*—Specify a source interface name, which is mandatory to configure **stream host**.



**NOTE:** The **source-address** and **source-interface** are alternate values. Using one of the options is mandatory.

---

- **utc-time-stamp**—Specify to use UTC time for security log timestamps.

The remaining statements are explained separately. See [CLI Explorer](#).

<b>Required Privilege</b>	security—To view this statement in the configuration.
<b>Level</b>	security-control—To add this statement to the configuration.

## mime-pattern

---

<b>Syntax</b>	<code>mime-pattern <i>object-name</i> {     value [<i>value</i>]; }</code>
<b>Hierarchy Level</b>	[edit security utm custom-objects]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	The gateway device uses MIME (Multipurpose Internet Mail Extension) types to decide which traffic is allowed to bypass various types of scanning.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b><i>object-name</i></b>—Name of the MIME object.</li><li>• <b><i>value value</i></b>—Value of the MIME object. You can configure multiple values separated by spaces and enclosed in square brackets.</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## mime-whitelist

---

**Syntax**

```
mime-whitelist {  
    exception listname;  
    list listname {  
        exception listname;  
    }  
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus]

**Release Information** Statement introduced in Junos OS Release 9.5. Statement updated for Sophos antivirus support in Junos OS Release 11.1.

**Description** Configure the antivirus scanner to use MIME bypass lists and exception lists. You can use your own custom object lists, or you can use the default list that ships with the device called junos-default-bypass-mime.



**WARNING:** When you configure the MIME whitelist feature, be aware that, because header information in HTTP traffic can be spoofed, you cannot always trust HTTP headers to be legitimate. When a Web browser is determining the appropriate action for a given file type, it detects the file type without checking the MIME header contents. However, the MIME whitelist feature does refer to the MIME encoding in the HTTP header. For these reasons, it is possible in certain cases for a malicious website to provide an invalid HTTP header. For example, a network administrator might inadvertently add a malicious website to a MIME whitelist, and, because the site is in the whitelist, it will not be blocked by Sophos even though Sophos has identified the site as malicious in its database. Internal hosts would then be able to reach this site and could become infected.

---

**Options** The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege** security—To view this statement in the configuration.  
**Level** security-control—To add this statement to the configuration.

## no-autoupdate

<b>Syntax</b>	no-autoupdate;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine pattern-update]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 for Sophos engine .
<b>Description</b>	Turn off automatic data file (pattern file) update for the Sophos engines.



**NOTE:** The data files used with Sophos are not typical virus pattern files; they are small files that help guide virus scanning logic. The full virus pattern database is stored on an external Sophos server called the Sophos Extensible List (SXL) server.

<b>Required Privilege</b>	security—To view this statement in the configuration.
<b>Level</b>	security-control—To add this statement to the configuration.

## no-notify-mail-recipient

<b>Syntax</b>	no-notify-mail-recipient;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options fallback-non-block]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
<b>Description</b>	<p>Do not notify the e-mail recipient about errors returned by the antivirus scan engine when a fallback nonblocking action occurs.</p> <p>You can specify that the e-mail recipient is to be notified with the <b>notify-mail-recipient</b> statement.</p>
<b>Required Privilege</b>	security—To view this statement in the configuration.
<b>Level</b>	security-control—To add this statement to the configuration.

## no-notify-mail-sender (Security Content Filtering Notification Options)

---

<b>Syntax</b>	no-notify-mail-sender;
<b>Hierarchy Level</b>	[edit security utm feature-profile content-filtering profile <i>profile-name</i> notification-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Do not notify the e-mail sender.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Content Filtering Overview on page 71</a></li></ul>

## no-notify-mail-sender (Security Fallback Block)

---

<b>Syntax</b>	no-notify-mail-sender;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options fallback-block]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	<p>Do not notify the e-mail sender about errors returned by the antivirus scan engine when a fallback action occurs.</p> <p>You can specify that the e-mail sender is to be notified with the <b>notify-mail-sender</b> statement.</p>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## no-notify-mail-sender (Security Virus Detection)

---

<b>Syntax</b>	no-notify-mail-sender;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options virus-detection]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	<p>Do not notify the e-mail sender when a virus is detected by the antivirus engine.</p> <p>You can specify that the e-mail sender is to be notified with the <b>notify-mail-sender</b> statement.</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>

## no-sbl-default-server

---

<b>Syntax</b>	no-sbl-default-server;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-spam sbl profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Disable the default SBL server lookup.
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Antispam Filtering Overview on page 19</a></li> </ul>

## notification-options (Security Antivirus)

```
Syntax  notification-options {
        fallback-block {
            administrator-email email-address;
            allow-email;
            custom-message message;
            custom-message-subject message-subject;
            display-host;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
        fallback-non-block {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-recipient | no-notify-mail-recipient);
        }
        virus-detection {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
    }
```

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine profile *profile-name*]

**Release Information** Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .

**Description** There are multiple notification options you can configure to trigger when a virus is detected.

**Options** The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege** security—To view this statement in the configuration.  
**Level** security-control—To add this statement to the configuration.

## notification-options (Security Content Filtering)

<b>Syntax</b>	notification-options { custom-message <i>message</i> ; (notify-mail-sender   no-notify-mail-sender); type (message   protocol-only); }
<b>Hierarchy Level</b>	[edit security utm feature-profile content-filtering profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	You can configure a message notification to trigger when a content filter is matched.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Content Filtering Overview on page 71</a></li> </ul>

## notify-mail-recipient

<b>Syntax</b>	notify-mail-recipient;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options fallback-non-block]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
<b>Description</b>	<p>Notify the e-mail recipient about errors returned by the antivirus scan engine when a fallback nonblocking action occurs.</p> <p>You can specify that the e-mail recipient is not to be notified with the <b>no-notify-mail-recipient</b> statement.</p>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## notify-mail-sender (Security Content Filtering Notification Options)

---

<b>Syntax</b>	notify-mail-sender;
<b>Hierarchy Level</b>	[edit security utm feature-profile content-filtering profile <i>profile-name</i> notification-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Notify the e-mail sender.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Content Filtering Overview on page 71</a></li></ul>

## notify-mail-sender (Security Fallback Block)

---

<b>Syntax</b>	notify-mail-sender;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options fallback-block]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	<p>E-mail notification is used to notify the sender or the recipient about the errors returned by either the scan engine or the scan manager when a fallback action occurs.</p> <p>You can specify that the sender is not to be notified with the <b>no-notify-mail-sender</b> statement.</p>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## notify-mail-sender (Security Virus Detection)

---

<b>Syntax</b>	notify-mail-sender;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options virus-detection]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	<p>E-mail notification is used to notify the sender or the recipient about the detected viruses or the scanning errors. When a virus is detected, an e-mail is sent to the sender upon virus detection.</p> <p>You can specify that the sender is not to be notified with the <b>no-notify-mail-sender</b> statement.</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>

## no-uri-check

---

<b>Syntax</b>	no-uri-check;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> scan-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 .
<b>Description</b>	<p>Do not perform Sophos antivirus Uniform Resource Identifier (URI) checking. URI checking is performed by analyzing HTTP traffic URI content against a remote Sophos database server to identify malware or malicious content. URI checking is on by default.</p> <p>You can enable Sophos antivirus URI checking with the <b>uri-check</b> statement.</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>

## out-of-resources (Security Antivirus Sophos Engine)

---

<b>Syntax</b>	default (block   log-and-permit   permit);
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> fallback-options]
<b>Release Information</b>	Statement introduced in Release 11.1 .
<b>Description</b>	Virus scanning requires a great deal of memory and CPU resources. Due to resource constraints, memory allocation requests can be denied by the system. When out-of-resources occurs, scanning is aborted.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>block</b>—Log the error and deny the traffic</li><li>• <b>log-and-permit</b>—Log the error and permit the traffic</li><li>• <b>permit</b>—Permit the traffic</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Sophos Antivirus Configuration Overview on page 48</a></li></ul>

## over-limit

---

<b>Syntax</b>	over-limit (block   log-and-permit);
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> traffic-options sessions-per-client]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle to limit sessions and configure an action to occur when the limit is exceeded.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>block</b>—Log the error and deny the traffic</li><li>• <b>log-and-permit</b>—Log the error and permit the traffic</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">utm on page 248</a></li></ul>

## packet-filter

<b>Syntax</b>	<pre>packet-filter <i>packet-filter-name</i> {   action-profile (<i>profile-name</i>   default);   destination-port (<i>port-range</i>   <i>protocol-name</i>);   destination-prefix <i>destination-prefix</i>;   interface <i>logical-interface-name</i>;   protocol (<i>protocol-number</i>   <i>protocol-name</i>;   source-port (<i>port-range</i>   <i>protocol-name</i>);   source-prefix <i>source-prefix</i>; }</pre>
<b>Hierarchy Level</b>	[edit security datapath-debug]
<b>Release Information</b>	<p>Command introduced in Junos OS Release 9.6 ; Support for IPv6 addresses for the <b>destination-prefix</b> and <b>source-prefix</b> options added in Junos OS Release 10.4.</p> <p>Support for IPv6 filter for the <b>interface</b> option added in Junos OS Release 10.4.</p>
<b>Description</b>	Set packet filter for taking the datapath-debug action. A maximum of four filters are supported at the same time.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>action-profile</b> (<i>profile-name</i>   default)—Identify the action profile to use. You can specify the name of the action profile to use or select default action profile.</li> <li>• <b>destination-port</b> (<i>port-range</i>   <i>protocol name</i>)—Specify a destination port to match TCP/UDP destination port.</li> <li>• <b>destination-prefix</b> <i>destination-prefix</i>—Specify a destination IPv4/IPv6 address prefix.</li> <li>• <b>interface</b> <i>logical-interface-name</i>—Specify a logical interface name.</li> <li>• <b>protocol</b> (<i>protocol-number</i>   <i>protocol-name</i>)—Match IP protocol type.</li> <li>• <b>source-port</b> (<i>port-range</i>   <i>protocol-name</i>)—Match TCP/UDP source port.</li> <li>• <b>source-prefix</b> <i>source-prefix</i>—Specify a source IP address prefix.</li> </ul>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration</p> <p>security-control—To add this statement to the configuration.</p>

## password (Security Antivirus)

---

<b>Syntax</b>	<code>password password-string;</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]
<b>Release Information</b>	Statement introduced in Release 11.2 .
<b>Description</b>	Set the password for the proxy server.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">utm on page 248</a></li></ul>

## pattern-update (Security Antivirus)

---

<b>Syntax</b>	<pre>pattern-update {   email-notify {     admin-email email-address;     custom-message message;     custom-message-subject message-subject;   }   interval value;   no-autoupdate;   proxy {     password password-string;     port port-number;     server address-or-url;     username name;   }   url url; }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 forSophos engine.
<b>Description</b>	Updates to the pattern file are added as new viruses are discovered. You can configure the security device to regularly update the pattern file automatically, or you can update the file manually.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## permit-command

---

<b>Syntax</b>	permit-command <i>protocol-command-list</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile content-filtering profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Apply protocol permit command custom-objects to the content-filtering profile.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Content Filtering Overview on page 71</a></li></ul>

## policies

---

```
Syntax  policies {
        default-policy (deny-all | permit-all);
        from-zone zone-name to-zone zone-name {
            policy policy-name {
                description description;
                match {
                    application {
                        [application];
                        any;
                    }
                    destination-address {
                        [address];
                        any;
                        any-ipv4;
                        any-ipv6;
                    }
                    source-address {
                        [address];
                        any;
                        any-ipv4;
                        any-ipv6;
                    }
                    source-identity {
                        [role-name];
                        any;
                        authenticated-user;
                        unauthenticated-user;
                        unknown-user;
                    }
                }
            }
            scheduler-name scheduler-name;
            then {
                count {
                    alarm {
                        per-minute-threshold number;
                        per-second-threshold number;
                    }
                }
                deny;
                log {
                    session-close;
                    session-init;
                }
                permit {
                    application-services {
                        application-firewall {
                            rule-set rule-set-name;
                        }
                    }
                    application-traffic-control {
                        rule-set rule-set-name;
                    }
                    gprs-gtp-profile profile-name;
                }
            }
        }
    }
```

```

    gprs-sctp-profile profile-name;
    idp;
    redirect-wx | reverse-redirect-wx;
    ssl-proxy {
        profile-name profile-name;
    }
    uac-policy {
        captive-portal captive-portal;
    }
    utm-policy policy-name;
}
destination-address {
    drop-translated;
    drop-untranslated;
}
firewall-authentication {
    pass-through {
        access-profile profile-name;
        client-match user-or-group-name;
        ssl-termination-profile profile-name;
        web-redirect;
        web-redirect-to-https;
    }
    user-firewall {
        access-profile profile-name;
        domain domain-name;
        ssl-termination-profile profile-name;
    }
    web-authentication {
        client-match user-or-group-name;
    }
}
services-offload;
tcp-options {
    sequence-check-required;
    syn-check-required;
}
tunnel {
    ipsec-group-vpn group-vpn;
    ipsec-vpn vpn-name;
    pair-policy pair-policy;
}
}
reject;
}
}
global {
    policy policy-name {
        description description;
        match {
            application {
                [application];
                any;
            }
            destination-address {

```

```
[address];
any;
any-ipv4;
any-ipv6;
}
from-zone {
  [zone-name];
  any;
}
source-address {
  [address];
  any;
  any-ipv4;
  any-ipv6;
}
source-identity {
  [role-name];
  any;
  authenticated-user;
  unauthenticated-user;
  unknown-user;
}
to-zone {
  [zone-name];
  any;
}
}
scheduler-name scheduler-name;
then {
  count {
    alarm {
      per-minute-threshold number;
      per-second-threshold number;
    }
  }
  deny;
  log {
    session-close;
    session-init;
  }
  permit {
    application-services {
      application-firewall {
        rule-set rule-set-name;
      }
      application-traffic-control {
        rule-set rule-set-name;
      }
      gprs-gtp-profile profile-name;
      gprs-sctp-profile profile-name;
      idp;
      redirect-wx | reverse-redirect-wx;
      ssl-proxy {
        profile-name profile-name;
      }
      uac-policy {
```

```

        captive-portal captive-portal;
    }
    utm-policy policy-name;
}
destination-address {
    drop-translated;
    drop-untranslated;
}
firewall-authentication {
    pass-through {
        access-profile profile-name;
        client-match user-or-group-name;
        ssl-termination-profile profile-name;
        web-redirect;
        web-redirect-to-https;
    }
    web-authentication {
        client-match user-or-group-name;
    }
}
services-offload;
tcp-options {
    initial-tcp-mss mss-value;
    reverse-tcp-mss mss-value;
    sequence-check-required;
    syn-check-required;
}
}
reject;
}
}
}
policy-rematch;
policy-stats {
    system-wide (disable | enable) ;
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}

```

Hierarchy Level [edit security]

<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. Support for the <b>services-offload</b> option added in Junos OS Release 11.4. Support for the <b>source-identity</b> option added in Junos OS Release 12.1. Support for the <b>description</b> option added in Junos OS Release 12.1. Support for the <b>ssl-termination-profile</b> and <b>web-redirect-to-https</b> options added on high-end SRX Series Services Gateways starting from Junos OS Release 12.1X44-D10 and on vSRX, SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 Services Gateways starting from Junos OS Release 15.1X49-D40. Support for the <b>user-firewall</b> option added in Junos OS Release 12.1X45-D10. Support for the <b>domain</b> option, and for the <b>from-zone</b> and <b>to-zone</b> global policy match options, added in Junos OS Release 12.1X47-D10. Support for the <b>initial-tcp-mss</b> and <b>reverse-tcp-mss</b> options added in Junos OS Release 12.3X48-D20. Support for the <b>extensive</b> option for <b>policy-rematch</b> added in Junos OS Release 15.1X49-D20.
<b>Description</b>	Configure network security policies.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Security Policies Overview</i></li></ul>

---

## pop3-profile (Security UTM Policy Antivirus)

---

<b>Syntax</b>	pop3-profile <i>profile-name</i> ;
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> anti-virus]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the antivirus POP3 protocol and attach this policy to a security profile to implement it.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

---

## pop3-profile (Security UTM Policy Content Filtering)

---

<b>Syntax</b>	pop3-profile <i>profile-name</i> ;
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> content-filtering]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the content filtering POP3 protocol and attach this policy to a security profile to implement it.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## port (Security Antivirus)

---

<b>Syntax</b>	<code>port <i>port-number</i>;</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 .
<b>Description</b>	Set the port number for the proxy server.
<b>Options</b>	<b>Range:</b> 0 through 65,535
<b>Required Privilege</b>	security—To view this statement in the configuration.
<b>Level</b>	security-control—To add this statement to the configuration.

## port (Security Web Filtering Server)

---

<b>Syntax</b>	<code>port <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering websense-redirect profile <i>profile-name</i> server] [edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> server]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	Enter the port number for communicating with the server. (Default ports are 80, 8080, and 8081.)
<b>Required Privilege</b>	security—To view this statement in the configuration.
<b>Level</b>	security-control—To add this statement to the configuration.

## primary-server

---

<b>Syntax</b>	<pre>primary-server {     address <i>ipv4-address</i>;     login <i>sender-email-address</i> {         password <i>password</i>;     } }</pre>
<b>Hierarchy Level</b>	[edit smtp]
<b>Release Information</b>	Statement added in Junos OS Release 10.0.
<b>Description</b>	Configure Simple Mail Transfer Protocol (SMTP) primary server for access authorization for SMTP requests.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## profile (Security Antispam SBL)

---

<b>Syntax</b>	<pre>profile <i>profile-name</i> {     custom-tag-string [<i>string</i>];     (sbl-default-server   no-sbl-default-server);     spam-action (block   tag-header   tag-subject); }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-spam sbl]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Create a profile for the antispam sbl feature. This profile includes all subsequent configuration options.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## profile (Security Content Filtering)

**Syntax**    `profile profile-name {`  
                   `block-command protocol-command-list;`  
                   `block-content-type (activex | exe | http-cookie | java-applet | zip);`  
                   `block-extension extension-list;`  
                   `block-mime {`  
                     `exception list-name;`  
                     `list list-name;`  
                   `}`  
                   `notification-options {`  
                     `custom-message message;`  
                     `(notify-mail-sender | no-notify-mail-sender);`  
                     `type (message | protocol-only);`  
                   `}`  
                   `permit-command protocol-command-list;`  
                   `}`

**Hierarchy Level**    [edit security utm feature-profile content-filtering]

**Release Information**    Statement introduced in Junos OS Release 9.5 .

**Description**    Create a profile for the content-filtering feature. This profile includes all subsequent configuration options.

**Options**    The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege**    security—To view this statement in the configuration.  
**Level**    security-control—To add this statement to the configuration.

**Related Documentation**    • [Content Filtering Overview on page 71](#)

## profile (Security Sophos Engine Antivirus)

```
Syntax  profile <name> {
        fallback-options {
            content-size (block | log-and-permit | permit);
            default (block | log-and-permit | permit);
            engine-not-ready (block | log-and-permit | permit);
            out-of-resources (block | log-and-permit | permit);
            timeout (block | log-and-permit | permit);
            too-many-requests (block | log-and-permit | permit);
        }
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
        }
        scan-options {
            content-size-limit value;
            (no-uri-check | uri-check);
            timeout value;
        }
        trickling {
            timeout value;
        }
    }
```

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine]

**Release Information** Statement introduced in Junos OS Release 11.1 .

**Description** Create a profile for the Sophos antivirus engine. This profile includes all subsequent configuration options.

**Options** The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege** security—To view this statement in the configuration.  
**Level** security-control—To add this statement to the configuration.

**Related Documentation** • [Sophos Antivirus Configuration Overview on page 48](#)

## profile (Security Web Filtering Juniper Enhanced)

**Syntax**

```
profile profile-name {
    category customurl-list name {
        action (block | log-and-permit | permit | quarantine);
    }
    custom-block-message value;
    custom-quarantine-message value;
    default (block | log-and-permit | permit | quarantine);
    fallback-settings {
        default (block | log-and-permit);
        server-connectivity (block | log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
    }
    no-safe-search;
    site-reputation-action {
        fairly-safe (block | log-and-permit | permit | quarantine);
        harmful (block | log-and-permit | permit | quarantine);
        moderately-safe (block | log-and-permit | permit | quarantine);
        suspicious (block | log-and-permit | permit | quarantine);
        very-safe (block | log-and-permit | permit | quarantine);
    }
    timeout value;
}
```

**Hierarchy Level** [edit security utm feature-profile web-filtering juniper-enhanced]

**Release Information** Statement introduced in Junos OS Release 11.4 .

**Description** Create a profile for the juniper-enhanced feature. This profile includes all subsequent configuration options.

**Options** The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege** security—To view this statement in the configuration.  
**Level** security-control—To add this statement to the configuration.

**Related Documentation** • [Monitoring Web Filtering Configurations on page 129](#)

## profile (Security Web Filtering Juniper Local)

---

<b>Syntax</b>	<pre>profile <i>profile-name</i> {     custom-block-message <i>value</i>;     default (block   log-and-permit   permit);     fallback-settings {         default (block   log-and-permit);         server-connectivity (block   log-and-permit);         timeout (block   log-and-permit);         too-many-requests (block   log-and-permit);     }     timeout <i>value</i>; }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering juniper-local]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0 .
<b>Description</b>	Create a profile for the web-filtering juniper-local feature. This profile includes all subsequent configuration options.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Monitoring Web Filtering Configurations on page 129</a></li><li>• <a href="#">Example: Configuring Local Web Filtering on page 114</a></li></ul>

## profile (Security Web Filtering Websense Redirect)

**Syntax**

```
profile profile-name {
  account value;
  custom-block-message value;
  fallback-settings {
    default (block | log-and-permit);
    server-connectivity (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  server {
    host host-name;
    port number;
  }
  sockets value;
  timeout value;
}
```

**Hierarchy Level** [security utm feature-profile web-filtering websense-redirect]

**Release Information** Statement introduced in Junos OS Release 9.5 .

**Description** Create a profile for the web-filtering web-sense feature. This profile includes all subsequent configuration options.

**Options** The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- [Monitoring Web Filtering Configurations on page 129](#)

## protocol-command

---

<b>Syntax</b>	<code>protocol-command <i>object-name</i> {     value [<i>value</i>]; }</code>
<b>Hierarchy Level</b>	[edit security utm custom-objects]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Different protocols use different commands to communicate between servers and clients. By blocking or allowing certain commands, traffic can be controlled on the protocol command level.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b><i>object-name</i></b>—Name of the command-list object.</li><li>• <b><i>value value</i></b>—Value of the command-list object. You can configure multiple values separated by spaces and enclosed in square brackets.</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Understanding UTM Custom Objects on page 4</a></li></ul>

## proxy (Security Antivirus)

---

<b>Syntax</b>	<code>proxy {     password <i>password-string</i>;     port <i>port-number</i>;     server <i>address-or-url</i>;     username <i>name</i>; }</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine pattern-update]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 .
<b>Description</b>	Update the pattern file on the proxy server.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## quarantine-message (Security UTM)

<b>Syntax</b>	<pre>quarantine-message {   type {     custom-redirect-url;   }   url <i>url</i>; }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1X44-D10 for Enhanced Web Filtering.
<b>Description</b>	Configure Juniper enhanced quarantine message settings.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>type</b>—Specify the following type of the quarantine message:           <ul style="list-style-type: none"> <li>• <b>custom-redirect-url</b>—Specify Custom redirect URL server.</li> </ul> </li> <li>• <b>url <i>url</i></b>—Specify an URL of the quarantine message.</li> </ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## sbl

<b>Syntax</b>	<pre>sbl {   profile <i>profile-name</i> {     custom-tag-string [<i>string</i>];     (sbl-default-server   no-sbl-default-server);     spam-action (block   tag-header   tag-subject);   } }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-spam]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure UTM server-based antispam features.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## sbl-default-server

---

<b>Syntax</b>	sbl-default-server;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-spam sbl profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Enable the default SBL server lookup. You should enable this feature if you are using server-based spam filtering. (The SBL server is predefined on the device. It ships with the name and address of the SBL server.)
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## scan-options (Security Antivirus Sophos Engine)

---

<b>Syntax</b>	scan-options { content-size-limit <i>value</i> ; (no-uri-check   uri-check); timeout <i>value</i> ; }
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 .
<b>Description</b>	Configure the antivirus feature to scan specific types of traffic based on various scanning configuration parameters.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## secondary-server

---

<b>Syntax</b>	secondary-server { address <i>ipv4-address</i> ; login <i>sender-email-address</i> { password <i>password</i> ; } }
<b>Hierarchy Level</b>	[edit smtp]
<b>Release Information</b>	Statement added in Junos OS Release 10.0.
<b>Description</b>	Configure Simple Mail Transfer Protocol (SMTP) secondary server for access authorization for SMTP requests.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## server (Security Antivirus)

---

<b>Syntax</b>	server <i>address-or-url</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 .
<b>Description</b>	Set the IP address or URL for the proxy server.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## server (Security Web Filtering)

---

<b>Syntax</b>	server { host <i>host-name</i> ; port <i>number</i> ; }
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering websense-redirect profile <i>profile-name</i> ] [edit security utm feature-profile web-filtering juniper-enhanced]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	Set server parameters by entering the server name or IP address.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## server-connectivity

---

<b>Syntax</b>	server-connectivity (block   log-and-permit);
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering websense-redirect profile <i>profile-name</i> fallback-settings] [edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> fallback-settings]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	Fallback settings tell the system how to handle errors. This is the action that occurs when a request fails for this reason.
<b>Options</b>	<ul style="list-style-type: none"><li>• block—Log the error and deny the traffic</li><li>• log-and-permit—Log the error and permit the traffic</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## sessions-per-client

---

**Syntax**    sessions-per-client {  
                  limit *value*;  
                  over-limit (block | log-and-permit);  
          }

**Hierarchy Level**    [edit security utm utm-policy *policy-name* traffic-options]

**Release Information**    Statement introduced in Junos OS Release 9.5 .

**Description**    In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle.



**NOTE:** The `sessions-per-client limit` command supports the antispam, content filtering, and antivirus UTM features. It does not support Web filtering.

**Options**    The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege Level**    security—To view this statement in the configuration.  
                  security-control—To add this statement to the configuration.

## site-reputation-action

---

<b>Syntax</b>	<pre>site-reputation-action {     harmful (block   log-and-permit   permit   quarantine);     fairly-safe (block   log-and-permit   permit   quarantine);     moderately-safe (block   log-and-permit   permit   quarantine);     suspicious (block   log-and-permit   permit   quarantine);     very-safe (block   log-and-permit   permit   quarantine); }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> category <i>category-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4 .
<b>Description</b>	Specify the action to be taken depending on the site reputation returned for all types of URLs whether it is categorized or uncategorized.
<b>Options</b>	<p><b>fairly-safe</b>—Permit, log-and-permit, block or quarantine a request if a site-reputation of 70 through 79 is returned.</p> <p><b>harmful</b>—Permit, log-and-permit, block or quarantine a request if a site-reputation of zero through 59 is returned.</p> <p><b>moderately-safe</b>—Permit, log-and-permit, block or quarantine a request if a site-reputation of 80 through 89 is returned.</p> <p><b>suspicious</b>—Permit, log-and-permit, block or quarantine a request if a site-reputation of 60 through 69 is returned.</p> <p><b>very-safe</b>—Permit, log-and-permit, block or quarantine a request if a site-reputation of 90 through 100 is returned.</p>
<b>Required Privilege Level</b>	<p><b>security</b>—To view this statement in the configuration.</p> <p><b>security-control</b>—To add this statement to the configuration.</p>

## size (Security Web Filtering Cache)

---

<b>Syntax</b>	<pre>size value;</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering juniper-enhanced cache]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	Set the cache size parameters for Web filtering.
<b>Options</b>	<b>Range:</b> 0 through 4096 kilobytes.
<b>Required Privilege Level</b>	<p><b>security</b>—To view this statement in the configuration.</p> <p><b>security-control</b>—To add this statement to the configuration.</p>

## smtp-profile (Security UTM Policy Antispam)

---

<b>Syntax</b>	<code>smtp-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit security utm utm-policy <i>policy-name</i> anti-spam]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the antispam SMTP protocol and attach this policy to a security profile to implement it.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">smtp-profile (Security UTM Policy Antivirus) on page 225</a></li> </ul>

## smtp-profile (Security UTM Policy Antivirus)

---

<b>Syntax</b>	<code>smtp-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit security utm utm-policy <i>policy-name</i> anti-virus]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the antivirus SMTP protocol and attach this policy to a security profile to implement it.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## smtp-profile (Security UTM Policy Content Filtering)

---

<b>Syntax</b>	<code>smtp-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit security utm utm-policy <i>policy-name</i> content-filtering]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the content-filtering SMTP protocol and attach this policy to a security profile to implement it.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## sockets

---

<b>Syntax</b>	<code>sockets <i>value</i>;</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering websense-redirect profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Enter the number of sockets used for communicating between the client and server. The default is 1.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## sophos-engine

```
Syntax  sophos-engine {
        pattern-update {
            email-notify {
                admin-email email-address;
                custom-message message;
                custom-message-subject message-subject;
            }
            interval value;
            no-autoupdate;
            proxy {
                password password-string;
                port port-number;
                server address-or-url;
                username name;
            }
            url url;
        }
        profile <name> {
            fallback-options {
                content-size (block | log-and-permit | permit);
                default (block | log-and-permit | permit);
                engine-not-ready (block | log-and-permit | permit);
                out-of-resources (block | log-and-permit | permit);
                timeout (block | log-and-permit | permit);
                too-many-requests (block | log-and-permit | permit);
            }
            notification-options {
                fallback-block {
                    administrator-email email-address;
                    allow-email;
                    custom-message message;
                    custom-message-subject message-subject;
                    display-host;
                    (notify-mail-sender | no-notify-mail-sender);
                    type (message | protocol-only);
                }
                fallback-non-block {
                    custom-message message;
                    custom-message-subject message-subject;
                    (notify-mail-recipient | no-notify-mail-recipient);
                }
                virus-detection {
                    custom-message message;
                    custom-message-subject message-subject;
                    (notify-mail-sender | no-notify-mail-sender);
                    type (message | protocol-only);
                }
            }
            scan-options {
                content-size-limit value;
                (no-uri-check | uri-check);
                timeout value;
            }
        }
    }
```

```
    }
    trickling {
        timeout value;
    }
}
sxl-retry value;
sxl-timeout seconds;
}
```

<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 .
<b>Description</b>	Configure the UTM Sophos antivirus feature.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

---

## spam-action

<b>Syntax</b>	spam-action (block   tag-header   tag-subject);
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-spam sbl profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure the action to be taken by the device when spam is detected.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>block</b>—Block e-mail.</li><li>• <b>tag-header</b>—Tag header of e-mail.</li><li>• <b>tag-subject</b>—Tag subject of e-mail.</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Example: Configuring Server-Based Antispam Filtering on page 23</a></li><li>• <a href="#">Example: Configuring Local List Antispam Filtering on page 30</a></li></ul>

## sxl-retry

---

<b>Syntax</b>	<code>sxl-retry <i>value</i>;</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 .
<b>Description</b>	Configure the number of retry attempts to the remote Sophos Extensible List (SXL) server when a request timeout occurs.
<b>Options</b>	<p><b><i>value</i></b> —Number of retries.</p> <p><b>Range:</b> 0 through 5</p> <p><b>Default:</b> 1</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>

## sxl-timeout

---

<b>Syntax</b>	<code>sxl-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 .
<b>Description</b>	Configure the timeout value for responses to a Sophos checksum or URI query.
<b>Options</b>	<p><b><i>seconds</i></b> —Number of seconds before timeout occurs.</p> <p><b>Range:</b> 1 through 5 seconds</p> <p><b>Default:</b> 2 seconds</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>

## timeout (Security Antivirus Fallback Options Sophos Engine)

---

<b>Syntax</b>	default (block   log-and-permit   permit);
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> fallback-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 .
<b>Description</b>	Scanning a complex file could consume resources and time. If the time it is taking to scan exceeds the timeout setting in the antivirus profile, the processing is aborted and the content is either passed or blocked without completing the virus checking. The decision is made based on the timeout fallback option.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>block</b>—Log the error and deny the traffic</li><li>• <b>log-and-permit</b>—Log the error and permit the traffic</li><li>• <b>permit</b>—Permit the traffic</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## timeout (Security Antivirus Scan Options)

---

<b>Syntax</b>	timeout <i>value</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> scan-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	The scanning timeout value includes the time frame from when the scan request is generated to when the scan result is returned by the scan engine. The time range can be 1 to 1800 seconds. By default, it is 180 seconds.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## timeout (Security Web Filtering)

---

<b>Syntax</b>	<code>timeout <i>value</i>;</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering websense-redirect profile <i>profile-name</i> ] [edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	Enter a timeout limit for requests. Once this limit is reached, fail mode settings are applied. The default here is 15 seconds.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## timeout (Security Web Filtering Cache)

---

<b>Syntax</b>	<code>timeout <i>value</i>;</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering juniper-enhanced cache]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	Set the cache timeout parameters.
<b>Options</b>	<b>Range:</b> 1 through 1800 minutes.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## timeout (Security Web Filtering Fallback Settings)

---

<b>Syntax</b>	timeout (block   log-and-permit);
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering websense-redirect profile <i>profile-name</i> fallback-settings] [edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> fallback-settings]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	Fallback settings tell the system how to handle errors.
<b>Options</b>	<ul style="list-style-type: none"><li>• log-and-permit—Log the error and permit the traffic</li><li>• block—Log the error and deny the traffic</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## too-many-requests (Security Antivirus Fallback Options Sophos Engine)

---

<b>Syntax</b>	default (block   log-and-permit   permit);
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> fallback-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 .
<b>Description</b>	If the total number of messages received concurrently exceeds the device limits, the content is either passed or blocked depending on the too-many-request fallback option. (The allowed request limit is not configurable.)
<b>Options</b>	<ul style="list-style-type: none"><li>• block—Log the error and deny the traffic</li><li>• log-and-permit—Log the error and permit the traffic</li><li>• permit—Permit the traffic</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

---

## too-many-requests (Security Web Filtering Fallback Settings)

---

<b>Syntax</b>	too-many-requests (block   log-and-permit);
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering websense-redirect profile <i>profile-name</i> fallback-settings] [edit security utm feature-profile web-filtering juniper-enhanced profile <i>profile-name</i> fallback-settings]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	If the total number of messages received concurrently exceeds the device limits, the content is either passed or blocked depending on the too-many-request fallback option. The default action is BLOCK. (The allowed request limit is not configurable.)
<b>Options</b>	<ul style="list-style-type: none"><li>• block—Log the error and deny the traffic</li><li>• log-and-permit—Log the error and permit the traffic</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## to-zone (Security Policies)

---

```
Syntax  to-zone zone-name {  
        policy policy-name {  
            description description;  
            match {  
                application {  
                    [application];  
                    any;  
                }  
                destination-address {  
                    [address];  
                    any;  
                    any-ipv4;  
                    any-ipv6;  
                }  
                source-address {  
                    [address];  
                    any;  
                    any-ipv4;  
                    any-ipv6;  
                }  
                source-identity {  
                    [role-name];  
                    any;  
                    authenticated-user;  
                    unauthenticated-user;  
                    unknown-user;  
                }  
            }  
            scheduler-name scheduler-name;  
            then {  
                count {  
                    alarm {  
                        per-minute-threshold number;  
                        per-second-threshold number;  
                    }  
                }  
                deny;  
                log {  
                    session-close;  
                    session-init;  
                }  
                permit {  
                    application-services {  
                        application-firewall {  
                            rule-set rule-set-name;  
                        }  
                    }  
                    application-traffic-control {  
                        rule-set rule-set-name;  
                    }  
                    gprs-gtp-profile profile-name;  
                    gprs-sctp-profile profile-name;  
                    idp;  
                }  
            }  
        }  
    }
```

```

    redirect-wx | reverse-redirect-wx;
    ssl-proxy {
        profile-name profile-name;
    }
    uac-policy {
        captive-portal captive-portal;
    }
    utm-policy policy-name;
}
destination-address {
    drop-translated;
    drop-untranslated;
}
firewall-authentication {
    pass-through {
        access-profile profile-name;
        client-match user-or-group-name;
        ssl-termination-profile profile-name;
        web-redirect;
        web-redirect-to-https;
    }
    web-authentication {
        client-match user-or-group-name;
    }
}
services-offload;
tcp-options {
    sequence-check-required;
    syn-check-required;
}
tunnel {
    ipsec-group-vpn group-vpn;
    ipsec-vpn vpn-name;
    pair-policy pair-policy;
}
}
reject;
}
}

```

**Hierarchy Level** [edit security policies from-zone *zone-name*]

**Release Information** Statement introduced in Junos OS Release 8.5. Support for the **services-offload** and **junos-host** options added in Junos OS Release 11.4. Support for the **source-identity** option added in Junos OS Release 12.1. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10.

**Description** Specify a destination zone to be associated with the security policy.

- Options**
- **zone-name**—Name of the destination zone object.
  - **junos-host**—Default security zone for self-traffic of the device.

The remaining statements are explained separately. See [CLI Explorer](#).

<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Security Policies Overview</i></li><li>• <i>Understanding Security Policy Rules</i></li><li>• <i>Understanding Security Policy Elements</i></li></ul>

---

## traceoptions (Security Antispam)

---

<b>Syntax</b>	traceoptions flag <i>flag</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-spam]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Define tracing operations for UTM antispam features.
<b>Options</b>	<ul style="list-style-type: none"><li>• <i>flag</i>:<ul style="list-style-type: none"><li>• <b>all</b>—Enable all antispam trace flags.</li><li>• <b>manager</b> —Trace antispam manager information.</li><li>• <b>sbl</b>—Trace SBL server information.</li></ul></li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## traceoptions (Security Antivirus)

---

<b>Syntax</b>	traceoptions flag <i>flag</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Define tracing operations for UTM antivirus features.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>flag</b>—Trace operation to perform. To specify more than one trace operation, include multiple <b>flag</b> statements. <ul style="list-style-type: none"> <li>• <b>all</b>—Enable trace all antivirus trace options.</li> <li>• <b>basic</b>—Trace antivirus module generic basic information.</li> <li>• <b>detail</b>—Trace antivirus module generic detail information.</li> <li>• <b>engine</b>—Trace scan engine information.</li> <li>• <b>event</b>—Trace communication events between routing engine side processes.</li> <li>• <b>ipc</b>—Trace communication events with Packet Forwarding Engine.</li> <li>• <b>manager</b>—Trace antivirus manager process activities.</li> <li>• <b>pattern</b>—Trace detail information of pattern loading.</li> <li>• <b>sendmail</b>—Trace mail notifying process activities.</li> <li>• <b>statistics</b>—Trace statistics information.</li> <li>• <b>updater</b>—Trace pattern updater process activities.</li> <li>• <b>worker</b>—Trace antivirus worker process activities.</li> </ul> </li> </ul>
<b>Required Privilege Level</b>	trace—To view this statement in the configuration. trace-control—To add this statement to the configuration.

## traceoptions (Security Application Proxy)

---

<b>Syntax</b>	<pre>traceoptions {     flag <i>flag</i>; }</pre>
<b>Hierarchy Level</b>	[edit security utm application-proxy]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure tracing options for application proxy.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>flag</b>—Trace operation to perform. To specify more than one trace operation, include multiple <b>flag</b> statements.</li><li>• <b>abort</b>—Trace aborted sessions for application proxy.</li><li>• <b>all</b>—Trace with all flags enabled.</li><li>• <b>anti-virus</b>—Trace anti-virus information.</li><li>• <b>application-objects</b>—Trace application-proxy objects information.</li><li>• <b>basic</b>—Trace application-proxy related basic information.</li><li>• <b>buffer</b>— Trace application-proxy data buffer information.</li><li>• <b>connection-rating</b>—Trace connection rating information.</li><li>• <b>detail</b>—Trace application-proxy related detailed information.</li><li>• <b>ftp-control</b>—Trace FTP control connection information.</li><li>• <b>ftp-data</b>—Trace FTP data connection information.</li><li>• <b>http</b>—Trace HTTP protocol information.</li><li>• <b>imap</b>—Trace IMAP protocol information.</li><li>• <b>memory</b>—Trace memory usage.</li><li>• <b>mime</b>—Trace MIME parser information.</li><li>• <b>parser</b>— Trace protocol parser information.</li><li>• <b>pfe</b>—Trace communication with PFE.</li><li>• <b>pop3</b>—Trace POP3 protocol information.</li><li>• <b>queue</b>—Trace queue information.</li><li>• <b>regex-engine</b>—Trace Pattern Match Engine (PME) information.</li><li>• <b>smtp</b>—Trace SMTP protocol information.</li><li>• <b>sophos-anti-virus</b>—Trace anti-virus sophos engine information.</li><li>• <b>tcp</b>—Trace TCP level information.</li><li>• <b>timer</b>—Trace timer processing.</li></ul>

- **utm-realtime**—Trace application-proxy realtime-thread information

**Required Privilege** trace—To view this statement in the configuration.  
**Level** trace-control—To add this statement to the configuration.

### traceoptions (Security Content Filtering)

**Syntax** traceoptions flag *flag*;

**Hierarchy Level** [edit security utm feature-profile content-filtering]

**Release Information** Statement introduced in Junos OS Release 9.5 .

**Description** Define tracing options for content filtering features.

- Options**
- **flag**:
    - **all**—Enable all content filtering trace flags.
    - **basic** —Trace content filtering basic information.
    - **detail**—Trace content filtering detailed information.

**Required Privilege** security—To view this statement in the configuration.  
**Level** security-control—To add this statement to the configuration.

### traceoptions (Security UTM)

**Syntax** traceoptions flag *flag*;

**Hierarchy Level** [edit security utm]

**Release Information** Statement introduced in Junos OS Release 9.5 .

**Description** Define tracing operations for UTM features.

- Options**
- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
    - **all**—Enable trace for all UTM trace options.
    - **cli**—Trace CLI configuration activity and command changes.
    - **daemon**—Trace daemon information.
    - **ipc**—Trace communication events with Packet Forwarding Engine (PFE).
    - **pfe**—Trace PFE information.

**Required Privilege** trace—To view this statement in the configuration.  
**Level** trace-control—To add this statement to the configuration.

## traceoptions (Security Web Filtering)

---

<b>Syntax</b>	traceoptions flag <i>flag</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering]
<b>Release Information</b>	Command introduced in Junos OS Release 10.1 . Command introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
<b>Description</b>	Define tracing operations for individual Web filtering modules. To specify more than one tracing operation, include multiple flag statements.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>flag</b>:<ul style="list-style-type: none"><li>• <b>all</b>—Enable all Web filtering trace flags.</li><li>• <b>basic</b> —Trace basic information on the Web filtering module.</li><li>• <b>cache</b>—Enable Web filtering flags for the Web filtering cache maintained on the Web filtering module.</li><li>• <b>enhanced</b>—Enable Web filtering flags for processing through Enhanced Web Filtering.</li><li>• <b>heartbeat</b>—Trace connectivity information with Web filter server.</li><li>• <b>ipc</b>—Trace Web filtering IPC messages.</li><li>• <b>packet</b>—Trace packet information from session management.</li><li>• <b>profile</b>—Trace profile configuration information.</li><li>• <b>requests</b>—Trace requests sent to Web filter server.</li><li>• <b>response</b>—Trace response received from Web filter server.</li><li>• <b>session manager</b>—Trace session management information.</li><li>• <b>socket</b>—Trace the communication socket with Web filter server.</li><li>• <b>timer</b>—Trace aging information for requests sent to server.</li></ul></li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## traceoptions (SMTP)


<b>Syntax</b>	<pre> traceoptions {     flag {         all;         configuration;         IPC;         protocol-exchange;         send-request;     } } </pre>
<b>Hierarchy Level</b>	[edit smtp]
<b>Release Information</b>	Statement added in Junos OS Release 10.0.
<b>Description</b>	Set the Simple Mail Transfer Protocol (SMTP) traceoptions.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">utm on page 248</a></li> </ul>

## traffic-options

<b>Syntax</b>	<pre> traffic-options {     sessions-per-client {         limit <i>value</i>;         over-limit (block   log-and-permit);     } } </pre>
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## trickling

---

<b>Syntax</b>	trickling { timeout <i>value</i> ; }
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Statement updated for Sophos support in Junos OS Release 11.1.
<b>Description</b>	HTTP trickling is a mechanism used to prevent the HTTP client or server from timing-out during a file transfer or during antivirus scanning. HTTP Trickling is time-based and there is only one parameter to configure for this feature, which is the timeout Interval. By default, trickling is disabled.
<div><b>WARNING:</b> When you enable the trickling option, keep in mind that trickling might send part of a file to the client during its antivirus scan. It is therefore possible that some of the content could be received by the client before the file has been fully scanned.</div>	
<b>Options</b>	<b>value</b> —Timeout interval in seconds. <b>Range:</b> 0 through 600 seconds
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## type (Security Antivirus Feature Profile)

---

<b>Syntax</b>	type sophos-engine;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Statement updated for Sophos in Junos OS Release 11.1 .
<b>Description</b>	Set the antivirus engine that will be used on the device. You can only have one engine type running.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## type (Security Content Filtering Notification Options)

---

<b>Syntax</b>	type (message   protocol-only);
<b>Hierarchy Level</b>	[edit security utm feature-profile content-filtering profile <i>profile-name</i> notification-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	When content is blocked, the client generally still receives a successful response code but with modified content (file replacement) containing a warning message. But with protocol-only notifications, a protocol-specific error code might be returned to the client.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>message</b>—Send a generic notification.</li> <li>• <b>protocol-only</b>—Send a protocol-specific notification.</li> </ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## type (Security Fallback Block)

---

<b>Syntax</b>	type (message   protocol-only);
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options fallback-block]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	You can configure notifications for both fallback blocking and fallback nonblocking actions. With protocol-only notifications, a protocol-specific error code may be returned to the client.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>message</b>—Send a generic notification.</li> <li>• <b>protocol-only</b>—Send a protocol-specific notification.</li> </ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## type (Security Virus Detection)

---

<b>Syntax</b>	type (message   protocol-only);
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options virus-detection]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
<b>Description</b>	When content is blocked because a virus is found or a scan error occurs, the client generally still receives a successful response code but with modified content (file replacement) containing a warning message. But with protocol-only notifications, a protocol-specific error code might be returned to the client.
<b>Options</b>	<ul style="list-style-type: none"><li>• message—Send a generic notification.</li><li>• protocol-only—Send a protocol-specific notification.</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## upload-profile (Security Antivirus FTP)

---

<b>Syntax</b>	upload-profile <i>profile-name</i> ;
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> anti-virus ftp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the antivirus FTP (upload) protocol and attach this policy to a security profile to implement it.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## upload-profile (Security Content Filtering FTP)

---

<b>Syntax</b>	upload-profile <i>profile-name</i> ;
<b>Hierarchy Level</b>	[edit security utm utm-policy <i>policy-name</i> content-filtering ftp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure a UTM policy for the content-filtering FTP (upload) protocol and attach this policy to a security profile to implement it.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## uri-check

---

<b>Syntax</b>	uri-check;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> scan-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1 .
<b>Description</b>	<p>Perform Sophos antivirus Uniform Resource Identifier (URI) checking. URI checking is a way of analyzing URI content in HTTP traffic against a remote Sophos database to identify malware or malicious content. URI checking is on by default.</p> <p>You can disable Sophos antivirus URI checking with the <b>no-uri-check</b> statement.</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>

## url (Security Antivirus)

---

<b>Syntax</b>	url <i>url</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine pattern-update]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	Specify the URL for the pattern database. You should not change the default URL unless you are experiencing problems with it and have called for support.
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>

## url-blacklist

---

<b>Syntax</b>	url-blacklist <i>listname</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	This is a global blacklist category, blocking content for Web filtering.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>

## url-pattern

---

<b>Syntax</b>	<code>url-pattern <i>object-name</i> {     value [<i>value</i>]; }</code>
<b>Hierarchy Level</b>	[edit security utm custom-objects]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Use URL pattern lists to create custom URL category lists. These are lists of patterns that bypass scanning.



**WARNING:** Custom category does not take precedence over predefined categories when it has the same name as one of the predefined categories. We do not recommend having a custom category name be the same as the predefined category name.

<b>Options</b>	<ul style="list-style-type: none"><li>• <b><i>object-name</i></b>—Name of the URL list object.</li><li>• <b><i>value value</i></b>—Value of the URL list object. You can configure multiple values separated by spaces and enclosed in square brackets.</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Building Blocks Feature Guide for Security Devices</i></li></ul>

## url-whitelist (Security Antivirus)

---

<b>Syntax</b>	<code>url-whitelist <i>listname</i>;</code>
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	A URL whitelist is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for scanning.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## url-whitelist (Security Web Filtering)

---

<b>Syntax</b>	url-whitelist <i>listname</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering]
<b>Description</b>	A URL whitelist is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for filtering
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege</b>	security—To view this statement in the configuration.
<b>Level</b>	security-control—To add this statement to the configuration.

## username (Security Antivirus)

---

<b>Syntax</b>	username <i>name</i> ;
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 .
<b>Description</b>	Set the username for the proxy server.
<b>Required Privilege</b>	security—To view this statement in the configuration.
<b>Level</b>	security-control—To add this statement to the configuration.

## utm

```

Syntax  utm {
        application-proxy {
            traceoptions {
                flag flag;
            }
        }
        custom-objects {
            custom-url-category object-name {
                value [value];
            }
            filename-extension object-name {
                value [value];
            }
            mime-pattern object-name {
                value [value];
            }
            protocol-command object-name {
                value [value];
            }
            url-pattern object-name {
                value [value];
            }
        }
        feature-profile {
            anti-spam {
                address-blacklist list-name;
                address-whitelist list-name;
                sbl {
                    profile profile-name {
                        custom-tag-string [string];
                        (sbl-default-server | no-sbl-default-server);
                        spam-action (block | tag-header | tag-subject);
                    }
                }
                traceoptions {
                    flag flag;
                }
            }
            anti-virus {
                mime-whitelist {
                    exception listname;
                    list listname {
                        exception listname;
                    }
                }
                sophos-engine {
                    pattern-update {
                        email-notify {
                            admin-email email-address;
                            custom-message message;
                            custom-message-subject message-subject;
                        }
                    }
                }
            }
        }
    }

```

```

interval value;
no-autoupdate;
proxy {
    password password-string;
    port port-number;
    server address-or-url;
    username name;
}
url url;
}
profile <name> {
    fallback-options {
        content-size (block | log-and-permit | permit);
        default (block | log-and-permit | permit);
        engine-not-ready (block | log-and-permit | permit);
        out-of-resources (block | log-and-permit | permit);
        timeout (block | log-and-permit | permit);
        too-many-requests (block | log-and-permit | permit);
    }
    notification-options {
        fallback-block {
            administrator-email email-address;
            allow-email;
            custom-message message;
            custom-message-subject message-subject;
            display-host;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
        fallback-non-block {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-recipient | no-notify-mail-recipient);
        }
        virus-detection {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
    }
    scan-options {
        content-size-limit value;
        (no-uri-check | uri-check);
        timeout value;
    }
    trickling {
        timeout value;
    }
}
sxl-retry value;
sxl-timeout seconds;
}
traceoptions {
    flag flag;
}

```

```

    url-whitelist listname;
}
content-filtering {
  profile profile-name {
    block-command protocol-command-list;
    block-content-type (activex | exe | http-cookie | java-applet | zip);
    block-extension extension-list;
    block-mime {
      exception list-name;
      list list-name;
    }
    notification-options {
      custom-message message;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
    permit-command protocol-command-list;
  }
  traceoptions {
    flag flag;
  }
}
web-filtering {
  juniper-enhanced {
    cache {
      size value;
      timeout value;
    }
    profile profile-name {
      block-message {
        type {
          custom-redirect-url;
        }
        url url;
      }
      quarantine-message {
        type {
          custom-redirect-url;
        }
        url url;
      }
    }
    category customurl-list name {
      action (block | log-and-permit | permit | quarantine);
    }
    custom-block-message value;
    custom-quarantine-message value;
    default (block | log-and-permit | permit | quarantine);
    fallback-settings {
      default (block | log-and-permit);
      server-connectivity (block | log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
    no-safe-search;
    site-reputation-action {
      fairly-safe (block | log-and-permit | permit | quarantine);
    }
  }
}

```

```

        harmful (block | log-and-permit | permit | quarantine);
        moderately-safe (block | log-and-permit | permit | quarantine);
        suspicious (block | log-and-permit | permit | quarantine);
        very-safe (block | log-and-permit | permit | quarantine);
    }
    timeout value;
}
server {
    host host-name;
    port number;
}
}
juniper-local {
    profile profile-name {
        custom-block-message value;
        default (block | log-and-permit | permit);
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        timeout value;
    }
}
}
traceoptions {
    flag flag;
}
url-blacklist listname;
url-whitelist listname;
websense-redirect {
    profile profile-name {
        account value;
        custom-block-message value;
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
    }
    server {
        host host-name;
        port number;
    }
    sockets value;
    timeout value;
}
}
}
}
ipc {
    traceoptions flag flag;
}
}
traceoptions {
    flag flag;
}
}

```

```

utm-policy policy-name {
  anti-spam {
    smtp-profile profile-name;
  }
  anti-virus {
    ftp {
      download-profile profile-name;
      upload-profile profile-name;
    }
    http-profile profile-name;
    imap-profile profile-name;
    pop3-profile profile-name;
    smtp-profile profile-name;
  }
  content-filtering {
    ftp {
      download-profile profile-name;
      upload-profile profile-name;
    }
    http-profile profile-name;
    imap-profile profile-name;
    pop3-profile profile-name;
    smtp-profile profile-name;
  }
  traffic-options {
    sessions-per-client {
      limit value;
      over-limit (block | log-and-permit);
    }
  }
  web-filtering {
    http-profile profile-name;
  }
}

```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Junos OS Release 9.5 .

**Description** Configure UTM features.

**Options** The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

## utm-policy

```
Syntax  utm-policy policy-name {
        anti-spam {
            smtp-profile profile-name;
        }
        anti-virus {
            ftp {
                download-profile profile-name;
                upload-profile profile-name;
            }
            http-profile profile-name;
            imap-profile profile-name;
            pop3-profile profile-name;
            smtp-profile profile-name;
        }
        content-filtering {
            ftp {
                download-profile profile-name;
                upload-profile profile-name;
            }
            http-profile profile-name;
            imap-profile profile-name;
            pop3-profile profile-name;
            smtp-profile profile-name;
        }
        traffic-options {
            sessions-per-client {
                limit value;
                over-limit (block | log-and-permit);
            }
        }
        web-filtering {
            http-profile profile-name;
        }
    }
```

**Hierarchy Level** [edit security utm]

**Release Information** Statement introduced in Junos OS Release 9.5.

**Description** Configure a UTM policy for antivirus, antispam, content-filtering, traffic-options, and Web-filtering protocols and attach this policy to a security profile to implement it.

**Options** *policy-name*—Specify name of the UTM policy.

The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- [Security Policies Overview](#)

- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*

## utm-policy (Application Services)

---

<b>Syntax</b>	utm-policy <i>policy-name</i> ;
<b>Hierarchy Level</b>	[edit security policies from-zone <i>zone-name</i> to-zone <i>zone-name</i> policy <i>policy-name</i> then permit application-services]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1.
<b>Description</b>	Configure a UTM policy for application services and attach this policy to a security profile to implement it.
<b>Options</b>	<i>policy-name</i> —Specify the name of the UTM policy.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## virus-detection (Security Antivirus)

---

<b>Syntax</b>	virus-detection { custom-message <i>message</i> ; custom-message-subject <i>message-subject</i> ; (notify-mail-sender   no-notify-mail-sender); type (message   protocol-only); }
<b>Hierarchy Level</b>	[edit security utm feature-profile anti-virus sophos-engine profile <i>profile-name</i> notification-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1 .
<b>Description</b>	Configure a notification to send when a virus is detected.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

## web-filtering

```

Syntax  web-filtering {
            url-whitelist custwhitelist;
            url-blacklist custblacklist;
            http-reassemble;
            http-persist;
            type juniper-enhanced;
            juniper-enhanced {
                cache {
                    timeout 1800;
                    size 500;
                }
                server {
                    host rp.cloud.threatseeker.com;
                    port 80;
                }
            }
            profile junos-wf-enhanced-default {
                category {
                    Enhanced_Hacking {
                        action log-and-permit;
                    }
                    Enhanced_Government {
                        action quarantine;
                    }
                }
                site-reputation-action {
                    very-safe permit;
                    moderately-safe log-and-permit;
                    fairly-safe log-and-permit;
                    harmful block;
                    suspicious block;
                }
                default block;
                custom-block-message "****access denied ****";
                fallback-settings {
                    default block;
                    server-connectivity block;
                    timeout block;
                    too-many-requests block;
                }
                timeout 10;
                no-safe-search;
            }
            utm-policy mypolicy {
                web-filtering {
                    http-profile my_ewfprofile01;
                }
            }
        }

```

**Hierarchy Level** [edit security utm feature-profile]

**Release Information** Statement introduced in Junos OS Release 9.5 .

<b>Description</b>	Configure UTM web-filtering features.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Understanding Local Web Filtering on page 112</a></li><li>• <a href="#">Monitoring Web Filtering Configurations on page 129</a></li></ul>

---

## websense-redirect

---

<b>Syntax</b>	<pre>websense-redirect {   profile <i>profile-name</i> {     account <i>value</i>;     custom-block-message <i>value</i>;     fallback-settings {       default (block   log-and-permit);       server-connectivity (block   log-and-permit);       timeout (block   log-and-permit);       too-many-requests (block   log-and-permit);     }     server {       host <i>host-name</i>;       port <i>number</i>;     }     sockets <i>value</i>;     timeout <i>value</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit security utm feature-profile web-filtering]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 .
<b>Description</b>	Configure the websense redirect engine features.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Example: Enhancing Security by Configuring Redirect Web Filtering Using Custom Objects on page 121</a></li></ul>

## CHAPTER 13

# Operational Commands

- clear security utm anti-spam statistics
- clear security utm antivirus statistics
- clear security utm content-filtering statistics
- clear security utm session
- clear security utm web-filtering statistics
- request security utm anti-virus sophos-engine
- request system license update
- show configuration smtp
- show groups junos-defaults
- show security log
- show security policies
- show security utm anti-spam statistics
- show security utm anti-spam status
- show security utm anti-virus statistics
- show security utm anti-virus status
- show security utm content-filtering statistics
- show security utm session
- show security utm status
- show security utm web-filtering statistics
- show security utm web-filtering status

## clear security utm anti-spam statistics

---

<b>Syntax</b>	clear security utm anti-spam statistics
<b>Release Information</b>	Command introduced in Junos OS Release 9.5 . Support for UTM in chassis cluster added in Junos OS Release 11.4 .
<b>Description</b>	Clear antispam statistics information. With chassis cluster support for UTM, statistics from both the nodes is cleared.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security utm anti-spam statistics on page 279</a></li><li>• <a href="#">show security utm anti-spam status on page 280</a></li></ul>
<b>Output Fields</b>	This command produces no output.

## Sample Output

### clear security utm anti-spam statistics

```
user@host> clear security utm anti-spam statistics
```

## clear security utm antivirus statistics

---

<b>Syntax</b>	clear security utm anti-virus statistics
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Support for Sophos Antivirus added in Junos OS Release 11.1. Support for UTM in chassis cluster added in Junos OS Release 11.4.
<b>Description</b>	Clear antivirus statistics information. With chassis cluster support for UTM, statistics from both the nodes are cleared.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security utm anti-virus statistics on page 281</a></li><li>• <a href="#">show security utm anti-virus status on page 283</a></li></ul>
<b>Output Fields</b>	This command produces no output.

## clear security utm content-filtering statistics

---

<b>Syntax</b>	clear security utm content-filtering statistics
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Support for UTM in chassis cluster added in Junos OS Release 11.4.
<b>Description</b>	Clear content-filtering statistics information. With chassis cluster support for UTM, statistics from both the nodes are cleared.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security utm content-filtering statistics on page 285</a></li></ul>
<b>Output Fields</b>	This command produces no output.

## clear security utm session

---

<b>Syntax</b>	clear security utm session
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Support for UTM in chassis cluster added in Junos OS Release 11.4.
<b>Description</b>	Clear UTM session information. With chassis cluster support for UTM, sessions on both the nodes are cleared.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security utm session on page 286</a></li><li>• <a href="#">show security utm status on page 287</a></li></ul>
<b>Output Fields</b>	This command produces no output.

## clear security utm web-filtering statistics

---

<b>Syntax</b>	clear security utm web-filtering statistics
<b>Release Information</b>	Command introduced in Junos OS Release 9.5 . Support for UTM in chassis cluster added in Junos OS Release 11.4 .
<b>Description</b>	Clear web filtering statistics information. With chassis cluster support for UTM, statistics from both the nodes is cleared.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security utm web-filtering statistics on page 288</a></li><li>• <a href="#">show security utm web-filtering status on page 291</a></li></ul>
<b>Output Fields</b>	This command produces no output.

## request security utm anti-virus sophos-engine

<b>Syntax</b>	request security utm anti-virus sophos-engine
<b>Release Information</b>	Command introduced in Junos OS Release 11.1 . Support for UTM in chassis cluster added in Junos OS Release 11.4 .
<b>Description</b>	Manually update the Sophos antivirus pattern database using the command described. To update automatically you use the configuration statement <b>set security utm feature-profile anti-virus sophos-engine pattern-update interval <i>seconds</i></b> . With full chassis cluster support for UTM this command is operational on both the nodes.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>pattern-delete</b> — Delete the current Sophos antivirus pattern database.</li> <li>• <b>pattern-reload</b> — Reload the Sophos antivirus pattern database.</li> <li>• <b>pattern-update</b> — Update the Sophos antivirus pattern database with the latest signatures.</li> </ul>
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear security utm antivirus statistics on page 259</a></li> <li>• <a href="#">show security utm anti-virus statistics on page 281</a></li> <li>• <a href="#">show security utm anti-virus status on page 283</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">request security utm anti-virus sophos-engine pattern-update on page 263</a>
<b>Output Fields</b>	request security utm anti-virus sophos-engine pattern-update  When you enter this command, you are provided feedback on the status of your request.

### Sample Output

#### request security utm anti-virus sophos-engine pattern-update

```
user@host> request security utm anti-virus sophos-engine pattern-update
```

## request system license update

---

<b>Syntax</b>	<code>request system license update</code>
<b>Release Information</b>	Command introduced in Junos OS Release 9.5.
<b>Description</b>	Start autoupdating license keys from the LMS server.
<b>Options</b>	<code>trial</code> —Starts autoupdating trial license keys from the LMS server.
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show system license (View)</a></li></ul>
<b>List of Sample Output</b>	<a href="#">request system license update on page 264</a> <a href="#">request system license update trial on page 264</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

### Sample Output

#### request system license update

```
user@host> request system license update
```

```
Request to automatically update license keys from https://ae1.juniper.net has  
been sent, use show system license to check status.
```

#### request system license update trial

```
user@host> request system license update trial
```

```
Request to automatically update trial license keys from https://ae1.juniper.net  
has been sent, use show system license to check status.
```

## show configuration smtp

<b>Syntax</b>	show configuration smtp
<b>Release Information</b>	Command introduced in Junos OS Release 10.0 .
<b>Description</b>	Display complete SMTP information.
<b>Options</b>	<ul style="list-style-type: none"> <li>• apply-groups—Groups from which SMTP inherits configuration data.</li> <li>• apply-groups-except—Groups from which SMTP restricts inheriting configuration data.</li> </ul>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">utm on page 248</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show configuration smtp on page 265</a>
<b>Output Fields</b>	<a href="#">Table 5 on page 265</a> describes the output fields for the <b>show configuration smtp</b> command.

Table 5: show configuration smtp

Field Name	Field Description	Level of Output
address	SMTP server's IPv4 address	All levels
login	Configure a mail sender account to the server	All levels
password	Default sender password for user authentication	All levels

## Sample Output

### show configuration smtp

```

user@host> show configuration smtp
primary-server {
    address 218.102.48.213;
    login "dayone@example.com" {
        password "$ABC123"; ## SECRET-DATA
    }
}

```

## show groups junos-defaults

---

**Syntax**    show groups junos-defaults

**Release Information**    Command introduced before Junos OS Release 7.4.

**Description**    Display the full set of available preset statements from the Junos OS defaults group.

```
user@host# show groups junos-defaults
groups {
  junos-defaults {
    applications {
      # File Transfer Protocol
      application junos-ftp {
        application-protocol ftp;
        protocol tcp;
        destination-port 21;
      }
      # Trivial File Transfer Protocol
      application junos-tftp {
        application-protocol tftp;
        protocol udp;
        destination-port 69;
      }
      # RPC port mapper on TCP
      application junos-rpc-portmap-tcp {
        application-protocol rpc-portmap;
        protocol tcp;
        destination-port 111;
      }
      # RPC port mapper on UDP
    }
  }
}
```

**Required Privilege Level**    view

**Related Documentation**

- [Using Junos OS Defaults Groups.](#)

## show security log

<b>Syntax</b>	<code>show security log {all  destination-address  destination-port  event-id  failure  interface-name  newer-than  older-than  process  protocol  severity  sort-by  source-address  source-port  success  user}</code>
<b>Release Information</b>	Command introduced in Junos OS Release 11.2 .
<b>Description</b>	Display security event logs. This command continuously displays security events on the screen. To stop the display, press Ctrl+c.
<b>Options</b>	<p><b>all</b>—Displays all audit event logs stored in the device memory.</p> <p><b>destination-address</b>—Displays audit event logs with the specified destination address.</p> <p><b>destination-port</b>—Displays audit event logs with the specified destination port.</p> <p><b>event-id</b>—Displays audit event logs with the specified event identification number.</p> <p><b>failure</b>—Displays failed audit event logs.</p> <p><b>interface-name</b>—Displays audit event logs with the specified interface.</p> <p><b>newer-than</b>—Displays audit event logs newer than the specified date and time.</p> <p><b>older-than</b>—Displays audit event logs older than the specified date and time.</p> <p><b>process</b>—Displays audit event logs with the specified process that generated the event.</p> <p><b>protocol</b>—Displays audit event logs generated through the specified protocol.</p> <p><b>severity</b>—Displays audit event logs generated with the specified severity.</p> <p><b>sort-by</b>—Displays audit event logs generated sorted with the specified options.</p> <p><b>source-address</b>—Displays audit event logs with the specified source address.</p> <p><b>source-port</b>—Displays audit event logs with the specified source port.</p> <p><b>success</b>—Displays successful audit event logs.</p> <p><b>username</b>—Displays audit event logs generated for the specified user.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>exclude (Security Log)</i></li> <li>• <i>clear security log</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security log on page 268</a>

**Output Fields** Table 6 on page 268 lists the output fields for the **show security log** command. Output fields are listed in the approximate order in which they appear.

**Table 6: show security log Output Fields**

Field Name	Field Description
Event time	The timestamp of the events received.  On SRX Series devices, security logs were always timestamped using the UTC time zone by running <b>set system time-zone utc</b> and <b>set security log utc-timestamp</b> CLI commands. Now, time zone can be defined using the local time zone by running the <b>set system time-zone time-zone</b> command to specify the local time zone that the system should use when timestamping the security logs.
Message	Security events are listed.

## Sample Output

### show security log

```

user@host> show security log
Event time      Message
2010-10-22 13:28:37 CST session created 1.1.1.2/1-->2.2.2.2/1308
icmp 1.1.1.2/1-->2.2.2.2/1308
None None 1 policy1 trustZone untrustZone 52 N/A(N/A) ge-0/0/1.0
2010-10-22 13:28:38 CST session created 1.1.1.2/1-->2.2.2.2/1308 icmp
1.1.1.2/1-->2.2.2.2/1308 None None 1 policy1 trustZone untrustZone 54 N/A(N/A)
ge-0/0/1.0

...

2010-10-22 13:36:12 CST session denied m icmp 1(8) policy1 trustZone untrustZone
N/A(N/A) ge-0/0/1.0
2010-10-22 13:36:14 CST session denied 1.1.1.2/2-->2.2.2.2/54812 icmp 1(8)
policy1 trustZone untrustZone N/A(N/A) ge-0/0/1.0

...

2010-10-27 15:50:11 CST IP spoofing! source: 2.2.2.20, destination: 2.2.2.2,
protocol-id: 17, zone name: trustZone, interface name: ge-0/0/1.0, action: drop
2010-10-27 15:50:11 CST IP spoofing! source: source: 2.2.2.20, destination:
2.2.2.2, protocol-id: 17, zone name: trustZone, interface name: ge-0/0/1.0, action:
drop

...

2011-02-18 15:53:34 CST PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/certification-authority/ca-profile1-ca1.cert
2011-02-18 15:53:35 CST PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/cr1/ca-profile1.cr1
2011-02-18 15:53:35 CST PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/system-key-pair/system-generated.priv
2011-02-18 15:53:35 CST PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/system-cert/system-generated.cert
2011-02-18 15:53:35 CST PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/key-pair/cert1.priv
2011-02-18 15:53:42 CST PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/key-pair/test2.priv

```

```

...
2011-03-14 23:00:40 PDT   IDP_COMMIT_COMPLETED: IDP policy commit is complete.
                        IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

, failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT   ]
                        IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

, failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT   ]
                        IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

, failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT   ]

...
Event time              Message
2011-03-21 14:21:49 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:01 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
9.9.9.1 source-address 6.6.6.1 .5 '
2011-03-21 14:23:05 CST  KMD_PM_SA_ESTABLISHED: Local gateway: 7.7.7.1, Remote
gateway: 8.8.8.1, Local ID: ipv4(any:0,[0..3]=6.6.6.1), Remote ID:
ipv4(any:0,[0..3]=9.9.9.1), Direction: inbound, SPI: 37a2a179, AUX-SPI: 0, Mode:
tunnel, Type: dynamic
2011-03-21 14:23:05 CST  KMD_PM_SA_ESTABLISHED: Local gateway: 7.7.7.1, Remote
gateway: 8.8.8.1, Local ID: ipv4(any:0,[0..3]=6.6.6.1), Remote ID:
ipv4(any:0,[0..3]=9.9.9.1), Direction: outbound, SPI: b2231c1f, AUX-SPI: 0, Mode:
tunnel, Type: dynamic
2011-03-21 14:23:08 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:13 CST  UI_CMDLINE_READ_LINE: User 'root', command 'show security
log '

```

## show security policies

---

<b>Syntax</b>	<code>show security policies</code> <code>&lt;detail&gt;</code> <code>&lt;none&gt;</code> <code>policy-name <i>policy-name</i></code> <code>&lt;detail&gt;</code> <code>&lt;global&gt;</code>
<b>Release Information</b>	Command modified in Junos OS Release 9.2. Support for IPv6 addresses added in Junos OS Release 10.2. Support for IPv6 addresses in active/active chassis cluster configurations in addition to the existing support of active/passive chassis cluster configurations added in Junos OS Release 10.4. Support for wildcard addresses added in Junos OS Release 11.1. Support for global policy added in Junos OS Release 11.4. Support for services offloading added in Junos OS Release 11.4. Support for source-identities added in Junos OS Release 12.1. The <b>Description</b> output field added in Junos OS Release 12.1. Support for negated address added in Junos OS Release 12.1X45-D10. The output fields for Policy Statistics expanded, and the output fields for the <b>global</b> and <b>policy-name</b> options expanded to include from-zone and to-zone global match criteria in Junos OS Release 12.1X47-D10. Support for the <b>initial-tcp-mss</b> and <b>reverse-tcp-mss</b> options added in Junos OS Release 12.3X48-D20. Output field and description for <b>source-end-user-profile</b> option added in Junos OS Release 15.1x49-D70.
<b>Description</b>	Display a summary of all security policies configured on the device. If a particular policy is specified, display information particular to that policy.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>none</b>—Display basic information about all configured policies.</li><li>• <b>detail</b>—(Optional) Display a detailed view of all of the policies configured on the device.</li><li>• <b>policy-name <i>policy-name</i></b>—(Optional) Display information about the specified policy.</li><li>• <b>global</b>—Display information about global policies.</li></ul>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Security Policies Overview</i></li><li>• <i>Understanding Security Policy Rules</i></li><li>• <i>Understanding Security Policy Elements</i></li></ul>
<b>List of Sample Output</b>	<a href="#">show security policies on page 273</a> <a href="#">show security policies policy-name p1 detail on page 274</a> <a href="#">show security policies (services-offload) on page 275</a> <a href="#">show security policies (device identity) on page 275</a> <a href="#">show security policies detail on page 275</a> <a href="#">show security policies detail (TCP Options) on page 276</a> <a href="#">show security policies policy-name p1 (Negated Address) on page 277</a> <a href="#">show security policies policy-name p1 detail (Negated Address) on page 277</a>

[show security policies global on page 277](#)

**Output Fields** [Table 7 on page 271](#) lists the output fields for the **show security policies** command. Output fields are listed in the approximate order in which they appear.

**Table 7: show security policies Output Fields**

Field Name	Field Description
From zone	Name of the source zone.
To zone	Name of the destination zone.
Policy	Name of the applicable policy.
Description	Description of the applicable policy.
State	Status of the policy: <ul style="list-style-type: none"> <li>• <b>enabled:</b> The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it.</li> <li>• <b>disabled:</b> The policy cannot be used in the policy lookup process, and therefore it is not available for access control.</li> </ul>
Index	Internal number associated with the policy.
Sequence number	Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, 4.
Source addresses	For standard display mode, the names of the source addresses for a policy. Address sets are resolved to their individual names.  For detail display mode, the names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs.
Destination addresses	Name of the destination address (or address set) as it was entered in the destination zone's address book. A packet's destination address must match this value for the policy to apply to it.
source-end-user-profile	Name of the device identity profile (also referred to as the end user profile) that contains attributes, or characteristics of a device. Specification of the device identity profile in the <b>source-end-user-profile</b> field is part of the device identity feature. If a device matches the attributes specified in the profile and other security policy parameters, then the security policy's action is applied to traffic issuing from the device.
Source addresses (excluded)	Name of the source address excluded from the policy.
Destination addresses (excluded)	Name of the destination address excluded from the policy.
Source identities	One or more user roles specified for a policy.

Table 7: show security policies Output Fields (*continued*)

Field Name	Field Description
Applications	<p>Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time.</p> <ul style="list-style-type: none"> <li>• <b>IP protocol</b>: The Internet protocol used by the application—for example, TCP, UDP, ICMP.</li> <li>• <b>ALG</b>: If an ALG is explicitly associated with the policy, the name of the ALG is displayed. If <b>application-protocol ignore</b> is configured, ignore is displayed. Otherwise, 0 is displayed. However, even if this command shows ALG: 0, ALGs might be triggered for packets destined to well-known ports on which ALGs are listening, unless ALGs are explicitly disabled or when <b>application-protocol ignore</b> is not configured for custom applications.</li> <li>• <b>Inactivity timeout</b>: Elapsed time without activity after which the application is terminated.</li> <li>• <b>Source port range</b>: The low-high source port range for the session application.</li> </ul>
Destination Address Translation	<p>Status of the destination address translation traffic:</p> <ul style="list-style-type: none"> <li>• <b>drop translated</b>—Drop the packets with translated destination addresses.</li> <li>• <b>drop untranslated</b>—Drop the packets without translated destination addresses.</li> </ul>
Application Firewall	<p>An application firewall includes the following:</p> <ul style="list-style-type: none"> <li>• <b>Rule-set</b>—Name of the rule set.</li> <li>• <b>Rule</b>—Name of the rule. <ul style="list-style-type: none"> <li>• <b>Dynamic applications</b>—Name of the applications.</li> <li>• <b>Dynamic application groups</b>—Name of the application groups.</li> <li>• <b>Action</b>—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following: <ul style="list-style-type: none"> <li>• <b>permit</b></li> <li>• <b>deny</b></li> </ul> </li> </ul> </li> <li>• <b>Default rule</b>—The default rule applied when the identified application is not specified in any rules of the rule set.</li> </ul>
Action or Action-type	<ul style="list-style-type: none"> <li>• The action taken in regard to a packet that matches the policy's tuples. Actions include the following: <ul style="list-style-type: none"> <li>• <b>permit</b></li> <li>• <b>firewall-authentication</b></li> <li>• <b>tunnel ipsec-vpn</b> <i>vpn-name</i></li> <li>• <b>pair-policy</b> <i>pair-policy-name</i></li> <li>• <b>source-nat pool</b> <i>pool-name</i></li> <li>• <b>pool-set</b> <i>pool-set-name</i></li> <li>• <b>interface</b></li> <li>• <b>destination-nat</b> <i>name</i></li> <li>• <b>deny</b></li> <li>• <b>reject</b></li> <li>• <b>services-offload</b></li> </ul> </li> </ul>
Session log	<p>Session log entry that indicates whether the <b>at-create</b> and <b>at-close</b> flags were set at configuration time to log session information.</p>

Table 7: show security policies Output Fields (*continued*)

Field Name	Field Description
<b>Scheduler name</b>	Name of a preconfigured scheduler whose schedule determines when the policy is active and can be used as a possible match for traffic.
<b>Policy statistics</b>	<ul style="list-style-type: none"> <li>• <b>Input bytes</b>—The total number of bytes presented for processing by the device. <ul style="list-style-type: none"> <li>• <b>Initial direction</b>—The number of bytes presented for processing by the device from the initial direction.</li> <li>• <b>Reply direction</b>—The number of bytes presented for processing by the device from the reply direction.</li> </ul> </li> <li>• <b>Output bytes</b>—The total number of bytes actually processed by the device. <ul style="list-style-type: none"> <li>• <b>Initial direction</b>—The number of bytes from the initial direction actually processed by the device.</li> <li>• <b>Reply direction</b>—The number of bytes from the reply direction actually processed by the device.</li> </ul> </li> <li>• <b>Input packets</b>—The total number of packets presented for processing by the device. <ul style="list-style-type: none"> <li>• <b>Initial direction</b>—The number of packets presented for processing by the device from the initial direction.</li> <li>• <b>Reply direction</b>—The number of packets presented for processing by the device from the reply direction.</li> </ul> </li> <li>• <b>Output packets</b>—The total number of packets actually processed by the device. <ul style="list-style-type: none"> <li>• <b>Initial direction</b>—The number of packets actually processed by the device from the initial direction.</li> <li>• <b>Reply direction</b>—The number of packets actually processed by the device from the reply direction.</li> </ul> </li> <li>• <b>Session rate</b>—The total number of active and deleted sessions.</li> <li>• <b>Active sessions</b>—The number of sessions currently present because of access control lookups that used this policy.</li> <li>• <b>Session deletions</b>—The number of sessions deleted since system startup.</li> <li>• <b>Policy lookups</b>—The number of times the policy was accessed to check for a match.</li> </ul> <p><b>NOTE:</b> Configure the Policy P1 with the <b>count</b> option to display policy statistics.</p>
<b>Per policy TCP Options</b>	Configured sync and sequence checks, and the configured TCP MSS value for the initial direction and /or the reverse direction.

## Sample Output

### show security policies

```

user@host> show security policies
From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Sequence number: 1
Source addresses:
sa-1-ipv4: 198.51.100.11/24
sa-2-ipv6: 2001:db8:a0b:12f0::1/32
sa-3-ipv6: 2001:db8:a0b:12f0::22/32
sa-4-wc: 203.0.113.1/255.255.0.255
Destination addresses:
da-1-ipv4: 2.2.2.2/24
da-2-ipv6: 2001:db8:a0b:12f0::8/32

```

```

da-3-ipv6: 2001:db8:a0b:12f0::9/32
da-4-wc: 192.168.22.11/255.255.0.255
Source identities: role1, role2, role4
Applications: any
Action: permit, application services, log, scheduled
Application firewall : my_ruleset1
Policy: p2, State: enabled, Index: 5, Sequence number: 2
Source addresses:
sa-1-ipv4: 198.51.100.11/24
sa-2-ipv6: 2001:db8:a0b:12f0::1/32
sa-3-ipv6: 2001:db8:a0b:12f0::22/32
Destination addresses:
da-1-ipv4: 2.2.2.2/24
da-2-ipv6: 2001:db8:a0b:12f0::1/32
da-3-ipv6: 2001:db8:a0b:12f0::9/32
Source identities: role1, role4
Applications: any
Action: deny, scheduled

```

#### show security policies policy-name p1 detail

```

user@host> show security policies policy-name p1 detail
Policy: p1, action-type: permit, State: enabled, Index: 4
Description: The policy p1 is for the sales team
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses:
sa-1-ipv4: 198.51.100.11/24
sa-2-ipv6: 2001:db8:a0b:12f0::1/32
sa-3-ipv6: 2001:db8:a0b:12f0::9/32
sa-4-wc: 203.0.113.1/255.255.0.255
Destination addresses:
da-1-ipv4: 2.2.2.2/24
da-2-ipv6: 2001:db8:a0b:12f0::1/32
da-3-ipv6: 2001:db8:a0b:12f0::9/32
da-4-wc: 192.168.22.11/255.255.0.255
Source identities:
role1
role2
role4
Application: any
IP protocol: 0, ALG: 0, Inactivity timeout: 0
Source port range: [0-0]
Destination port range: [0-0]
Destination Address Translation: drop translated
Application firewall :
Rule-set: my_ruleset1
Rule: rule1
Dynamic Applications: junos:FACEBOOK, junos:YMSG
Dynamic Application groups: junos:web, junos:chat
Action: deny
Default rule: permit
Session log: at-create, at-close
Scheduler name: sch20
Per policy TCP Options: SYN check: No, SEQ check: No
Policy statistics:
Input bytes      : 18144      545 bps
Initial direction: 9072      272 bps
Reply direction  : 9072      272 bps
Output bytes     : 18144      545 bps
Initial direction: 9072      272 bps

```

Reply direction :	9072	272 bps
Input packets :	216	6 pps
Initial direction:	108	3 bps
Reply direction :	108	3 bps
Output packets :	216	6 pps
Initial direction:	108	3 bps
Reply direction :	108	3 bps
Session rate :	108	3 sps
Active sessions :	93	
Session deletions :	15	
Policy lookups :	108	

#### show security policies (services-offload)

```

user@host> show security policies
Default policy: deny-all
From zone: trust, To zone: untrust
  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, services-offload, count
From zone: untrust, To zone: trust
  Policy: p2, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, services-offload

```

#### show security policies (device identity)

```

user@host > show security policies
From zone: trust, To zone: untrust
  Policy: dev-id-marketing, State: enabled, Index: 5, Scope Policy: 0,
Sequence number: 1
    Source addresses: any
    Destination addresses: any
    source-end-user-profile: marketing-profile
    Applications: any
    Action: permit

```

#### show security policies detail

```

user@host> show security policies detail
Default policy: deny-all
Policy: p1, action-type: permit, services-offload:enabled , State: enabled, Index:
4, Scope Policy: 0
  Policy Type: Configured
  Description: The policy p1 is for the sales team
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Source identities:
    role1
    role2

```

```

role4
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
  Source port range: [0-0]
  Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No
Policy statistics:
  Input bytes      :      18144      545 bps
  Initial direction:      9072      272 bps
  Reply direction  :      9072      272 bps
  Output bytes     :      18144      545 bps
  Initial direction:      9072      272 bps
  Reply direction  :      9072      272 bps
  Input packets    :        216        6 pps
  Initial direction:        108        3 bps
  Reply direction  :        108        3 bps
  Output packets   :        216        6 pps
  Initial direction:        108        3 bps
  Reply direction  :        108        3 bps
  Session rate     :        108        3 sps
  Active sessions  :         93
  Session deletions:         15
  Policy lookups   :         108
Policy: p2, action-type: permit, services-offload:enabled , State: enabled, Index:
5, Scope Policy: 0
Policy Type: Configured
Description: The policy p2 is for the sales team
Sequence number: 1
From zone: untrust, To zone: trust
Source addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Source identities:
role1
role2
role4
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
  Source port range: [0-0]
  Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No

```

#### show security policies detail (TCP Options)

```

user@host> show security policies policy-name policy1 detail
node0:
-----
Policy: policy1, action-type: permit, State: enabled, Index: 7, Scope Policy: 0
Policy Type: Configured
Sequence number: 2
From zone: trust, To zone: untrust
Source addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Application: any

```

```

IP protocol: 0, ALG: 0, Inactivity timeout: 0
Source port range: [0-0]
Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No
Per policy TCP MSS: initial: 800, reverse: 900

```

### show security policies policy-name p1 (Negated Address)

```

user@host>show security policies policy-name p1
node0:
-----
From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
Source addresses(excluded): as1
Destination addresses(excluded): as2
Applications: any
Action: permit

```

### show security policies policy-name p1 detail (Negated Address)

```

user@host>show security policies policy-name p1 detail
node0:
-----
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
Policy Type: Configured
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses(excluded):
  ad1(ad): 255.255.255.255/32
  ad2(ad): 198.51.100.1/24
  ad3(ad): 198.51.100.6 ~ 198.51.100.56
  ad4(ad): 192.0.2.8/24
  ad5(ad): 198.51.100.99 ~ 198.51.100.199
  ad6(ad): 203.0.113.9/24
  ad7(ad): 203.0.113.23/24
Destination addresses(excluded):
  ad13(ad2): 198.51.100.76/24
  ad12(ad2): 198.51.100.88/24
  ad11(ad2): 192.0.2.23 ~ 192.0.2.66
  ad10(ad2): 192.0.2.93
  ad9(ad2): 203.0.113.76 ~ 203.0.113.106
  ad8(ad2): 203.0.113.199
Application: any
IP protocol: 0, ALG: 0, Inactivity timeout: 0
Source port range: [0-0]
Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No

```

### show security policies global

```

user@host>show security policies global policy-name Pa
node0:
-----
Global policies:
Policy: Pa, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
From zones: zone1, zone2
To zones: zone3, zone4 Source addresses: any
Destination addresses: any
Applications: any
Action: permit

```



## show security utm anti-spam statistics

<b>Syntax</b>	show security utm anti-spam statistics
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Support for UTM in chassis cluster added in Junos OS Release 11.4.
<b>Description</b>	Display antispam statistics for connections including total e-mail scanned, tagged, and dropped connections.  Statistics from both the nodes (with full chassis cluster support for UTM) are displayed.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear security utm anti-spam statistics on page 258</a></li> <li>• <a href="#">show security utm anti-spam status on page 280</a></li> </ul>
<b>Output Fields</b>	show security utm anti-spam statistics  Output fields are listed in the approximate order in which they appear.

## show security utm anti-spam statistics

```

user@host> show security utm anti-spam statistics
Total connections:    0
Denied connections:   0
Total greetings:      0
Denied greetings:     0
Total e-mail scanned: 0
White list hit:       0
Black list hit:       0
Spam total:           0
Spam tagged:          0
Spam dropped:         0
DNS errors:           0
Timeout errors:       0
Return errors:        0
Invalid parameter errors: 0

```

## show security utm anti-spam status

---

<b>Syntax</b>	show security utm anti-spam status
<b>Release Information</b>	Command introduced in Junos OS Release 9.5 . Support for UTM in chassis cluster added in Junos OS Release 11.4 .
<b>Description</b>	Display antispam status for connections including whitelist and blacklist server information. Status of both the nodes (with full chassis cluster support for UTM) is displayed.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">clear security utm anti-spam statistics on page 258</a></li><li>• <a href="#">show security utm anti-spam statistics on page 279</a></li></ul>
<b>Output Fields</b>	show security utm anti-spam status  Output fields are listed in the approximate order in which they appear.

## show security utm anti-spam status

```
user@host> show security utm anti-spam status
SBL Whitelist Server:
SBL Blacklist Server:
    msgsecurity.example.net

DNS Server:
  Primary   :    1.2.3.4, Src Interface: ge-0/0/0
  Secondary :    0.0.0.0, Src Interface: ge-0/0/1
  Ternary   :    0.0.0.0, Src Interface: fe-0/0/2
```

## show security utm anti-virus statistics

<b>Syntax</b>	show security utm anti-virus statistics <fpc <fpc-slot <i>fpc-slot</i> pic-slot <i>pic-slot</i> >>
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Support for Sophos Antivirus added in Junos OS Release 11.1. Support for UTM in chassis cluster added in Junos OS Release 11.4. Support for Flexible PIC Concentrator (FPC) and PIC status added in Junos OS Release 12.1X46-D10.
<b>Description</b>	Display antivirus statistics for connections including clean and infected files, scan engine status, and aggregated statistics from all FPCs and PICs. Statistics from both the nodes (with full chassis cluster support for UTM) are displayed.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear security utm antivirus statistics on page 259</a></li> <li>• <a href="#">show security utm anti-virus status on page 283</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security utm anti-virus statistics on page 281</a> <a href="#">show security utm anti-virus statistics fpc on page 281</a> <a href="#">show security utm anti-virus statistics fpc fpc-slot 5 pic-slot 0 on page 282</a>
<b>Output Fields</b>	show security utm anti-virus statistics  Output fields are listed in the approximate order in which they appear.

## Sample Output

### show security utm anti-virus statistics

```

user@host>show security utm anti-virus statistics
  UTM Anti Virus statistics:
  MIME-whitelist passed:           0
  URL-whitelist passed:            0
  Scan Request:
                                     Total      Clean      Threat-found      Fallback
                                     0          0          0          0

  Fallback:
                                     Log-and-Permit      Block      Permit
  Engine not ready:                0          0          0
  Out of resources:                0          0          0
  Timeout:                        0          0          0
  Maximum content size:            0          0          0
  Too many requests:              0          0          0
  Others:                         0          0          0

```

### show security utm anti-virus statistics fpc

```

user@host>show security utm anti-virus statistics fpc

fpc-slot 5 pic-slot 0

```

## UTM Anti Virus statistics:

MIME-whitelist passed: 0

URL-whitelist passed: 0

Scan Request:

Total	Clean	Threat-found	Fallback
0	0	0	0

## Fallback:

	Log-and-Permit	Block	Permit
Engine not ready:	0	0	0
Out of resources:	0	0	0
Timeout:	0	0	0
Maximum content size:	0	0	0
Too many requests:	0	0	0
Others:	0	0	0

## show security utm anti-virus statistics fpc fpc-slot 5 pic-slot 0

user@host&gt;show security utm anti-virus statistics fpc fpc-slot 5 pic-slot 0

## UTM Anti Virus statistics:

MIME-whitelist passed: 0

URL-whitelist passed: 0

Scan Request:

Total	Clean	Threat-found	Fallback
0	0	0	0

## Fallback:

	Log-and-Permit	Block	Permit
Engine not ready:	0	0	0
Out of resources:	0	0	0
Timeout:	0	0	0
Maximum content size:	0	0	0
Too many requests:	0	0	0
Others:	0	0	0

## show security utm anti-virus status

<b>Syntax</b>	show security utm anti-virus status <fpc <fpc-slot <i>fpc-slot</i> pic-slot <i>pic-slot</i> >>
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Support for UTM in chassis cluster added in Junos OS Release 11.4. Support for Flexible PIC Concentrator (FPC) and PIC status added in Junos OS Release 12.1X46-D10.
<b>Description</b>	Display antivirus status for connections including clean and infected files, scan engine status, and aggregated status from all FPCs and PICs. Status of both the nodes (with full chassis cluster support for UTM) is displayed.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear security utm antivirus statistics on page 259</a></li> <li>• <a href="#">show security utm anti-virus statistics on page 281</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security utm anti-virus status on page 283</a> <a href="#">show security utm anti-virus status fpc on page 283</a> <a href="#">show security utm anti-virus status fpc fpc-slot 5 pic-slot 0 on page 284</a>
<b>Output Fields</b>	show security utm anti-virus status  Output fields are listed in the approximate order in which they appear.

## Sample Output

### show security utm anti-virus status

```

user@host> show security utm anti-virus status
UTM anti-virus status:

Anti-virus key expire date: 2017-04-01 00:00:00
Update server: https://update.juniper-updates.net/SAV/
Interval: 1440 minutes
Pattern update status: next update in 1439 minutes
Last result: new database downloaded
Anti-virus signature version: 1.13 (1.02)
Scan engine type: sophos-engine
Scan engine information: last action result: No error

```

### show security utm anti-virus status fpc

```

user@host> show security utm anti-virus status fpc
fpc-slot 5 pic-slot 0
UTM anti-virus status:

Anti-virus key expire date: license not installed
Update server: http://update.juniper-updates.net/SAV/
Interval: 1440 minutes
Pattern update status: update disabled due to no license
Last result: already have latest database
Anti-virus signature version: 000000_00

```

```
Scan engine type: sophos-engine  
Scan engine information: last action result: No error
```

#### show security utm anti-virus status fpc fpc-slot 5 pic-slot 0

```
user@host> show security utm anti-virus status fpc fpc-slot 5 pic-slot 0  
UTM anti-virus status:  
  
Anti-virus key expire date: license not installed  
Update server: http://update.juniper-updates.net/SAV/  
Interval: 1440 minutes  
Pattern update status: update disabled due to no license  
Last result: already have latest database  
Anti-virus signature version: 000000_00  
Scan engine type: sophos-engine  
Scan engine information: last action result: No error
```

## show security utm content-filtering statistics

<b>Syntax</b>	show security utm content-filtering statistics
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Support for UTM in chassis cluster added in Junos OS Release 11.4.
<b>Description</b>	Display content-filtering statistics for connections including lists of blocked files and the reasons for blocking. Statistics from both the nodes (with full chassis cluster support for UTM) are displayed.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear security utm content-filtering statistics on page 260</a></li> </ul>
<b>Output Fields</b>	show security utm content-filtering statistics  Output fields are listed in the approximate order in which they appear.

## show security utm content-filtering statistics

```

user@host> show security utm content-filtering statistics
Content-filtering-statistic:      Blocked
Base on command list:            0
Base on mime list:               0
Base on extension list:          0
ActiveX plugin:                  0
Java applet:                     0
EXE files:                       0
ZIP files:                       0
HTTP cookie:                     0

```

## show security utm session

---

<b>Syntax</b>	show security utm session
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Support for UTM in chassis cluster added in Junos OS Release 11.4.
<b>Description</b>	Display general UTM session information including all allocated sessions and active sessions. Also, display information from both nodes in a chassis cluster.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">clear security utm session on page 261</a></li><li>• <a href="#">show security utm status on page 287</a></li></ul>
<b>Output Fields</b>	show security utm session  When you enter this command, you are provided feedback on the status of your request.

## show security utm session

```
user@host> show security utm session
Maximum sessions:      4000
Total allocated sessions: 0
Total freed sessions:  0
Active sessions:       0
```

## show security utm status

---

<b>Syntax</b>	show security utm status
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Support for UTM in chassis cluster added in Junos OS Release 11.4.
<b>Description</b>	Display whether the UTM service is running or not and status of both the nodes (with full chassis cluster support for UTM).
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">clear security utm session on page 261</a></li><li>• <a href="#">show security utm session on page 286</a></li></ul>
<b>Output Fields</b>	show security utm status  When you enter this command, you are provided feedback on the status of your request.

## show security utm status

```
user@host> show security utm status
UTM service status: Running
```

## show security utm web-filtering statistics

<b>Syntax</b>	show security utm web-filtering statistics <fpc <fpc-slot fpc-slot pic-slot pic-slot>>
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Support for UTM in chassis cluster added in Junos OS Release 11.4. Support for Flexible PIC Concentrator (FPC) and PIC statistics added in Junos OS Release 12.1X46-D10.
<b>Description</b>	Display Web filtering statistics for connections including whitelist and blacklist hits and custom category hits. The aggregated statistics from all FPCs and PICs and statistics from both the nodes (with full chassis cluster support for UTM) are also displayed.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear security utm web-filtering statistics on page 262</a></li> <li>• <a href="#">show security utm web-filtering status on page 291</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security utm web-filtering statistics on page 288</a> <a href="#">show security utm web-filtering statistics fpc on page 289</a> <a href="#">show security utm web-filtering statistics fpc fpc-slot 5 pic-slot 0 on page 289</a>
<b>Output Fields</b>	show security utm web-filtering statistics  Output fields are listed in the approximate order in which they appear.

## Sample Output

### show security utm web-filtering statistics

```

user@host> show security utm web-filtering statistics
UTM web-filtering statistics:
  Total requests:                0
  white list hit:                 0
  Black list hit:                 0
  Queries to server:              0
  Server reply permit:            0
  Server reply block:             0
  Server reply quarantine:         0
  Server reply quarantine block:   0
  Server reply quarantine permit:  0
  Custom category permit:          0
  Custom category block:           0
  Custom category quarantine:      0
  Custom category quarantine block: 0
  Custom category quarantine permit: 0
  Site reputation permit:          0
  Site reputation block:           0
  Site reputation quarantine:      0
  Site reputation quarantine block: 0
  Site reputation quarantine permit: 0
  Site reputation by Category      0
  Site reputation by Global        0
  Cache hit permit:               0

```

```

Cache hit block:                0
Cache hit quarantine:           0
Cache hit quarantine block:     0
Cache hit quarantine permit:    0
Safe-search redirect:           0
Web-filtering sessions in total: 128000
Web-filtering sessions in use:  0
Fallback:                       log-and-permit      block
    Default                     0                0
    Timeout                     0                0
    Connectivity                 0                0
    Too-many-requests            0                0

```

### show security utm web-filtering statistics fpc

```
user@host> show security utm web-filtering statistics fpc
```

```

fpc-slot 5 pic-slot 0
UTM web-filtering statistics:
  Total requests:                0
  white list hit:                0
  Black list hit:                0
  Queries to server:             0
  Server reply permit:           0
  Server reply block:            0
  Server reply quarantine:        0
  Server reply quarantine block:  0
  Server reply quarantine permit: 0
  Custom category permit:         0
  Custom category block:          0
  Custom category quarantine:      0
  Custom category quarantine block: 0
  Custom category quarantine permit: 0
  Site reputation permit:         0
  Site reputation block:          0
  Site reputation quarantine:      0
  Site reputation quarantine block: 0
  Site reputation quarantine permit: 0
  Site reputation by Category     0
  Site reputation by Global       0
  Cache hit permit:               0
  Cache hit block:                0
  Cache hit quarantine:           0
  Cache hit quarantine block:     0
  Cache hit quarantine permit:    0
  Safe-search redirect:           0
  Web-filtering sessions in total: 128000
  Web-filtering sessions in use:  0
  Fallback:                       log-and-permit      block
    Default                     0                0
    Timeout                     0                0
    Connectivity                 0                0
    Too-many-requests            0                0

```

### show security utm web-filtering statistics fpc fpc-slot 5 pic-slot 0

```

user@host> show security utm web-filtering statistics fpc fpc-slot 5 pic-slot 0
UTM web-filtering statistics:
  Total requests:                0
  white list hit:                0

```

Black list hit:	0	
Queries to server:	0	
Server reply permit:	0	
Server reply block:	0	
Server reply quarantine:	0	
Server reply quarantine block:	0	
Server reply quarantine permit:	0	
Custom category permit:	0	
Custom category block:	0	
Custom category quarantine:	0	
Custom category quarantine block:	0	
Custom category quarantine permit:	0	
Site reputation permit:	0	
Site reputation block:	0	
Site reputation quarantine:	0	
Site reputation quarantine block:	0	
Site reputation quarantine permit:	0	
Site reputation by Category	0	
Site reputation by Global	0	
Cache hit permit:	0	
Cache hit block:	0	
Cache hit quarantine:	0	
Cache hit quarantine block:	0	
Cache hit quarantine permit:	0	
Safe-search redirect:	0	
Web-filtering sessions in total:	128000	
Web-filtering sessions in use:	0	
Fallback:	log-and-permit	block
Default	0	0
Timeout	0	0
Connectivity	0	0
Too-many-requests	0	0

## show security utm web-filtering status

<b>Syntax</b>	show security utm web-filtering status <fpc <fpc-slot fpc-slot pic-slot pic-slot>>
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Support for UTM in chassis cluster added in Junos OS Release 11.4. Support for Flexible PIC Concentrator (FPC) and PIC status added in Junos OS Release 12.1X46-D10.
<b>Description</b>	Display whether the Web filtering server connection is up or not. The aggregated status from all FPCs and PICs and status of both the nodes (with full chassis cluster support for UTM) are also displayed.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear security utm web-filtering statistics on page 262</a></li> <li>• <a href="#">show security utm web-filtering statistics on page 288</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security utm web-filtering status on page 291</a> <a href="#">show security utm web-filtering status fpc on page 291</a> <a href="#">show security utm web-filtering status fpc fpc-slot 5 pic-slot 0 on page 291</a>
<b>Output Fields</b>	show security utm web-filtering status  Output fields are listed in the approximate order in which they appear.

## Sample Output

### show security utm web-filtering status

```
user@host> show security utm web-filtering status
UTM web-filtering status:
  Server status: Juniper Enhanced using Websense server UP
```

### show security utm web-filtering status fpc

```
user@host> show security utm web-filtering status fpc
UTM web-filtering status fpc:
  fpc-slot 5 pic-slot 0
  Connectivity status: UP
  fpc-slot 0 pic-slot 1
  Connectivity status: UP
```

### show security utm web-filtering status fpc fpc-slot 5 pic-slot 0

```
user@host> show security utm web-filtering status fpc fpc-slot 5 pic-slot 0
UTM web-filtering status:
  Connectivity status: UP
```

