



# TELEPATH USER GUIDE

**Version 2.5**

May 2014

## **COPYRIGHT NOTICE**

**© 2014Hybrid Application Security, Inc. All Rights Reserved.**

This document is for informational purposes only. Hybrid Application Security, Inc. makes no warranties, expressed or implied. No part of this document may be used, disclosed, reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Hybrid Security, Inc.

Information in this document is subject to change without notice and does not represent a commitment on the part of Hybrid Security, Inc.

The software described in this document is furnished under a license agreement. The software may be used only in accordance with the terms of this agreement.

This document contains proprietary and confidential information of Hybrid Security, Inc., and is intended solely for the use of authorized Hybrid Security customers. The information furnished in this document is believed to be accurate and reliable. However, no responsibility is assumed by Hybrid Security, Inc. for the use of this material.

## **TRADEMARK ATTRIBUTIONS**

All other brand and product names are trademarks or registered trademarks of their respective owners.

Portions of the software described in this document have been developed by the following third parties, and their respective rights are listed below. Note that some of these products in turn incorporate software developed by additional third parties.

<b>Third Party Product</b>	<b>Developer</b>
Arbor	<a href="http://arborjs.org/">http://arborjs.org/</a>
Bro	<a href="http://www.bro.org">http://www.bro.org</a>
Boost	<a href="http://www.boost.org">http://www.boost.org</a>
FamFamFam	<a href="http://www.famfamfam.com">http://www.famfamfam.com</a>
Gulp	<a href="http://staff.washington.edu/corey/gulp/">http://staff.washington.edu/corey/gulp/</a>
JIT	<a href="http://philogb.github.io/jit/">http://philogb.github.io/jit/</a>
JSON	<a href="http://jsoncpp.sourceforge.net">http://jsoncpp.sourceforge.net</a>
LibMySQL	<a href="http://www.mysql.com">http://www.mysql.com</a>
LibPCAP	<a href="http://www.tcpdump.org">http://www.tcpdump.org</a>
MaxMind	<a href="http://www.maxmind.com">http://www.maxmind.com</a>
Mini-XML	<a href="http://www.msweet.org">http://www.msweet.org</a>
Nokia OVI Maps	<a href="http://api.maps.ovi.com/">http://api.maps.ovi.com/</a>
OpenSSL	<a href="http://www.openssl.org">http://www.openssl.org</a>
Oracle MySQL	<a href="http://www.mysql.com">http://www.mysql.com</a>
Sencha	<a href="http://www.sencha.com/">http://www.sencha.com/</a>
Zlib	<a href="http://zlib.net">http://zlib.net</a>

## **CONTACT INFORMATION**

Email: [info@hybridsec.com](mailto:info@hybridsec.com)

Phone: +1 (650) 319-7389

## Table of Contents

<b>Overview.....</b>	<b>5</b>
<b>Scope.....</b>	<b>5</b>
<b>Hybrid Security Telepath .....</b>	<b>5</b>
<b>Scope.....</b>	<b>6</b>
<b>Hybrid Security Telepath .....</b>	<b>6</b>
<b>Prerequisites.....</b>	<b>6</b>
<b>Hardware.....</b>	<b>6</b>
Minimum Requirements.....	6
Disk Requirements.....	6
Browser.....	6
<b>Software.....</b>	<b>7</b>
<b>Installing Ubuntu.....</b>	<b>7</b>
<b>Installing MySQL.....</b>	<b>7</b>
<b>Network Configuration.....</b>	<b>8</b>
<b>Installing Telepath.....</b>	<b>8</b>
<b>Installing Telepath repository.....</b>	<b>8</b>
<b>Running Configuration Utility.....</b>	<b>9</b>
<b>Configuring Telepath.....</b>	<b>10</b>
<b>Initial Configuration.....</b>	<b>10</b>
<b>Starting and Stopping Telepath.....</b>	<b>12</b>
<b>Uninstalling Telepath.....</b>	<b>13</b>
<b>Backing Up and Restoring the Telepath Database.....</b>	<b>13</b>
<b>Telepath Logs.....</b>	<b>13</b>
<b>Telepath Knowledgebase.....</b>	<b>13</b>
<b>Telepath in a VMware Environment.....</b>	<b>13</b>
<b>Allocating Hardware Resources.....</b>	<b>13</b>
<b>Configuring the Virtual Switch.....</b>	<b>14</b>
<b>Starting the Telepath GUI.....</b>	<b>15</b>
<b>Telepath Status Indicators.....</b>	<b>16</b>
<b>Rules.....</b>	<b>16</b>
<b>Defining Rule Categories .....</b>	<b>17</b>
<b>Defining a New Category.....</b>	<b>18</b>
<b>Editing an Existing Category.....</b>	<b>18</b>
<b>Deleting an Existing Category.....</b>	<b>18</b>
<b>Defining Rules .....</b>	<b>19</b>
<b>Defining a New Rule .....</b>	<b>19</b>
<b>Editing an Existing Rule .....</b>	<b>20</b>
<b>Disabling an Existing rule.....</b>	<b>20</b>

<b>Deleting an Existing Rule .....</b>	<b>20</b>
<b>Rule Parameters.....</b>	<b>21</b>
<b>Defining Criteria.....</b>	<b>21</b>
<b>Defining a New Criterion.....</b>	<b>21</b>
Parameter Criteria.....	22
Behavior Criteria.....	23
Pattern Criteria.....	24
Geographic Criteria.....	24
Bot-Intelligence Criteria .....	25
<b>Disabling a Criterion.....</b>	<b>25</b>
<b>Editing an Existing Criterion .....</b>	<b>26</b>
<b>Deleting an Existing Criterion .....</b>	<b>26</b>
<b>Telepath Dashboard.....</b>	<b>26</b>
<b>Dashboard Settings Pane.....</b>	<b>28</b>
<b>Attacks Pane.....</b>	<b>28</b>
<b>Hot Spots Pane.....</b>	<b>29</b>
<b>Attack Origins Pane.....</b>	<b>29</b>
<b>Alert Trends Pane.....</b>	<b>29</b>
<b>Top Suspects Pane.....</b>	<b>29</b>
<b>Sessions Pane.....</b>	<b>30</b>
<b>Alerts.....</b>	<b>30</b>
<b>Filtering the Alerts Display.....</b>	<b>32</b>
<b>Session Flow.....</b>	<b>32</b>
<b>Investigate.....</b>	<b>33</b>
<b>Business Actions.....</b>	<b>35</b>
<b>Settings.....</b>	<b>36</b>
<b>Administration.....</b>	<b>37</b>
Users.....	37
37.....	Adding New Users
38.....	Editing Users
38.....	Deleting Users
39.....	Viewing a User's Activity History
Groups.....	39
39.....	Adding New Groups
40.....	Editing Groups
40.....	Deleting Groups
40.....	Viewing a Group's Activity History
Activity Log.....	41
<b>Network.....</b>	<b>41</b>
Load Balancer IPs.....	41
Load Balancer Headers.....	42

SMTP Configuration.....	42
IP Whitelist.....	43
Proxy Configuration.....	43
Remote Syslog Server.....	44
Network Interfaces.....	44
User Agent Ignore List.....	44
Extension Ignore List.....	45
<b>Operation Mode.....</b>	<b>45</b>
<b>Reports.....</b>	<b>46</b>
<b>Web Applications.....</b>	<b>47</b>
Web Application - Nodes List.....	47
48.....Creating applications	
48.....Editing Applications	
48.....Searching the Nodes List	
49.....Uploading Application Logs to Telepath	
49.....Deleting Applications	
Web Application - General.....	49
Web Application - Authentication.....	50
Web Application - SSL.....	51
Web Application - Advanced.....	51
51.....Application Global Pages	
52.....API Settings	
<b>Parameter rules .....</b>	<b>54</b>
<b>Pattern Rules.....</b>	<b>56</b>
<b>Geographic Rules.....</b>	<b>58</b>
<b>Behavior Rules.....</b>	<b>60</b>
<b>Grouping different criterions under one rule.....</b>	<b>61</b>
<b>Telepath Engine not starting after Telepath installation.....</b>	<b>64</b>

# Introduction

---

## Overview

### Scope

This publication is intended for administrators tasked with installing and configuring Hybrid Security Telepath. A basic familiarity on the part of the reader with networking and database concepts and tools is assumed.

### Hybrid Security Telepath

Hybrid Security Telepath monitors the behavior of all web application users, both inside and outside the organization.

Telepath uses advanced artificial intelligence algorithms to build profiles of user behavior, adjusted over time according to the dynamic history of each user's activities. Telepath learns the "rules of the game" unique to each web application, and alerts administrators when it detects suspicious behavioral scenarios.

Telepath monitors web traffic passing through a switch configured to mirror traffic to the Telepath server.

# Installation and Initial Configuration

---

## Scope

This publication is intended for administrators tasked with configuring and installing Hybrid Security Telepath. A basic familiarity on the part of the reader with networking and database concepts and tools is assumed.

## Hybrid Security Telepath

Hybrid Security Telepath monitors the behavior of all web application users, both inside and outside the organization.

Telepath uses advanced artificial intelligence algorithms to build profiles of user behavior, adjusted over time according to the dynamic history of each user's activities. Telepath learns the "rules of the game" unique to each web application, and alerts administrators when it detects suspicious behavioral scenarios.

Telepath monitors web traffic passing through a switch configured to mirror traffic to the Telepath server.

## Prerequisites

### Hardware

#### Minimum Requirements



For information about installing and running Telepath in a VMware environment, see .

The minimum hardware requirements for the Telepath server are the following:

- 32 GB RAM
- 8 core CPU

### Disk Requirements

The disk space required by Telepath depends on the number of monitored sessions and the period of time you need to store information online before archiving (backing up).

You can estimate your disk requirements based on the following "rule of thumb":

An average-sized HTTP request requires about 1.5 KB of disk space, or about 150 GB for 100 million requests.

Your requirements may vary depending on the specific characteristics of your web traffic.

## Browser

The Telepath GUI runs in the following supported browsers:

- Google Chrome
- Mozilla Firefox
- Internet Explorer

It is recommended that you use the latest version of the browser.

## Software

Before installing and configuring Telepath, you will perform the following tasks, which are described in detail in the next sections:

1. Install a supported version of Ubuntu (12 , 13 or 14) on the Telepath server.
2. Install MySQL 5 or above on the Telepath server.

## Installing Ubuntu



The Telepath server must have access to the Internet for this process.

### To install Ubuntu:

1. Log in to the Telepath server machine as root.
2. Go to <http://www.ubuntu.com/download/server>.
3. Download the 64-bit version of one of the following Ubuntu OS server versions:
  - Precise (12)
  - Raring (13)
  - Trusty (14)
4. Install the Ubuntu OS server you just downloaded.

## Installing MySQL



The Telepath server must have access to the Internet for this process.

### To install MySQL:

1. Log in to the Telepath server machine as root.
2. Go to <http://dev.mysql.com/downloads/>.
3. Download MySQL 5 or above.
4. Install the version you just downloaded.

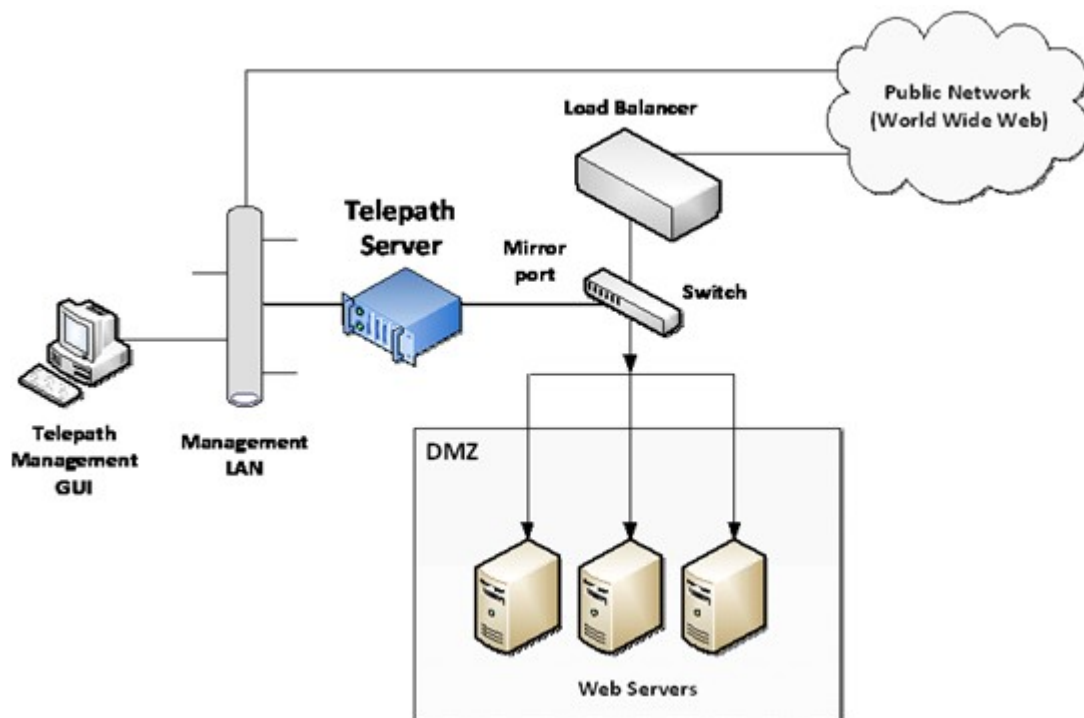


# Network Configuration

The figure below depicts a network configuration in which the Telepath server monitors traffic to the web servers. The critical issues are that:

- The Telepath server is positioned so that it can monitor all the relevant traffic.
- It is not possible to initiate a connection to the Telepath server from outside the management LAN.
- The Telepath server can initiate access to the Hybrid Security site through the management LAN in order to periodically download Telepath intelligence, for example, the IP addresses of malicious bots, hacking tools, blacklisted IP addresses, etc.

Since every network is unique, you should regard the depicted configuration only as a suggestion.



Typical Network Configuration

## Installing Telepath

Installation is a two-step process: installing the repository and running the configuration utility.

### Installing Telepath repository

1. Log into the Telepath server machine as root.



The Telepath server must have access to the Internet for downloading and installing Telepath.

2. Install the Telepath repository by executing one of the following commands, depending on the OS version.

#### **Ubuntu 12 (Precise)**

```
grep 192.241.171.59 /etc/apt/sources.list || echo "deb  
http://192.241.171.59/repo/deb precise main" >>  
/etc/apt/sources.list
```

#### **Ubuntu 13 (Raring)**

```
grep 192.241.171.59 /etc/apt/sources.list || echo "deb  
http://192.241.171.59/repo/deb raring main" >>  
/etc/apt/sources.list
```

#### **Ubuntu 14 (Trusty)**

```
grep 192.241.171.59 /etc/apt/sources.list || echo "deb  
http://192.241.171.59/repo/deb trusty main" >>  
/etc/apt/sources.list
```

#### **CentOS/RHEL 6.5 (Final)**

```
echo 0 >/selinux/enforce  
echo -e  
"[telepath]\nname=Telepath\nbaseurl=http://hybridsec.com/rep  
o/yum\nngpgcheck=0" > /etc/yum.repos.d/Telepath.repo
```

3. Install the Telepath server by executing the following command:

```
yum install telepath
```

4. Next, run the configuration utility.

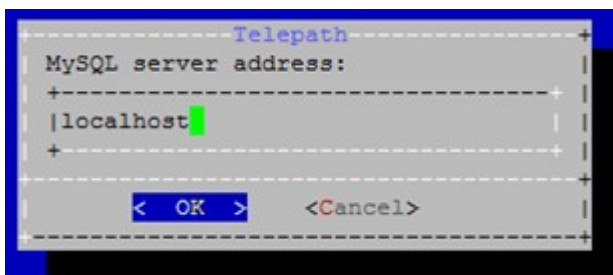
```
/opt/telepath/configure.sh
```

## Running Configuration Utility

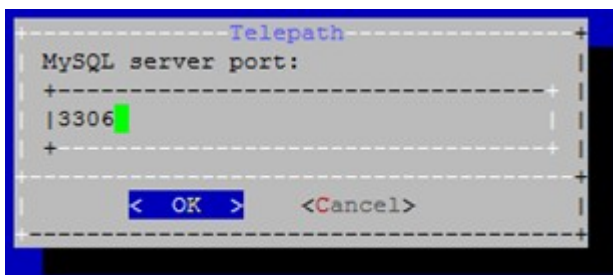
1. Select the interfaces (eth0, eth1, etc.) to which the sniffed traffic will be directed.



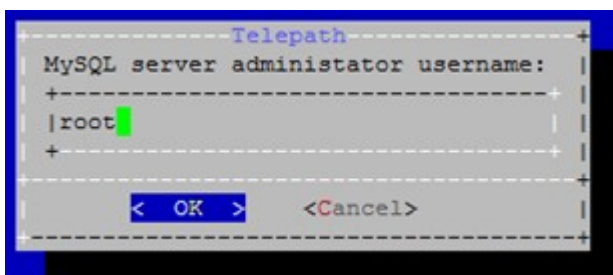
2. Enter the location of the Telepath database. Specify the IP address of the MySQL server.



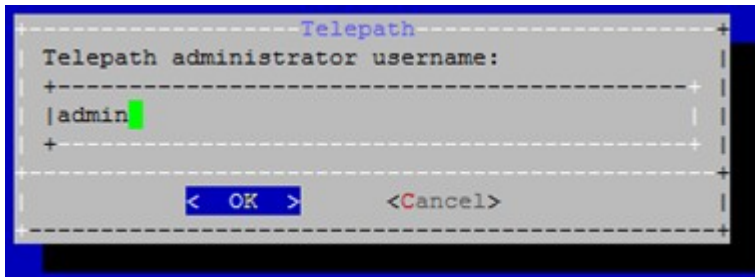
3. Specify the MySQL port. (Default is 3306).



4. The MySQL server administrator (root) user name and password.



5. Configure your Telepath administrator username and password.



6. Physically install ("rack") the Telepath server into your internal network. See on page 9 for one possible configuration.
  - Connect the sniffing interface you specified during the Telepath installation (step above) to the switch whose traffic will be mirrored.
  - On another interface, connect the Telepath server to the management LAN.
7. Power up and boot the Telepath server.
8. Confirm that the Telepath server can be accessed from the management LAN, using standard network tools such as the ping command.
9. Connect the switch to the Telepath server's sniffing interface.
10. Configure the switch so that it copies the relevant traffic to the Telepath server.

You must configure the switch so that traffic you want Telepath to monitor is copied to the Telepath server.

Different switch manufacturers use different terminology for this functionality: port mirroring, TAP, SPAN, etc. For information on how to configure this functionality for your switch, refer to its documentation.
11. Using standard network tools, confirm that the switch is copying the relevant traffic to the Telepath server.
12. Next, configure Telepath as appropriate.

## Configuring Telepath

This section guides you on how to customize the Telepath configuration to your network and your specific requirements.

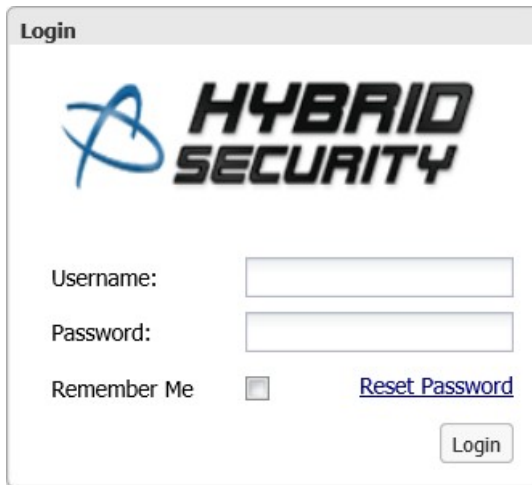
### Initial Configuration



For best results, use the latest Google Chrome or Firefox browser.

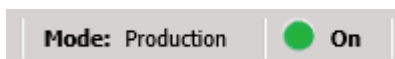
To configure Telepath:

1. From your web browser, go to the URL which was displayed at the end of the installation (of the form **http://<IP address>/telepath**). The Login window is displayed.



The image shows a web browser window titled "Login". Inside the window, there is a logo for "HYBRID SECURITY" with a blue stylized 'H' icon. Below the logo, there are two input fields: "Username:" and "Password:". Below the "Password:" field, there is a "Remember Me" checkbox and a "Reset Password" link. At the bottom right of the login area, there is a "Login" button.

2. In the **Login** window, enter your credentials (**User-Name** and **Password**) and click **Sign In**.



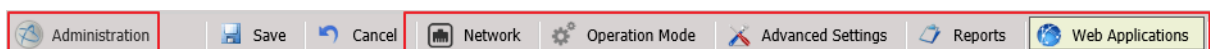
3. In the **Telepath Status** pane, confirm that:

- **Engine** is **On**.
- **Operation Mode** is **Training**.

If the values are different, you can change them as follows:

Field	Where to change
<b>Engine/Sniffer</b> status	Click the <b>Telepath Status On / Off</b> button in the top bar.
<b>Operation Mode</b>	<b>Settings</b> tab > <b>Mode</b> option

4. Click the **Settings** tab.





**Settings** tab options



If you change any of the settings, remember to click **Save** at the top of the **Settings** tab.

5. In the Settings tab, click **Network**.



In all the **Network** panes, you can add an item to a list by entering its information and clicking **Add**, delete an item by selecting it and clicking the trash icon  and configure an item by selecting it and clicking the settings icon .

6. If the Telepath server is behind a load balancer, enable **Web servers are behind a load balancer** and add the load balancer's IP addresses in the **Load Balancers** pane.

Load Balancer IPs

☒ Web servers are behind a load balancer

IP 

Add

Load balancer IP

10.236.2.4		
10.236.2.5		
10.236.2.6		
10.237.2.4		
10.236.2.102		
10.236.2.103		
10.236.2.104		
10.236.2.105		
10.236.2.6		
10.236.2.7		

7. The **Load Balancer Headers** pane displays the header fields added by the load balancer which specify, among other information, a packet's original IP address. You can change this list if required.

Load Balancer Headers

Header 

Add

Load balancer Headers

CLIENT_IP		
-----------	--	--

8. The **User Agent Ignore List** pane displays the user agents (typically” harmless’ bots) whose traffic Telepath should ignore. You can change this list if required.

**User Agent Ignore List**

User-Agent  Add

User-Agent		
baiduspider		
yandex		
yahoo		
facebookexternalhit		
adsbot-google		
msnbot-media		
googlebot		

9. The **IP Whitelist** pane displays the IP addresses from which Telepath should ignore all traffic. You can change this list if required.

**IP Whitelist**

Add IP(s)

IP		
192.168.1.1		
192.168.1.2		
172.17.0.1		
172.16.0.1		
172.16.0.2		
192.168.1.10		
192.168.1.11		
192.168.1.12		
192.168.1.13		
192.168.1.14		
192.168.1.15		
192.168.1.16		
192.168.1.17		
192.168.1.18		
192.168.1.19		
192.168.1.20		
192.168.1.21		
192.168.1.22		
192.168.1.23		
192.168.1.24		
192.168.1.25		
192.168.1.26		
192.168.1.27		
192.168.1.28		
192.168.1.29		
192.168.1.30		
192.168.1.31		
192.168.1.32		
192.168.1.33		
192.168.1.34		
192.168.1.35		
192.168.1.36		
192.168.1.37		
192.168.1.38		
192.168.1.39		
192.168.1.40		
192.168.1.41		
192.168.1.42		
192.168.1.43		
192.168.1.44		
192.168.1.45		
192.168.1.46		
192.168.1.47		
192.168.1.48		
192.168.1.49		
192.168.1.50		
192.168.1.51		
192.168.1.52		
192.168.1.53		
192.168.1.54		
192.168.1.55		
192.168.1.56		
192.168.1.57		
192.168.1.58		
192.168.1.59		
192.168.1.60		
192.168.1.61		
192.168.1.62		
192.168.1.63		
192.168.1.64		
192.168.1.65		
192.168.1.66		
192.168.1.67		
192.168.1.68		
192.168.1.69		
192.168.1.70		
192.168.1.71		
192.168.1.72		
192.168.1.73		
192.168.1.74		
192.168.1.75		
192.168.1.76		
192.168.1.77		
192.168.1.78		
192.168.1.79		
192.168.1.80		
192.168.1.81		
192.168.1.82		
192.168.1.83		
192.168.1.84		
192.168.1.85		
192.168.1.86		
192.168.1.87		
192.168.1.88		
192.168.1.89		
192.168.1.90		
192.168.1.91		
192.168.1.92		
192.168.1.93		
192.168.1.94		
192.168.1.95		
192.168.1.96		
192.168.1.97		
192.168.1.98		
192.168.1.99		
192.168.1.100		
192.168.1.101		
192.168.1.102		
192.168.1.103		
192.168.1.104		
192.168.1.105		
192.168.1.106		
192.168.1.107		
192.168.1.108		
192.168.1.109		
192.168.1.110		
192.168.1.111		
192.168.1.112		
192.168.1.113		
192.168.1.114		
192.168.1.115		
192.168.1.116		
192.168.1.117		
192.168.1.118		
192.168.1.119		
192.168.1.120		
192.168.1.121		
192.168.1.122		
192.168.1.123		
192.168.1.124		
192.168.1.125		
192.168.1.126		
192.168.1.127		
192.168.1.128		
192.168.1.129		
192.168.1.130		
192.168.1.131		
192.168.1.132		
192.168.1.133		
192.168.1.134		
192.168.1.135		
192.168.1.136		
192.168.1.137		
192.168.1.138		
192.168.1.139		
192.168.1.140		
192.168.1.141		
192.168.1.142		
192.168.1.143		
192.168.1.144		
192.168.1.145		
192.168.1.146		
192.168.1.147		
192.168.1.148		
192.168.1.149		
192.168.1.150		
192.168.1.151		
192.168.1.152		
192.168.1.153		
192.168.1.154		
192.168.1.155		
192.168.1.156		
192.168.1.157		
192.168.1.158		
192.168.1.159		
192.168.1.160		
192.168.1.161		
192.168.1.162		
192.168.1.163		
192.168.1.164		
192.168.1.165		
192.168.1.166		
192.168.1.167		
192.168.1.168		
192.168.1.169		
192.168.1.170		
192.168.1.171		
192.168.1.172		
192.168.1.173		
192.168.1.174		
192.168.1.175		
192.168.1.176		
192.168.1.177		
192.168.1.178		
192.168.1.179		
192.168.1.180		
192.168.1.181		
192.168.1.182		
192.168.1.183		
192.168.1.184		
192.168.1.185		
192.168.1.186		
192.168.1.187		
192.168.1.188		
192.168.1.189		
192.168.1.190		
192.168.1.191		
192.168.1.192		
192.168.1.193		
192.168.1.194		
192.168.1.195		
192.168.1.196		
192.168.1.197		
192.168.1.198		
192.168.1.199		
192.168.1.200		
192.168.1.201		
192.168.1.202		
192.168.1.203		
192.168.1.204		
192.168.1.205		
192.168.1.206		
192.168.1.207		
192.168.1.208		
192.168.1.209		
192.168.1.210		
192.168.1.211		
192.168.1.212		
192.168.1.213		
192.168.1.214		
192.168.1.215		
192.168.1.216		
192.168.1.217		
192.168.1.218		
192.168.1.219		
192.168.1.220		
192.168.1.221		
192.168.1.222		
192.168.1.223		
192.168.1.224		
192.168.1.225		
192.168.1.226		
192.168.1.227		
192.168.1.228		
192.168.1.229		
192.168.1.230		
192.168.1.231		
192.168.1.232		
192.168.1.233		
192.168.1.234		
192.168.1.235		
192.168.1.236		
192.168.1.237		
192.168.1.238		
192.168.1.239		
192.168.1.240		
192.168.1.241		
192.168.1.242		
192.168.1.243		
192.168.1.244		
192.168.1.245		
192.168.1.246		
192.168.1.247		
192.168.1.248		
192.168.1.249		
192.168.1.250		
192.168.1.251		
192.168.1.252		
192.168.1.253		
192.168.1.254		
192.168.1.255		

10. The **Extension Ignore List** pane displays the file extensions (for example, of graphic files) which Telepath should ignore. You can change this list if required.

The screenshot shows the 'Extension Ignore List' configuration pane. At the top, there is a header 'Extension Ignore List'. Below it, there is a text input field labeled 'Extension' and an 'Add' button. Below this is a table with the following structure:

Ignore Extension		
jpg		
jpeg		
gif		
css		
ico		
png		
swf		
ashx		

11. If your management LAN's Internet traffic requires a proxy server, then in the **Proxy Configuration** pane, set:

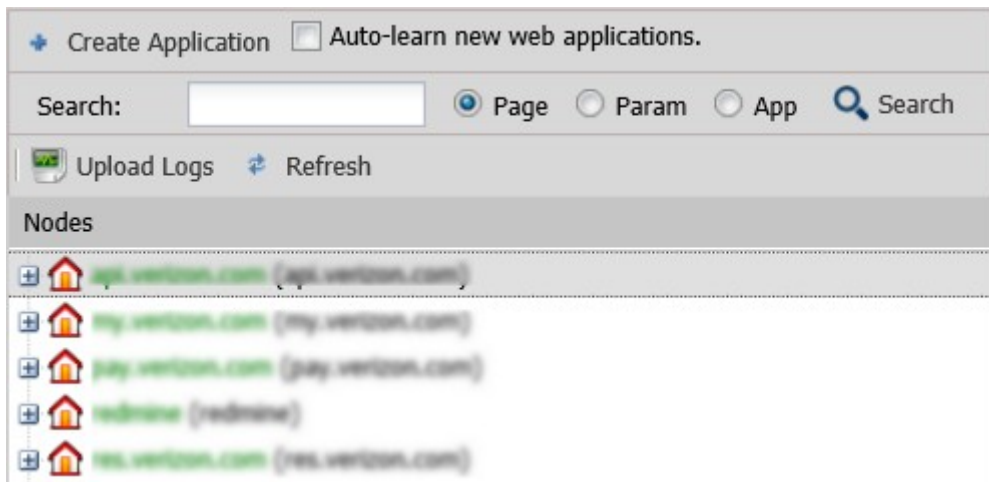
- **Proxy** to **On**
- **IP Address** to the corporate proxy server's IP address
- **Port** to the corporate proxy server's proxy port

The screenshot shows the 'Proxy Configuration' pane. It has a header 'Proxy Configuration'. Below it, there is a 'Proxy' section with two radio buttons: 'On' (selected) and 'Off'. Below this, there is an 'IP' section with a text input field containing '127.0.0.1'. Below that, there is a 'Port' section with a text input field containing '8123' and a small up/down arrow button.

12. In the Settings tab (), click **Web Applications**.

By the time you reach this point in the configuration process, Telepath will have been monitoring traffic long enough to have learned a list of your web applications, which is displayed in the left pane.





13. To edit an application, select it in the list and enter the data in the right pane. You can specify authentication and SSL parameters by clicking the buttons on the bottom.

## Starting and Stopping Telepath

To start the Telepath server, execute the following command:

```
telepath start
```

To stop the Telepath server, execute the following command:

```
telepath stop
```

## Uninstalling Telepath

To completely uninstall the Telepath server, execute the following command:

```
apt-get remove --purge telepath
```

## Backing Up and Restoring the Telepath Database

Telepath stores its data in a MySQL database. The DB name is "Telepath".



It is the user's responsibility to ensure that the database files are periodically backed up.

### Telepath Logs

Telepath stores logs in its MySQL database. The database files are located in the `/opt/telepath/db/sql/telepath` directory. The file names include the date range for the logs.

At regular intervals, Telepath closes the current log files and opens new ones. The Telepath GUI has access to all the database files on the disk, from the currently open database files as well as from earlier database files. This file division is transparent to the user.

When disk usage reaches 95% of available space, Telepath deletes the oldest database files in order to be able to allocate space for new data. It is essential that you monitor disk usage and regularly backup the database files (using the standard MySQL administration tools) so that no data are lost.

To avoid data loss, go to the `/opt/telepath/db/sql/telepath` directory and make sure you back up the .MYI and .MYD files beginning with the following filenames (e.g.

request\_scores\_from\_2013\_11\_22\_10\_39\_18\_to\_2013\_11\_27\_14\_44\_02.MYI):

- Request\_scores\_from\_
- Attribute\_scores\_from\_
- Alerts\_from \_
- Top\_suspects\_from\_

## Telepath Knowledgebase

The Telepath Knowledgebase consists of the information Telepath has learned about the web applications and users it monitors. The Knowledgebase files are stored in the `/opt/telepath/db/kb` directory.

# Telepath in a VMware Environment

In a VMware environment, you install and configure Telepath on one of the virtual machines in the same way that you would on a physical machine. There are however a number of considerations unique to the virtual environment.

## Allocating Hardware Resources

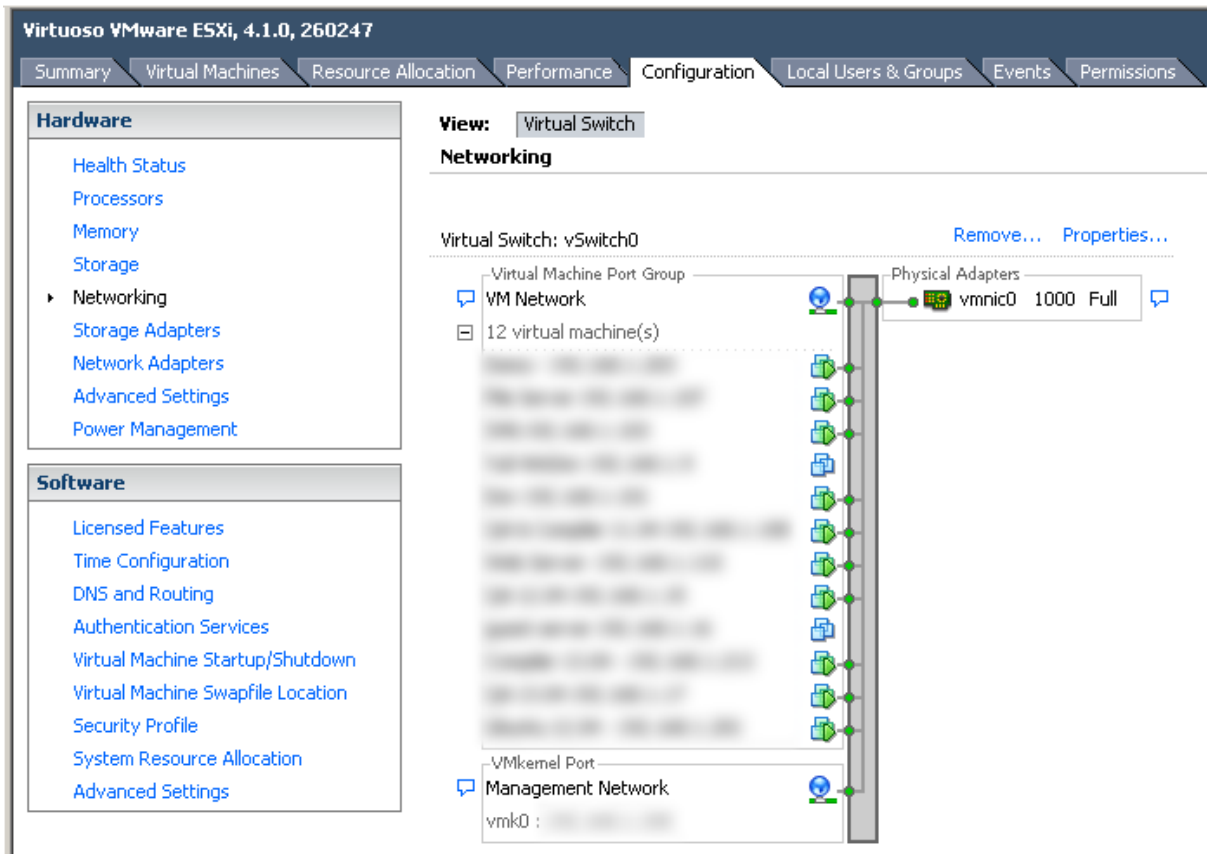
In a VMware environment, all hardware resources are shared among the virtual machines. In order to ensure Telepath's optimal performance, you must reserve adequate hardware resources exclusively for its use, as described in on page 7.

Refer to the VMware documentation for information on how to reserve hardware resources.

## Configuring the Virtual Switch

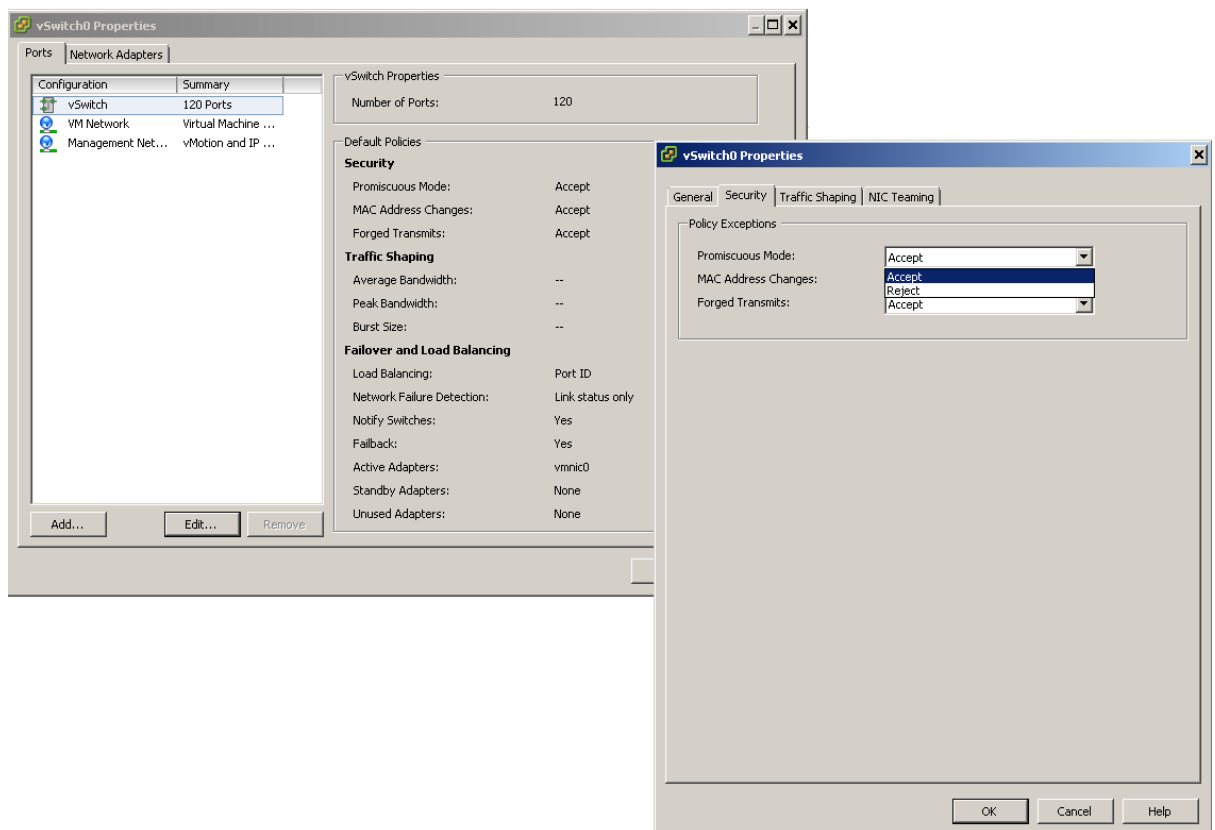
You must configure the virtual switch as follows:

1. Connect to the ESX server using the vSphere client software.
2. In the vSphere client main menu, go to the root of the virtual machines tree.
3. Click the **Configuration** tab in the upper menu.
4. In the **Hardware** pane, select **Networking**.
5. To the right of the virtual switch, click **Properties**.



6. Select the switch you want to configure and click **Edit**.
7. In the **Properties** window, click the **Security** tab.

8. Under **Policy Exceptions**, set **Promiscuous Mode** to **Accept**.



9. Click **OK**.

# Configuring Telepath



For best results, please use the latest Google Chrome or Firefox browser.

## Starting the Telepath GUI

### To start the Telepath GUI:

1. Open your web browser and go to **http://<IP address>/telepath**, where <IP address> is the interface of the Telepath server that faces the management LAN. The Login window is displayed.

A screenshot of the Telepath Login window. The window has a title bar that says "Login". Inside, there is a logo for "HYBRID SECURITY" with a blue stylized 'H' and 'S'. Below the logo, there are two input fields: "Username:" and "Password:". Below the "Password:" field, there is a "Remember Me" checkbox and a "Reset Password" link. At the bottom right, there is a "Login" button.

2. In the **Login** window, enter your credentials (**User-Name** and **Password**).  
You can optionally select **Remember me** to have Telepath automatically log you in the next time you open the application. To reset your password, click **Reset Password** and follow the directions.
3. Click **Login**.



After 3 successive failed login attempts, Telepath will lock out for 15 minutes.

If the login is successful, the Telepath GUI is displayed with the **Dashboard** tab initially in focus. The Telepath GUI has 6 tabs, as follows:

Tab	For more information, see
<b>Dashboard</b>	
<b>Alerts</b>	-
<b>Investigate</b>	-
<b>Business Actions</b>	

Tab	For more information, see
<b>Rules</b>	Error: Reference source not found
<b>Settings</b>	



The system does not automatically start after install. Make sure you turn on the engine by clicking the **Off** button in the tabs bar or issuing "telepath start" via command-line.

## Telepath Status Indicators

The tabs bar indicates the Telepath engine and sniffer's activation status, and the system's operation mode.



### Dashboard - Telepath Status indicators

Field	Description
<b>Learning Time Left</b>	<p>(Displayed in Training operation mode) If <b>Operation Mode</b> is Learning or Hybrid, this is the time left until learning stops.</p> <p>To change the times during which Telepath learns when in Hybrid mode, click the <b>Configure Schedule</b> in the <b>Operation Mode</b> window of the <b>Settings</b> tab.</p>
<b>On/Off button</b> (Engine/sniffer status button)	<p>Indicates whether the Telepath engine and sniffer are <b>On</b> or <b>Off</b>, that is, whether Telepath is monitoring traffic.</p> <p>To change the engine and sniffer status, click the engine/sniffer status button (red circle) in the tabs bar.</p> <p>For the engine version, click <b>Help &gt; About</b>.</p>



The Telepath engine processes the traffic it receives from the sniffer. If the engine and sniffer are off, the monitored traffic is ignored by the Telepath server.

Field	Description
<b>Mode</b>	<p>The operation mode can be:</p> <ul style="list-style-type: none"> <li>• <b>Training</b> - Telepath monitors web applications and learns their behavior, but does not alert when it detects anomalous activity. When Telepath is first installed, it remains in <b>Training</b> mode for the period specified in the <b>Training Level</b> option in the <b>Settings</b> tab, measured by either elapsed time or the number of requests processed by Telepath.</li> <li>• <b>Production</b> - Telepath monitors web applications and alerts when it detects anomalous activity.</li> <li>• <b>Hybrid</b> - Telepath monitors web applications and alerts when it detects anomalous activity, and in addition, it also continues to learn application behavior during the hours specified under <b>Hybrid Mode Schedule</b> in the <b>Operation Mode</b> window of the <b>Settings</b> tab.</li> </ul> <p>You can change the value of <b>Operation Mode</b> in the <b>Operation Mode</b> window in the <b>Settings</b> tab.</p>

## Rules

Rules define behavior patterns for which Telepath issues an alert.

For example, a rule might define conditions, or criteria, which indicate whether the user's IP address has changed in the course of the session. Criteria can be either pre-defined or user-defined.

There are three kinds of criteria:

- Pattern and behavior criteria – Pattern criteria predefined in Telepath which are inaccessible to Telepath administrators. Pattern criteria are defined or updated by Hybrid Security while behavior criteria look for anomalous behavior based on different user behavior perspectives, including queries, navigation speed, geographic location or navigation pattern – which pages are visited.

These criteria are applied only after learning has completed.

- Hybrid Intelligence criteria – criteria predefined in Telepath which Telepath administrators can view. These criteria are periodically updated by the Hybrid Security intelligence cloud.
- User-defined criteria – defined by Telepath administrators.

When all the criteria of a rule are matched for a session, we say that we have a “match” on the rule, and an alert is generated.

There are five types of rules, as follows:

Criterion Type	Description
Parameter Rule	A rule which relates to anomalies in a session's parameters.
Behavior Rule	A rule which relates to some characteristic of the session.
Pattern Rule	A rule which detects anomalous patterns in a session.
Geographic Rule	A rule which relates to anomalies in the geographic source of a session.
Bot-Intelligence Rule	A rule which detects the presence of bots rather than human users.

Rules are arranged in categories. Each category contains any number of rules, and each rule contains any number of criterions.



Rule with criterions

In the figure above, the category **MyRules** consists of the single rule **Bad Guys**, which consists in turn of three criterions: **Geo Suspect**, **Password Brute-Force Attack** and **Scraping**.

All the rules, except for disabled rules, are applied to all monitored traffic. Criterions within a rule are AND'ed, while rules and categories are OR'ed.



## EXAMPLE



Rules structure

In the case of the two categories (**MyRules** and **Web Fraud**) shown above, a session is identified as anomalous if, for example:

- There is a match on **all** of the criteria within the **Bad Guys** rule: **Geo Suspect**, **Password Brute-Force Attack** and **Scraping**.
- There is a match on **any** of the following rules: **Mass Passports per IP**, **Mass Phones per IP**, **Mass Requests per IP**, or **Multiple Credit Cards**.

Because each of these rules has only one criterion, matching the criterion means matching the rule, and because rules are OR'ed, it is enough for any criterion to be matched for Telepath to identify the session as anomalous.

On the other hand, a session is **not** identified as anomalous if, for example:

- There is a match on **two** of the following criteria: **Geo Suspect**, **Password Brute-Force Attack** and **Scraping**.

Because the criteria in the **Bad Guys** rule are AND'ed, there is no match on the rule unless all the criteria in the rule are matched.

To summarize,

- To define a criterion that identifies an anomalous session even if no other criteria are matched, define that criterion as the only one in its rule.
- To define a set of criteria that identify an anomalous session only if all the criteria are matched, define a rule that consists of all these criteria but no additional ones.

# Defining Rule Categories

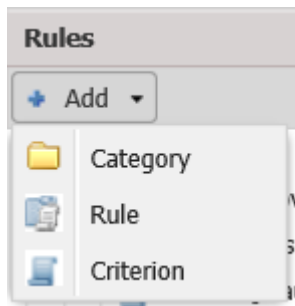


Telepath's predefined rules are grouped in the predefined **Hybrid Rules** category. You can change these rules, but the next time Telepath is updated, your changes will be lost.

## Defining a New Category

**To define a new category:**

1. Click the **Rules** tab.
2. In the **Rules** pane on the left, click **Add**.



3. From the menu, select **Category**.
4. In the **New Category** window, enter a **Category Name**.
5. Click **Create**.

## Editing an Existing Category

**To edit an existing category:**

1. Click the **Rules** tab.
2. In the **Rules** pane on the left, select a category.
3. Click **Edit**.
4. From the menu, select **Category**.
5. In the **Edit Category** window, enter a new **Category Name**.
6. Click **Create**.

## Deleting an Existing Category

**To delete an existing category:**

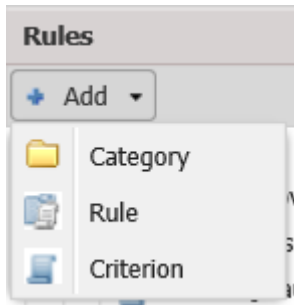
1. Click the **Rules** tab.
2. In the **Rules** pane on the left, select a category.
3. Click **Delete**.
4. In the **Delete Category** window, confirm the deletion.

# Defining Rules

## Defining a New Rule

To define a new rule:

1. Click the **Rules** tab.
2. In the **Rules** pane on the left, click **Add**.



3. From the menu, select **Rule**.

A screenshot of the 'New Rule' dialog box. The dialog has a title bar with 'New Rule' and a close button. Inside, there are two input fields: 'Category' with a dropdown menu showing 'Please select a category' and 'Rule Name' with a text box showing 'Please enter a name'. At the bottom right, there is a 'Create' button.

4. In the **New Rule** dialog, enter the following data:

Field	Description
<b>Category</b>	The name of the category to which the new rule belongs.
<b>Rule Name</b>	The name of the new rule.

5. Click **Create** and then click **OK** in the confirmation window that appears.
6. In the **Rules** pane on the left, select the rule you just created.
7. Enter the rule's parameters as defined in .

## Editing an Existing Rule

To edit an existing rule:

1. Click the **Rules** tab.
2. In the **Rules** pane on the left, select a rule.
3. Click **Edit**.
4. Enter the rule's parameters as defined in .
5. Click **Save**.

## Disabling an Existing rule

**To disable a rule:**

1. Click the **Rules** tab.
2. In the **Rules** pane on the left, right-click a rule and select **Disable all criteria**.
3. Click **OK** in the confirmation window that appears.

## Deleting an Existing Rule

**To delete an existing rule:**

1. Click the **Rules** tab.
2. In the **Rules** pane on the left, select a rule.
3. Click **Delete**.
4. In the **Delete Rule** window, confirm the deletion.

## Rule Parameters



A rule's parameters are as follows:

Field	Description
<b>Name</b>	The name of the new rule.

Field	Description
-------	-------------

## Actions

The action to be taken – in addition to alerting – if the rule is matched, that is, if all the enabled criterions in the rule are matched. Enable one or more of the following options:

- **Syslog** – A syslog will be sent to the syslog server (defined in the **Logs & Alerts** pane of the **Configuration** tab.
- **Header Injection** – Notify a Telepath agent installed on the application server to inject a header into the incoming web traffic which the application recognizes as a signal to terminate the session. For more information, see .
- **Flow** – Select a flow to associate with the alert.
- **Email** – An email will be sent to the specified email addresses. To add an address to the list, enter it in **Address** and click **Add**. You can change or delete addresses in the list using the  and  icons.

Note the **Log** option is always enabled.



To receive email alerts, the [SMTP Server](#) configured. For syslog alerts, the Remote Syslog Server must be defined.

## Parameters to show upon alert for the rule

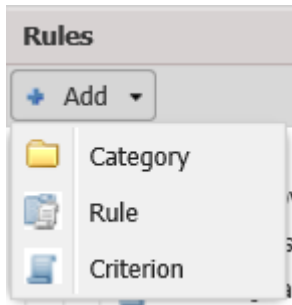
To add a parameter that will be included in the alert data when the rule is matched, click **Add** and select the parameter in the **Parameters** window by navigating to the application page, selecting parameters from the **Headers**, **GET** or **POST** lists and clicking **Add**. The new parameters will appear for alerts matching this rule only.

# Defining Criteria

## Defining a New Criterion

To define a new criterion:

1. Click the **Rules** tab.
2. In the **Rules** pane on the left, click **Add**.



3. From the menu, select **Criterion**.

The Rules Wizard opens, presenting you with a series of screens where you will specify the parameters that define the criterion.

A screenshot of a 'Category and Rule' configuration screen. It has a title bar 'Category and Rule'. The screen is divided into two main sections: 'Category' and 'Rule'. In the 'Category' section, there are two radio buttons: 'Create a new category' (unselected) and 'Add to existing category' (selected). Next to 'Add to existing category' is a dropdown menu showing 'MyRules'. In the 'Rule' section, there are also two radio buttons: 'Create a new rule' (unselected) and 'Add to existing rule' (selected). Next to 'Add to existing rule' is a dropdown menu showing 'Bad Guys'. Each section has a text input field for naming the new entity.

4. In the **Category and Rule** screen, specify the category to which the new rule belongs and the rule itself.

Field	Description
Category	Select one of the following:
	<ul style="list-style-type: none"><li>• <b>Create a new category</b> and specify the name of the new category.</li><li>• <b>Add to existing category</b> and select the name of an existing category from the menu. The default name displayed is the one which was selected when you clicked <b>Add</b> in the first step of this procedure.</li></ul>

Field	Description
-------	-------------

<b>Rule</b>	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Create a new rule</b> and specify the name of the new rule. If you select this option, enter the new rule's parameters in the next wizard window before continuing. For more information, see .</li> <li>• <b>Add to existing rule</b> and select the name of an existing rule from the menu. The default name displayed is the one which was selected when you clicked <b>Add</b> in the first step of this procedure.</li> </ul>
-------------	--

5. Click **Next**.

6. In the **Rule Information** screen, enter the following data:

Field	Description
<b>Criterion Name</b>	A descriptive name.
<b>Description</b>	A description of what the criterion does and its purpose.
<b>Owner</b>	The name of the rule's author.
<b>Criterion Type</b>	<p>Select one of the following from the dropdown menu:</p> <ul style="list-style-type: none"> <li>• <b>Parameter</b> – A criterion which relates to anomalies in a session's parameters.</li> <li>• <b>Behavior</b> – A criterion which relates to some characteristic of the session.</li> <li>• <b>Pattern</b> – A criterion which detects anomalous patterns in a session.</li> <li>• <b>Geographic</b> – A criterion which relate to anomalies in the geographic source of a session.</li> <li>• <b>Bot-Intelligence</b> – A criterion which detects the presence of bots rather than human users.</li> </ul> <p>Depending on which value you select, the wizard will display a different series of windows.</p>
<b>Application</b>	The criterion applies only to the specified application.
<b>Source IP</b>	The criterion applies only to the specified source IP address.
<b>User</b>	The criterion applies only to the specified user.
<b>Trigger alert after ... criterion matches</b>	An alert will be triggered only after the criterion has been matched the specified number of times during the session.
<b>Score Type</b>	Select <b>Numeric</b> or <b>Literal</b> and then select a value.

7. Click **Next**.

If you selected **Parameter** under **Criterion Type**, continue to Parameter .

If you selected **Behavior Rule** under **Criterion Type**, continue to Behavior .

If you selected **Pattern Rule** under **Rule Type**, continue to .

If you selected **Geographic Rule** under **Rule Type**, continue to Geographic .

If you selected **Bot-Intelligence Rule** under **Rule Type**, continue to .

## Parameter Criteria

**Step 3/3 - Parameter Criterion**

**Please select one of the following options:**

☒ Page  
☐ POST  
☐ GET

Parameter

**String Inspection**

☒ Heuristic

☐ Regex  ☐ Not

☐ String Contains  ☐ Not

☐ Fuzzy Length

☐ Length  Characters

☐ Length Between  and  Characters

☐ Parameter values differ by  characters between requests

### Parameter Criterion screen

1. In the **Parameter Criterion** screen, select one of the following:

Field	Description
<b>Page / Parameter</b>	Select the parameter in the <b>Parameters</b> window by navigating to the application page, selecting a parameter from the <b>Headers</b> , <b>GET</b> or <b>POST</b> lists and clicking <b>Add</b> .
<b>POST / GET</b>	Check <b>POST</b> and/or <b>GET</b> and specify a regular expression. A match occurs when regular expression matches any GET/POST parameter's value, as indicated. Check <b>Not</b> if a match occurs when the regular expression does not match the parameter's value.
<b>String Inspection</b>	- Check one of the values below and enter the corresponding data, which specify when a match occurs.
<b>Heuristic</b>	A match occurs when Telepath identifies a suspicious pattern based on its internal heuristic algorithms.



Field	Description
<b>Regex</b>	A match occurs when regular expression matches the parameter's value. Check <b>Not</b> if a match occurs when the regular expression does not match the parameter's value.
<b>String Contains</b>	A match occurs when the value in <b>String Contains</b> is a substring of the parameter's value. Check <b>Not</b> if a match occurs when the substring is not present in the parameter's value.
<b>Fuzzy Length</b>	Select a "fuzzy" value from the dropdown menu.
<b>Length</b>	A match occurs when the parameter is exactly <b>Length</b> characters long.
<b>Length Between</b>	A match occurs when the parameter length is within the specified range.
<b>Parameter values differ by characters between requests</b>	A match occurs when the value strings of successive occurrences of the parameter differ from each other by one character (e.g. "AAA", "AAB", "AAC") of the specified length. This parameter is intended for detecting scraping attacks.

2. Click **Submit** to finish defining the criterion.

## Behavior Criteria

Step 3/3 - Behavior Criterion

Aspect Value:

Query

Query
Speed
Location
Navigation

Behavior Criterion screen

1. In the **Behavior Criterion** screen, enter the following data:

Field	Description
Aspect Value	Select one of the following from the dropdown menu: <ul style="list-style-type: none"><li>• <b>Query</b> – A match occurs when the user submits a query different from typical queries.</li><li>• <b>Speed</b> – A match occurs when the page navigation speed is different from the typical page navigation speed.</li><li>• <b>Location</b> – A match occurs when the user's location is different from the typical client location.</li><li>• <b>Navigation</b> – A match occurs when the navigation among the application pages is different from the typical navigation pattern.</li></ul>
Personal	The criterion is matched based on the user's personal history. Otherwise, the match is based on the typical behavior of all users.

2. Click **Submit** to finish defining the criterion.

## Pattern Criteria

In a pattern criterion, Telepath examines whether a parameter's value changes across all sessions anchored by (originating from) the same IP address, session ID, device, user or other parameter.

Step 3/3 - Pattern Criterion

Anchor

☒ IP

☐ SID

☐ Device Fingerprint

☐ User

☐ Other

☐ Page

☐ Changing Parameter

☒ Repeating Action  ▼

Count  ▼

Time Window  ▼  ▼

**Pattern Criterion** screen

1. In the **Pattern Criterion** screen, enter the following data:

Field	Description
<b>Anchor</b>	<p>Select one of:</p> <ul style="list-style-type: none"> <li>• <b>IP</b> – Telepath implements this criterion in the context of all sessions originating from the same IP address.</li> <li>• <b>SID</b> – Telepath implements this rule in the context of all sessions with the same session ID.</li> <li>• <b>Device Fingerprint</b> – Telepath implements this criterion in the context of all sessions originating from the device.</li> <li>• <b>User</b> – Telepath implements this criterion in the context of all sessions originating from the same user.</li> <li>• <b>Other</b> – Telepath implements this criterion in the context of all sessions in which the value of the specified parameter is the same.</li> </ul>
<b>Page</b>	<p>An anomaly occurs when any the value of any parameter on this page changes.</p> <p>If selected,</p> <ol style="list-style-type: none"> <li>1. Click <b>Browse</b>.</li> <li>2. Select a page in the <b>Parameters</b> window by navigating to the application page.</li> <li>3. Select a parameter from the <b>Headers, GET or POST</b> lists.</li> <li>4. Click <b>Add</b>.</li> </ol> <p>Or, click <b>Remove</b> to delete a previously selected page.</p>
<b>Changing Parameter</b>	<p>An anomaly occurs when this parameter's value changes.</p> <p>If selected,</p> <ol style="list-style-type: none"> <li>1. Click <b>Browse</b>.</li> <li>2. Select a page in the <b>Parameters</b> window by navigating to the application page.</li> <li>3. Select a parameter from the <b>Headers, GET or POST</b> lists.</li> <li>4. Click <b>Add</b>.</li> </ol> <p>Or, click <b>Remove</b> to delete a previously selected parameter.</p>
<b>Repeating Action</b>	<p>A criterion match occurs when the business action is repeated the defined number of times within the scope of the anchor.</p>
<b>Count</b>	
<b>Time Window</b>	<p>The number of changes (<b>Count</b>) within <b>Time Window</b>.</p>

2. Click **Submit** to finish defining the criterion.

## Geographic Criteria

A geographic criterion defines anomalies based a session's geographic data.

**Step 3/3 - Geographic Criterion**

☒ Geographic Velocity      Time    Seconds      Distance    Km

☐ User Origin Outside of  
(Drag Country or Ctrl+Click)

All ▲  
Afghanistan  
Aland Islands  
Albania  
Algeria  
American Samoa  
Andorra

>>  
<<

Selected ▲

☐ User Origin Inside  
(Drag Country or Ctrl+Click)

All ▲  
Afghanistan  
Aland Islands  
Albania  
Algeria  
American Samoa  
Andorra

>>  
<<

Selected ▲

## Geographic Criterion screen

1. In the **Geographic Criterion** screen, select one of the following options:

Field	Description
<b>Geographic Velocity</b>	<p>An anomaly occurs when the client's location changes by more than <b>Distance</b> kilometers within <b>Time</b> seconds.</p>
<b>User Origin Outside Of</b>	<p>An anomaly occurs when the client's origin is not one of the <b>Selected</b> countries.</p> <p>To move a country between the <b>Selected</b> list and the list on the left, select it and use the arrows or drag it to the other list.</p> <p>To select multiple countries, Ctrl-click each one individually.</p> <p>To select a range of countries, click the first one and Shift-click the last one.</p>

Field	Description
<b>User Origin Inside</b>	<p>An anomaly occurs when the client's origin is one of the <b>Selected</b> countries.</p> <p>To move a country between the <b>Selected</b> list and the list on the left, select it and use the arrows or drag it to the other list.</p> <p>To select multiple countries, Ctrl-click each one individually.</p> <p>To select a range of countries, click the first one and Shift-click the last one.</p>

- Click **Submit** to finish defining the criterion.

## Bot-Intelligence Criteria

Bot-Intelligence criterions identify anomalous behavior based on the known behavior of bots.

Step 3/3 - Bot Criterion

**Bot Type:**

Tor
X
▼

Tor
Known-Bot
User-Agent.org

**Bot Criterion** screen

- In the **Bot Criterion** screen, , select the **Bot-Type**:

Field	Description
<b>Bot-Type</b>	<p>Select one of the following bots:</p> <p><b>Tor</b> - The Tor bot.</p> <p><b>Known-Bot</b> - IP address known to harbor malicious behavior, based on cloud intelligence gathered by Hybrid Security.</p> <p><b>User-Agent.org</b> - Bots cataloged by this security information site.</p>

- Click **Submit** to finish defining the criterion.

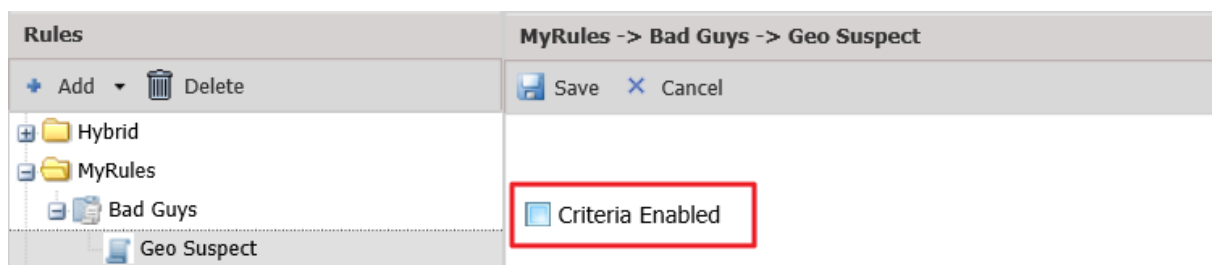
## Disabling a Criterion



A newly-defined criterion is enabled by default.

### To disable a criterion:

1. Click the **Rules** tab.
2. In the **Rules** pane, select the criterion to disable.
3. Unselect the **Criteria Enabled** checkbox in the right pane.



4. Click **Save**.

## Editing an Existing Criterion

### To edit an existing criterion:

1. Click the **Rules** tab.
2. In the **Rules** pane on the left, select a criterion.
3. Enter the rule's parameters in the right pane.
4. Click **Save**.

## Deleting an Existing Criterion

### To delete an existing criterion:

1. Click the **Rules** tab.
2. In the **Rules** pane on the left, select a criterion.
3. Click **Delete**.
4. In the **Delete Criterion** window, confirm the deletion.

# Telepath Dashboard

The Telepath dashboard, which is displayed when you login successfully, presents an overview of Telepath’s monitoring status, and consists of the following panes:

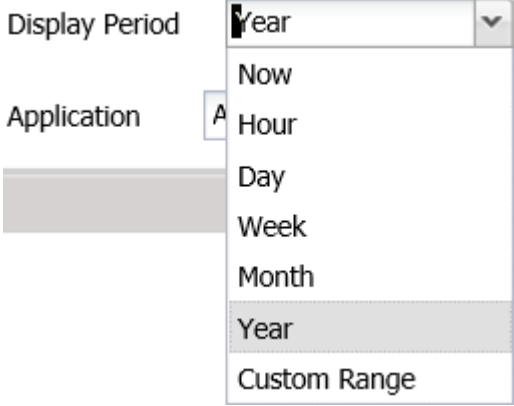
Pane	For more information, see
Dashboard Settings	
Attacks	
Hot Spots	
Attack Origins	
Alert Trends	
Top Suspects	
Sessions	

## Dashboard Settings Pane

Dashboard Settings							
Start Date	<input type="text" value="05/22/13"/>	End Date	<input type="text" value="05/12/14"/>	Display Period	<input type="text" value="Year"/>	Refresh Rate (Mins)	<input type="text" value="10"/>
Top Suspects Results	<input type="text" value="15"/>	Alert Trends Results	<input type="text" value="15"/>	Application	<input type="text" value="All"/>		

### Dashboard - Settings pane

The table below describes the data displayed in the **Telepath Settings**.

Field	Description
<b>Start Date</b>	<p>You can change the time period to display in the dashboard in the following ways:</p> <ul style="list-style-type: none"><li>Change the <b>Start Date</b> or <b>End Date</b>. In both cases, you can click the calendar icon to the right of the field and select a date from the calendar.</li><li>Select a time frame from the <b>Display Period</b> drop down menu.</li></ul> 
<b>End Date</b>	
<b>Display Period</b>	
<b>Refresh Rate</b>	<p><b>Now</b> means in the last 10 minutes.</p> <p>The values displayed in these three fields are synchronized, so that, for example, if you change <b>Display Period</b> to <b>Year</b>, the values in <b>Start Date</b> and <b>End Date</b> change accordingly.</p>
<b>Top Suspects Results</b>	<p>The frequency at which the dashboard data are refreshed.</p>
<b>Alert Trends Results</b>	<p>The number of items displayed in the <b>Top Suspects</b> pane of the dashboard.</p>
<b>Application</b>	<p>The number of items displayed in the <b>Alert Trends</b> pane of the dashboard.</p>
	<p>The applications for which the dashboard displays data.</p>

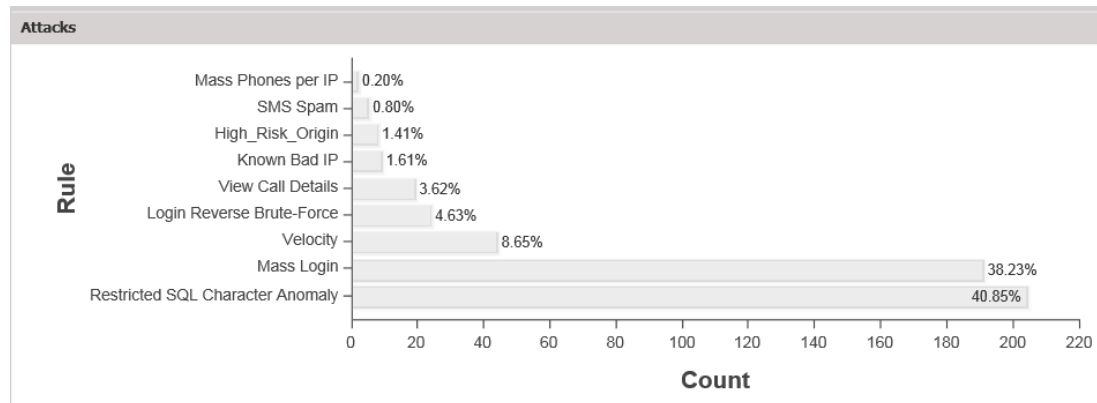
If you change any of these settings, the changes will take effect only after you click **Apply**.



You can restore the default settings by clicking **Reset**.

## Attacks Pane

The **Attacks** pane displays a column chart of the 10 most common attacks detected by Telepath.



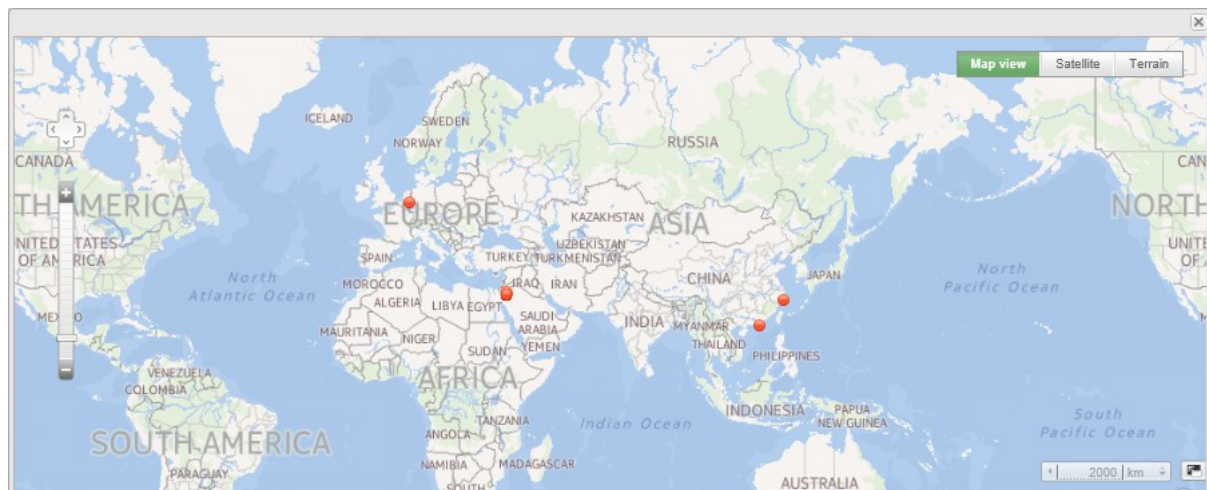
**Dashboard - Attacks** pane

If you hover over a column, the number of detected attacks is displayed. If you click a column, the relevant alerts are displayed in the **Alerts** tab (see ). You can return to the dashboard by clicking the **Dashboard** tab.

## Hot Spots Pane



The **Hot Spots** pane displays a global map indicating the source locations of ALL frequent attacks detected by Telepath.

This feature requires the Telepath server to have firewall access to the URL **api.maps.ovl.com**.



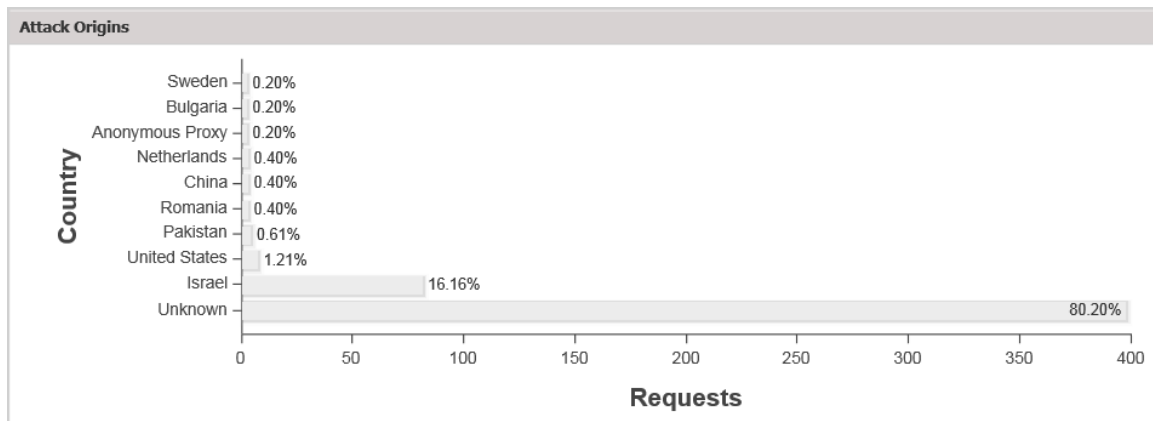
**Dashboard - Hot Spots** pane

If you hover over a hot spot, the geographic location, number of detected attacks and rule are displayed.

You can change the map view by clicking **Map view** (shown above) or **Satellite** or **Terrain**, or navigate in the map using the navigation icon , or change the map scale by clicking the scale icon .

## Attack Origins Pane

The **Attack Origins** pane displays a column chart of the ten countries from which the largest number of attacks has been detected by Telepath.

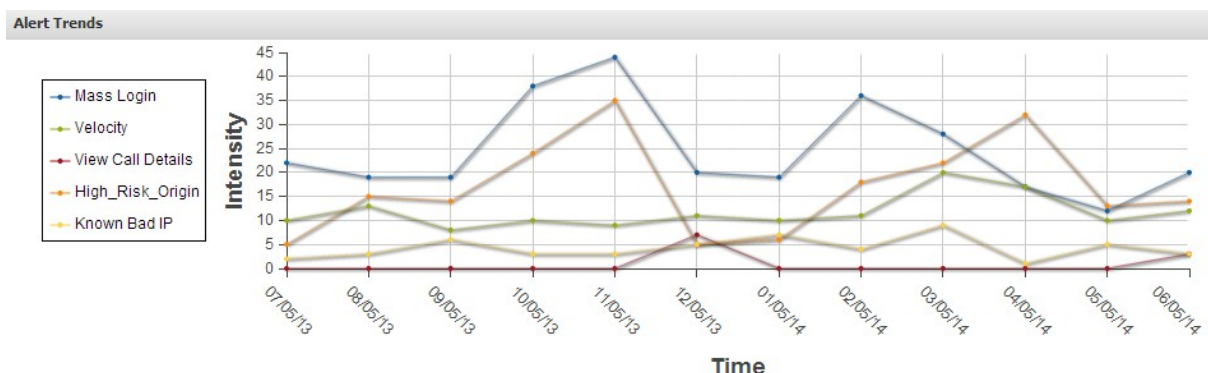


**Dashboard - Attack Origins** pane

If you hover over a column, the number of attacks originating from that country is displayed. If you click a column, the relevant alerts are displayed in the **Alerts** tab (see ). You can return to the dashboard by clicking the **Dashboard** tab.

## Alert Trends Pane

The **Alert Trends** pane plots the number of alerts for each alert type presented in the Attack Origins pane over time. A legend is displayed to the left of the graph.



**Dashboard - Alert Trends** pane

## Top Suspects Pane

The **Top Suspects** pane lists the IP addresses from which attacks most frequently originated, together with additional identification information.

Top Suspects				
Time ▾	IP	Location	Anomaly	User
28/11/13 13:48:30	197.146.128.252	 Russian Federation	94.66%	
28/11/13 06:35:26	188.128.240.107	 United States, Tampa	94.75%	
28/11/13 03:21:18	178.208.128.88	 France	94.21%	
28/11/13 00:21:16	193.228.17.10	 United States, Ashburn	94.00%	
25/11/13 21:45:03	198.76.255.107	 Germany	94.22%	
25/11/13 07:19:33	185.152.133.176	 India	93.84%	
25/11/13 06:24:45	125.208.208.11	 Korea, Republic of, Seongnam	94.53%	
25/11/13 03:31:41	207.244.208.238	 United States, San Francisco	94.69%	
25/11/13 03:31:11	193.208.128.88	 United States	95.81%	
25/11/13 01:12:26	193.227.76.100	 United States, Ashburn	94.61%	
24/11/13 19:44:26	193.252.198.11	 France, Biot	94.50%	
24/11/13 10:56:09	193.128.198.88	 United States, Manassas	94.51%	

### Dashboard - Top Suspects pane

You can re-sort the list by clicking the column headings.

**Anomaly** displays the percentage of connections from the IP address which have been identified as attacks.

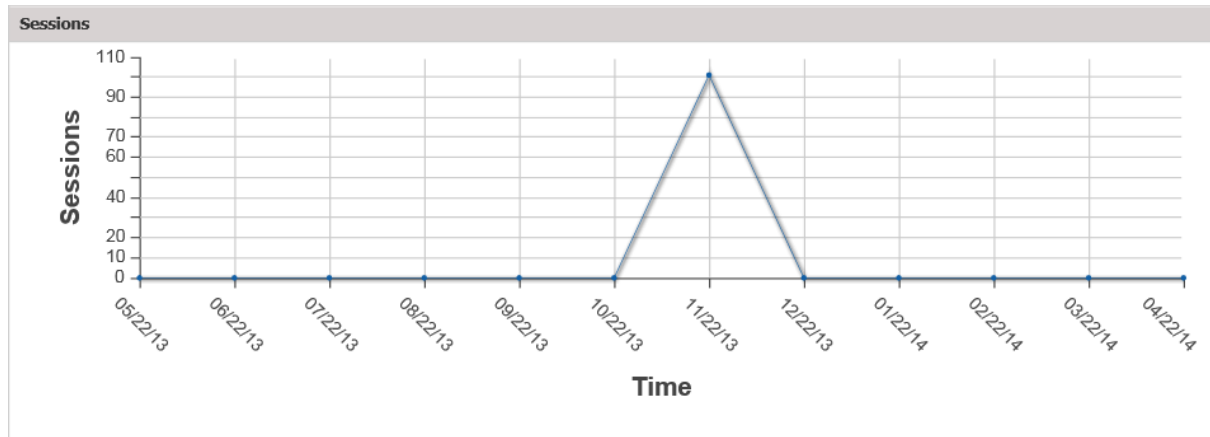
For more options, right click a suspect and select the appropriate option:

- Investigate this value
- Investigate session
- Investigate by IP
- Add to Investigate Filter
- Add IP to whitelist
- Copy to clipboard

Option	Description
<b>Investigate this value</b>	Display filter results for the selected value.
<b>Investigate session</b>	Display filter results for the session of the selected request.
<b>Investigate by IP</b>	Display filter results for the IP address of the selected request.
<b>Add to Investigate Filter</b>	Add the selected value to the filter, but do not display the results.
<b>Add IP to whitelist</b>	Add the request's source IP address to the IP whitelist.
<b>Copy to clipboard</b>	Copy the text of the selected field to the clipboard.

## Sessions Pane

The **Sessions** pane plots the number of sessions monitored by Telepath over time.



**Dashboard - Sessions** pane

## Alerts

The **Alerts** tab displays the alerts issued by Telepath when encountering anomalous behavior.



Note

In order to receive email alerts, the [SMTP Server](#) must be configured. For syslog alerts, the Remote Syslog Server must be defined. Proxy Server and Report Schedule have been configured before defining business actions.


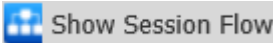






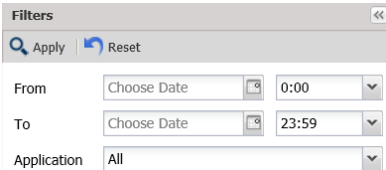
Dashboard	Alerts	Investigate	Business Actions	Rules	Settings	Help	Mode: Training	Off	Logout
Filters									
Delete Selected Show Session Flow Page 1 of 3 Auto-refresh (Mins) 1 Displaying 1 - 30 of 77									
Apply Reset									
From Choose Date 0:00									
To Choose Date 23:59									
Application All									
IP Filter									
IP Address									
2.179.222.252									
5.22.130.224									
5.28.189.130									
5.28.191.158									
46.116.130.191									
46.116.174.251									
64.74.218.6									
<input type="checkbox"/>	SID	Time	Score	IP	Location	Rule Group	Aggregate	Domain	Parameters
<input type="checkbox"/>	0	28/11/13 15:41:59	95%	109.65.141.9	Nigeria, Lagos	Mass Login	1	My version.com	User Name
<input type="checkbox"/>	1	28/11/13 15:11:30	95%	109.67.191.24	Netherlands, Amsterdam	Mass Login	1	My version.com	User Name
<input type="checkbox"/>	2	28/11/13 15:11:21	95%	5.28.191.158	Romania	Mass Login	1	My version.com	User Name
<input type="checkbox"/>	3	28/11/13 14:43:20	95%	109.65.149.71	United Kingdom	Mass Login	2	My version.com	User Name
<input type="checkbox"/>	4	28/11/13 14:31:52	95%	212.76.123.126	Israel	Mass Login	2	My version.com	User Name
<input type="checkbox"/>	5	28/11/13 14:18:56	95%	77.127.103.97	Bulgaria, Sofia	Mass Login	1	My version.com	User Name
<input type="checkbox"/>	6	28/11/13 14:04:46	100%	94.159.197.42	China, Shaoxing	Velocity	1	My version.com	
<input type="checkbox"/>	7	28/11/13 13:42:09	100%	72.251.244.17	Netherlands, Amsterdam	Velocity	2	My version.com	
<input type="checkbox"/>	8	28/11/13 13:39:51	95%	5.28.189.130	Russian Federation	Mass Login	1	My version.com	User Name
<input type="checkbox"/>	9	28/11/13 12:55:56	95%	172.27.226.151	United States, Atlanta	Mass Login	19	My version.com	User Name
<input type="checkbox"/>	10	28/11/13 11:01:42	95%	79.179.138.177	China, Guangzhou	Mass Login	1	My version.com	User Name


**Alerts** tab

The data displayed in the **Alerts** tab are described below. You can re-sort the list by clicking the column headings.

Field	Description
<b>SID</b>	The ID of the session that triggered the alert.
<b>Time</b>	The date and time of the alert.
<b>Score</b>	The percentage of connections from the IP address that have been identified as attacks.
<b>IP</b>	The IP address from which the connection that triggered the alert.
<b>Location</b>	The country and city (if available) from which the session that triggered the alert originated.
<b>Rule</b>	The Rule that triggered the alert.
<b>Aggregate</b>	The number of times this alert was triggered during the session.
<b>Domain</b>	The application that was attacked.
<b>Parameters</b>	Identification details about the alert. For more information, see <b>Parameters to show upon alert for the rule</b> in the section.

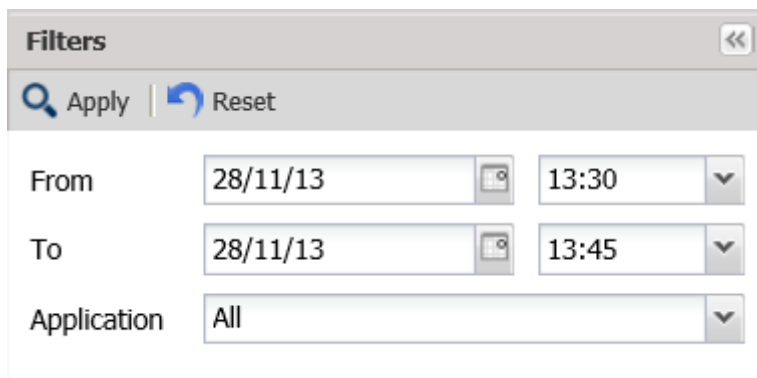
At the top of the **Alerts** window, a toolbar is displayed.

Tool	Description
	Delete the selected alert(s).
	Display the flow (the navigation from page to page) of the selected session. For more information, see <a href="#">. </a>
	Display the previous page.
	Display the first page.
	Display the next page.
	Display the last page.
	To display a specific page, enter the page number in the box.
	Refresh the data in the window.
	Filter the alerts (see <a href="#">Error: Reference source not found</a> ).

Tool	Description
<input checked="" type="checkbox"/> Auto-refresh (Mins) <input type="text" value="1"/> 	To specify how frequently the <b>Alerts</b> page will automatically be refreshed, select a value (in minutes) from the drop down menu.

## Filtering the Alerts Display

You can filter the alerts by time period and/or application.



The screenshot shows a 'Filters' window with a title bar and a close button. Below the title bar is a bar with 'Apply' and 'Reset' buttons. The main area contains three filter sections: 'From' with date '28/11/13' and time '13:30', 'To' with date '28/11/13' and time '13:45', and 'Application' with a dropdown menu set to 'All'. Each input field has a small calendar icon.

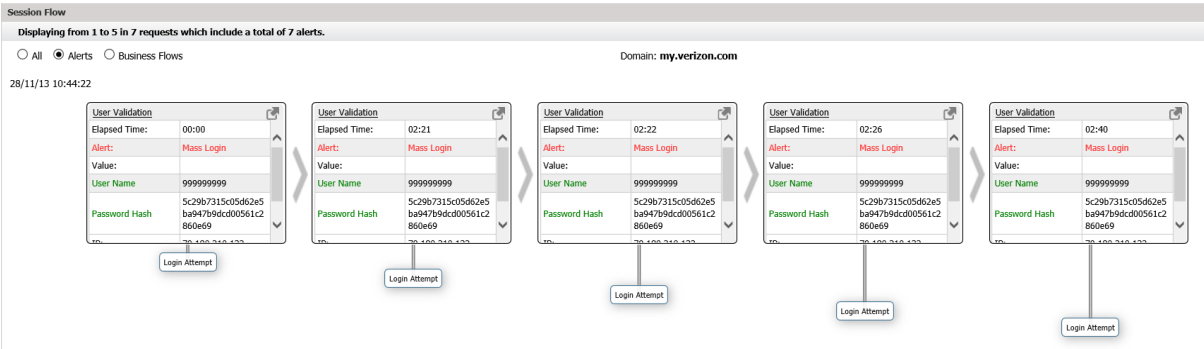
Search alerts window

Select time period and/or application and click **Apply**. To remove the filter, click **Reset**.

Tool	Description
From	Display alerts detected within the specified time range.
To	
Application	Display alerts originating from the selected application.

# Session Flow

When you click the **Show Session Workflow** button in the Alerts toolbar, the selected alert’s session flow is displayed in a series of boxes from left to right.



## Show Session Workflow window

The data that triggered the alert is shown in red while aliases defined by the Telepath user are shown in [REDACTED].

For additional options, right click a parameter within a session flow window.

\*

Mask Parameter

Edit Parameter Alias

Remove Parameter Alias

Option	Description
Mask Parameter	Encrypt sensitive data such as passwords, email addresses, ID numbers
Edit Parameter Alias	Specify a different name for the selected parameter
Remove Parameter Alias	Reset the parameter name

To add parameters to the session flow windows of an alert, see **Parameters to show upon alert for the rule** in the [section](#).

The following data are displayed by default:

Field	Description
<b>Display options</b>	Select the appropriate option: <ul style="list-style-type: none"><li>• <b>All</b> - all requests for the selected session</li><li>• <b>Alerts</b> - only requests that triggered alerts</li><li>• <b>Business Flows</b> - requests identified as being a part of a defined business flow</li></ul>
<b>Elapsed Time</b>	Time that has passed since the start of the current view (events displayed in the Session Flow pane).
<b>Alert</b>	The Rule Type of the rule which triggered the alert.
<b>Value</b>	Additional data about the request. For example, a heuristically detected bot alert would display a value of high, low or medium, depending on the certainty of the alert.
<b>User Name</b>	The session user's username.
<b>Password Hash</b>	The session user's password.
<b>App</b>	The application for which the alert was issued is displayed at the top middle of the Session Flow pane.
<b>IP</b>	The IP address of the client.
<b>Date</b>	The times and dates of the current view are displayed above in the top left and top right of the Session Flow pane.
<b>Score</b>	The severity of the anomaly that triggered the alert.
<b>Page</b>	The page on which the alert occurred.
<b>user-agent</b>	String identifying the browser.



# Investigate





In the **Search Suspects Filter** and **Advanced** panes of the **Investigate** tab, you can define a search on HTTP requests to be displayed in the **Requests** pane.

The screenshot shows the 'Investigate' tab interface. At the top is a navigation bar with links: Dashboard, Alerts, Investigate (active), Business Actions, Rules, Settings, Help, Mode: Production, Off, and Logout. Below this is the 'Search Suspects Filter' pane. It contains a 'Search Filters' section with a 'Range' dropdown set to 'Week', 'From' date/time '25/05/14 16:03', 'To' date/time '01/06/14 16:03', and an 'Application' dropdown set to 'All'. Below this is a 'Score' section with an 'Average' dropdown, an 'At Least' dropdown, a numeric input '0', and a 'Percent' label. The 'Advanced' section contains several input fields: 'User', 'User-Agent', 'Page' (with a 'Contains' dropdown), 'SID', 'IP', 'Parameter' (with a 'Browse' button), 'City', 'Country' (with a dropdown and a clear button), 'Value', 'Workflow' (with a dropdown and a clear button), and 'Method' (with a dropdown and a clear button). At the bottom of the filter pane are 'Search', 'Cancel', 'Reset', and 'Save Profile' buttons. Below the filter pane is the 'Requests' pane, which shows a table header with columns: SID, Time, Result, Click #, IP, Location, Type, Page, User, SSL, and Application. The table is currently empty, showing 'Total Results 0' and 'Results per Page 25'.

## Investigate tab

The search parameters in the **Investigate** tab are described below.

Field	Description
<b>Search Filters</b>	
<b>Range</b>	Display requests detected within the selected time range. Alternatively, use the <b>From/To</b> fields to select a different time period.
<b>From</b>	Display requests between these dates.
<b>To</b>	
<b>Application</b>	Select an application name from the dropdown menu.
<b>Score</b>	
	Select a severity score from the dropdown menu.
<b>Advanced</b>	
<b>User</b>	The user name.
<b>User-Agent</b>	The user agent.
<b>SID</b>	The session ID.
<b>IP</b>	The IP address from which the session originated.
<b>City</b>	The city from which the session originated.

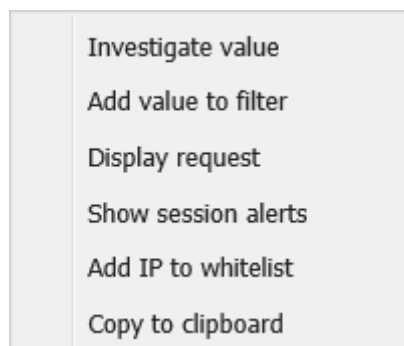
Field	Description
<b>Country</b>	Select country from which the session originated from the dropdown menu, or clear the field by clicking  .
<b>Workflow</b>	Select the workflow of which the request was a part, or clear the field by clicking  .
<b>Method</b>	Select an HTTP method from the dropdown menu, or clear the field by clicking  .
<b>Page</b>	The page accessed by the request.
<b>Parameter</b>	Select a request parameter, or clear the field by clicking  .
<b>Value</b>	The parameter's value. (Enabled when a Parameter is selected)

Click **Search** to perform the search, or **Reset** to clear the search parameters or **Save Profile** to save the search parameters as a search profile.

If there are existing search profiles, you can display them by clicking the double arrow in the upper right hand corner of the window and then select one of the profiles to apply. You can also delete profiles in this way.

The results are displayed in the **Requests** pane at the bottom of the tab.

You can refine the filter by selecting a value in one of the results and right-clicking on it.



From the menu, select one of the options:

Option	Description
<b>Investigate value</b>	Add the field and its value to the filter and display the results.
<b>Add value to filter</b>	Add the selected value to the filter, but do not display the results.
<b>Display request</b>	Display the request data in a separate window.
<b>Show session alerts</b>	Display the <b>Alerts</b> tab for any alerts triggered by the selected request.
<b>Add IP to whitelist</b>	Add the request's source IP address to the IP whitelist.

Option	Description
<b>Copy to clipboard</b>	Copy the text of the selected field to the clipboard.

## Business Actions

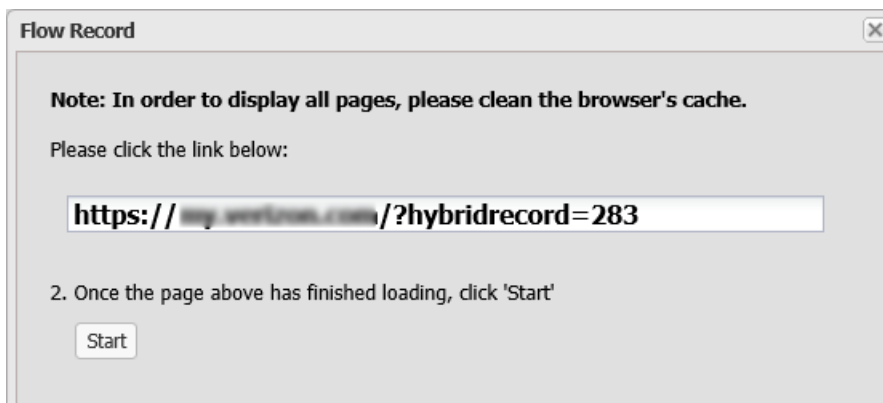
The **Business Actions** screen enables you to record workflows users may follow, such as navigating to certain pages and filling in forms on a web page. This way, the next time a recorded workflow is detected by Telepath, the system will know how to label the action taken by the user. For example, in an eCommerce site – "Add to Shopping Cart", and in a banking site – "Transfer Money" or "Check Balance".

### To record a business action:

1. Open the Business Actions screen.
2. In Nodes list, expand the application in which you want to record.
3. Click **Record new Action**.

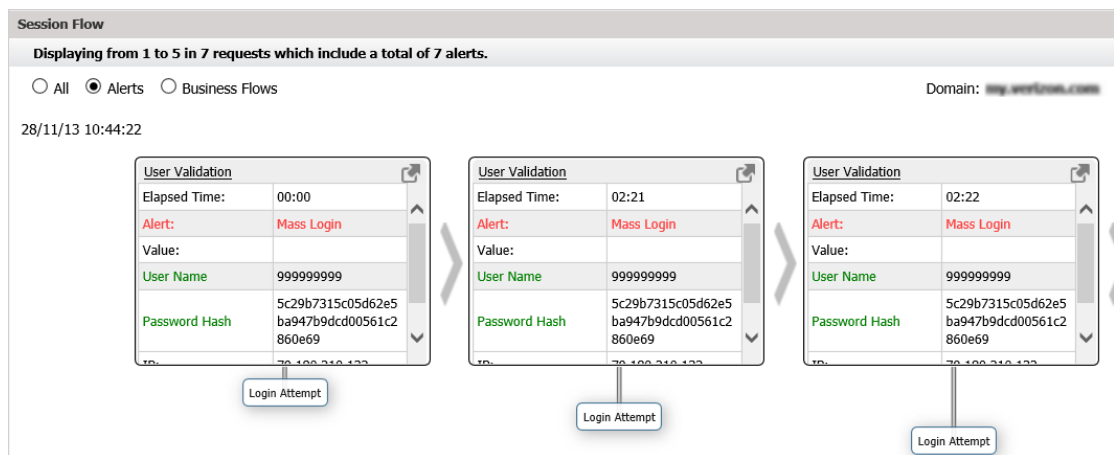


The Flow Record window is displayed with a link to the application and a temporary access token (e.g. "http://www.example.com/?hybridrecord=75"). The link can be viewed from a different browser or device



4. Click the link. A web browser opens, displaying the web page.
5. Navigate to the web page on which you want to start recording.
6. Return to the Flow Record window and click **Start**.
7. Perform the actions you want to record (i.e. navigate to the appropriate web pages, fill in web forms).
8. To finish, return to the Flow Record window and click **Stop**.

The sequence of events (pages) is displayed in the Session Flow pane in a series of windows with each window representing a separate event.



- Review the business action recording by clicking the appropriate event box, clicking the button and manually typing the new value.

For example, changing the username value specified in a registration form to an asterisk (\*) in order to allow all usernames.

## Settings

Click the **Settings** tab to display a list of the configuration options:

Option	For more information, see
<b>Administration</b>	
<b>Network</b>	
<b>Operation Mode</b>	
<b>Reports</b>	
<b>Web Applications</b>	

If you change any of the configuration options, remember to click the **Save** button in the **Settings** toolbar.

To display the configuration parameters for any of these options, click the appropriate tab:



**Settings** tab options

## Administration

The **Administration** tab enables you to create, edit and remove Telepath users and user groups, as well as view Telepath activity logs. This is meant for a multi-tenant environment and allows you to control user access to Telepath information on a need-to-use basis.

## Users

### Adding New Users

#### To create a new Telepath user:

1. Select the **Administration** tab.
2. Click the **Users** button. The Telepath Users window is displayed, listing all existing Telepath users.
3. Click **Add User**. The User Editor dialog is displayed.

The **User Editor** dialog box is used to create and manage Telepath users. It includes the following sections:

- Active:** A checkbox to enable the user.
- General Information:** Fields for Username, E-Mail, First Name, Last Name, Company, Phone, Password, and Password (again).
- Groups:** A list of groups to assign to the user, including 'admin' and 'users'.
- Applications:** A list of applications to assign to the user, including 'All', 'http://example.com', and 'www.example.com'.
- Permissions:** A table of permissions to assign to the user.

Scope	Type	Description
<input type="checkbox"/> Telepath	View	Access telepath UI and get engine status.
<input type="checkbox"/> Telepath	Modify	Start and stop telepath engine.
<input type="checkbox"/> Dashboard	View	Access dashboard screen.
<input type="checkbox"/> Dashboard	Modify	Modify dashboard settings, reorder panels.
<input type="checkbox"/> Alerts	Delete	Delete alerts.
<input type="checkbox"/> Investigate	View	Access investigate screen, investigate and view request...
<input type="checkbox"/> Investigate	Modify	Store investigate profiles for later use.
<input type="checkbox"/> Investigate	Delete	Delete investigate profiles.
<input type="checkbox"/> Workflow	View	Access workflows screen, view recorded flows.

Automatically add to the list applications created by the user ☒

4. Select the **Active** checkbox to enable the user.
5. Fill in the user's general details (Login, Email, etc.)
6. In the Permissions area, assign access permissions to the user.

Select a permission and click the appropriate button:

- **View** – Allows the user to view but not modify Telepath data.
- **Modify** – Allows the user to modify Telepath data and system settings.
- **Add** – Allows the user to add Telepath data and system settings.
- **Delete** – Allows the user to remove Telepath data and system settings.

7. In the Group Selection area, select the group(s) the user belongs to.
8. In the Applications area, select the applications this user can access or select **All** to grant the user access to all applications.
9. Click **Save User**.

## Editing Users

### To edit an existing Telepath user:

1. Select the **Administration** tab.
2. Click the **Users** button. The Telepath Users window is displayed, listing all existing Telepath users.
3. Click a user. The User Editor dialog is displayed.
4. Select/deselect the **Active** checkbox to enable or disable the user, respectively.
5. Edit the user's settings, as appropriate.
6. Click **Save User**.

## Deleting Users

### To delete an existing Telepath user:

1. Select the **Administration** tab.
2. Click the **Users** button. The Telepath Users window is displayed, listing all existing Telepath users.
3. Click a user. The User Editor dialog is displayed.
4. Click the **Delete** button.

## Viewing a User's Activity History

### To view a Telepath user's activity:

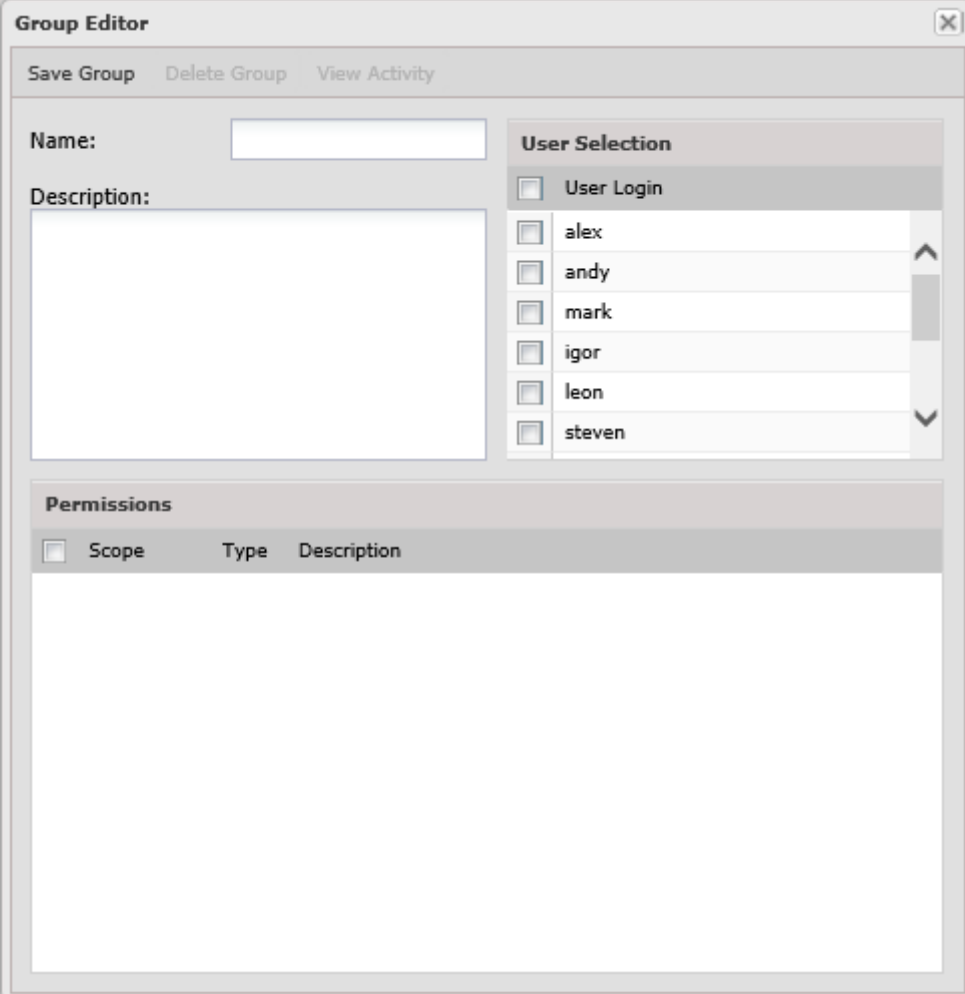
1. Select the **Administration** tab.
2. Click the **Users** button. The Telepath Users window is displayed, listing all existing Telepath users.
3. Click a user. The User Editor dialog is displayed.
4. Click the **View Activity** button. The user's activity log is displayed.

## Groups

### Adding New Groups

#### To add a new group:

1. Select the **Administration** tab.
2. Click the **Groups** button. The Telepath Groups window is displayed, listing all existing Telepath groups.
3. Click **Add Group**. The Group Editor dialog is displayed.



The Group Editor dialog box is shown with the following components:

- Buttons:** Save Group, Delete Group, View Activity.
- Name:** A text input field.
- Description:** A large text area.
- User Selection:** A list of users with checkboxes next to them: alex, andy, mark, igor, leon, steven. There is also a checkbox for User Login.
- Permissions:** A table with columns: Scope, Type, Description. The table is currently empty.

4. Specify a **Name** and **Description** for the group.
5. In the User Selection area, select the users you wish to assign to this group.
6. In the Permissions area, select the access permissions you wish to grant all group members.
7. Click **Save Group**.

## Editing Groups

### To edit an existing Telepath user:

1. Select the **Administration** tab.
2. Click the **Groups** button. The Telepath Groups window is displayed, listing all existing Telepath groups.
3. Click a group. The Group Editor dialog is displayed.
4. Edit the user's settings, as appropriate.
5. Click **Save Group**.

## Deleting Groups

### To delete an existing Telepath group:

1. Select the **Administration** tab.
2. Click the **Groups** button. The Telepath Groups window is displayed, listing all existing Telepath groups.
3. Click a group. The Group Editor dialog is displayed.
4. Click the **Delete** button.

## Viewing a Group's Activity History

### To view a Telepath group's activity:

1. Select the **Administration** tab.
2. Click the **Groups** button. The Telepath Groups window is displayed, listing all existing Telepath groups.
3. Click a group. The Group Editor dialog is displayed.
4. Click the **View Activity** button. The group's activity log is displayed.

## Activity Log

The activity log comprises the activity of all Telepath system users (for web users, use the **Administration** tab), for auditing purposes.

### To view the Telepath activity log:

1. Select the **Administration** tab.
2. Click the **Activity Log** button. The Telepath Activity Log is displayed, listing all user actions performed in Telepath.



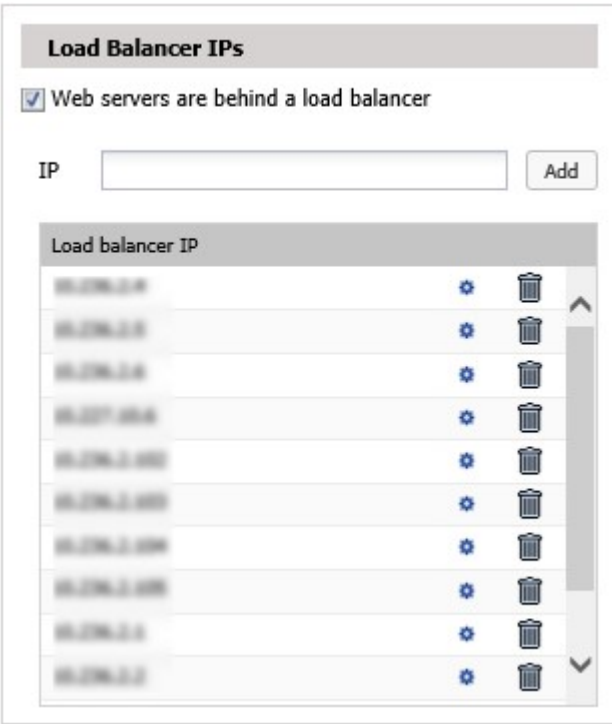
# Network

The **Network** tab consists of the following panes:

Field	For more information, see
Load Balancer IPs	
Load Balancer Headers	
SMTP Configuration	
IP Whitelist	
User Agent Ignore List	
Extension Ignore List	
Proxy Configuration	
Network Interfaces	

## Load Balancer IPs

The **Load Balancer IPs** pane displays a list of the IP addresses of a load balancer positioned in front of the Telepath server.



Load balancer IPs pane

This pane’s parameters are described below.

Field	Description
Web servers are behind a load balancer	Check if the Telepath server is behind a load balancer.

Field	Description
-------	-------------

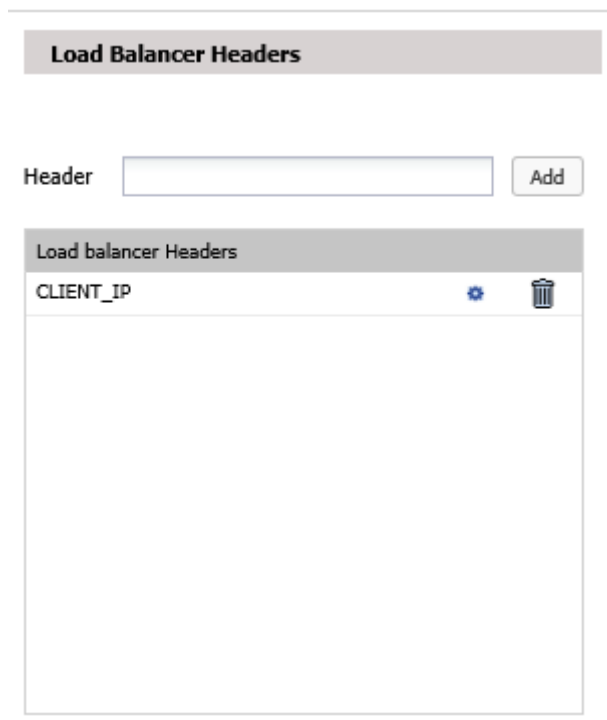
**IP** Enter the IP address of the load balancer and click **Add**.

The list of load balancer IP addresses is displayed in the list below.

To change an IP address, select it in the list and click .

To delete an IP address, select it in the list and click .

## Load Balancer Headers



The screenshot shows a web interface for configuring load balancer headers. At the top is a grey header bar with the text 'Load Balancer Headers'. Below this is a form with a label 'Header' followed by a text input field and an 'Add' button. Underneath the form is a list box titled 'Load balancer Headers'. The list contains one item, 'CLIENT\_IP', which has a blue gear icon (edit) and a trash can icon (delete) to its right. The list box is empty except for this one entry.

**Load Balancer Headers** pane

This pane's parameters are described below.

Field	Description
-------	-------------

**Header** Enter the ID of the header field added by the load balancer that specifies the web client's IP address and click **Add**.

The list of load balancer headers is displayed in the list below.

To change a header, select it in the list and click .

To delete a header, select it in the list and click .

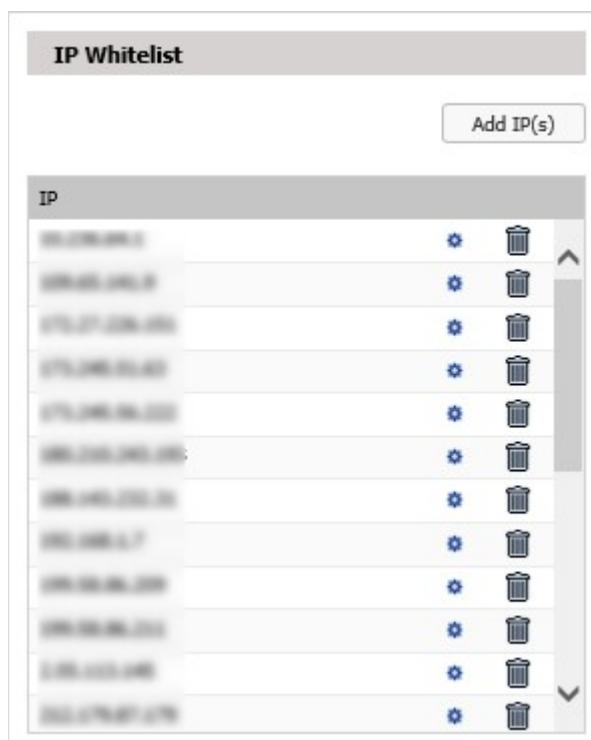
## SMTP Configuration

The SMTP Configuration pane enables the administrator to set the SMTP server settings.

Field	Description
<b>SMTP Server</b>	The IP address of the SMTP server Telepath uses for outgoing email on <b>SMTP Server</b> .
<b>Port</b>	Port Telepath uses for outgoing email.
<b>User Name</b>	The user name of the Telepath email account on <b>SMTP Server</b> .
<b>Password</b>	The password of the Telepath email account.

## IP Whitelist

The **IP Whitelist** pane displays the IP addresses from which Telepath should ignore all traffic. These typically represent network management tools.





**IP Whitelist** pane

This pane's parameters are described below.

Field	Description
<b>IP</b>	Enter an IP address from which Telepath should ignore traffic and click <b>Add</b> .

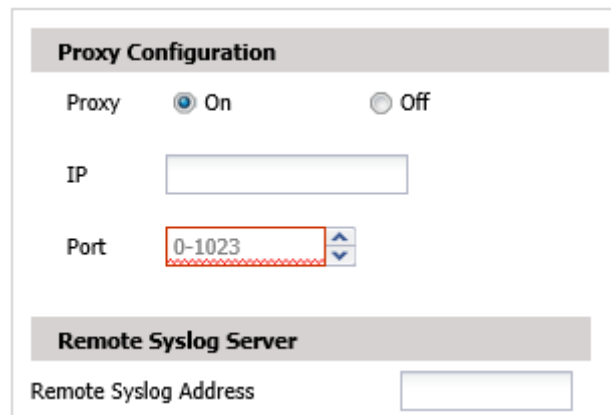
The list of whitelist IP addresses is displayed in the list below.

To change a whitelist IP address, select it in the list and click .

To delete a whitelist IP address, select it in the list and click .

## Proxy Configuration

The **Proxy Configuration** pane specifies whether the management LAN's Internet traffic requires a proxy server.



**Proxy Configuration**

Proxy ☒ On ☐ Off

IP

Port

**Remote Syslog Server**

Remote Syslog Address

**Proxy Configuration** pane

This pane's parameters are described below.

Field	Description
<b>Proxy</b>	Set <b>Proxy</b> to <b>On</b> if the management LAN's Internet traffic requires a proxy server.
<b>IP Address</b>	The proxy server's IP address.
<b>Port</b>	The proxy server's proxy port.

## Remote Syslog Server

For syslog alerts to be sent, the Remote Syslog Server must be defined.



**Remote Syslog Server**

Remote Syslog Address

**User Agent Ignore List** pane

## Network Interfaces

Use the **Network Interfaces** pane to define the sniffers to be used by Telepath.

If multiple sniffers have been defined, Telepath will use them for connection to different networks on the same machine. Multiple sniffers require multiple network interfaces to be installed on the machine.



**Note**

It is recommended to have at least two network interfaces, one for sniffing traffic and one to manage Telepath.

Network Interfaces

Add

	Name	Filter Expression	Interface	
1	sniffer108	tcp port 80	eth0	

**User Agent Ignore List** pane

## User Agent Ignore List

The **User Agent Ignore List** pane displays the user agents (typically "harmless" bots) whose traffic Telepath should ignore.

User Agent Ignore List

User-Agent

Add

User-Agent		
baiduspider		
yandex		
yahoo		
facebookexternalhit		
adsbot-google		
msnbot-media		
googlebot		

**User Agent Ignore List** pane

This pane's parameters are described below.

Field	Description
<b>User-Agent</b>	Enter the name of the user-agent and click <b>Add</b> .

The list of user-agents is displayed in the list below.

To change a user-agent, select it in the list and click .

To delete a user-agent, select it in the list and click .

## Extension Ignore List

The **Extension Ignore List** pane displays the file extensions (e.g. of graphic files) which Telepath should ignore.

Extension Ignore List

Extension

Add

Ignore Extension

jpg		
jpeg		
gif		
css		
ico		
png		
swf		
ashx		

Extension Ignore List pane

This pane's parameters are described below.

Field	Description
Extension	Enter a file name extension which Telepath should ignore traffic and click <b>Add</b> .

The list of file name extensions is displayed in the list below.

To change a file name extension, select it and click .

To delete a file name extension, select it and click .

## Operation Mode

This pane specifies the Telepath operation mode, and in the case of Hybrid mode, the times during which learning takes place.

The screenshot shows the 'Operation Mode' configuration pane. At the top is a navigation bar with tabs: 'Administration', 'Save', 'Cancel', 'Network', and 'Operation Mode' (which is highlighted). Below the navigation bar are three radio buttons: 'Training', 'Production' (which is selected), and 'Hybrid'. Below these is a text field labeled 'Stop learning when number of requests reaches' with the value '1000000'. Below that is a section titled 'Hybrid Mode Schedule' with a description: 'Scheduled time switches into Hybrid Mode, where Telepath learns new information while remaining in production'. There is a 'Configure Schedule' button below this section. At the bottom, there is a checkbox labeled 'Enable Debug Message Logging' which is currently checked, with 'On' and 'Off' radio buttons next to it.

**Operation Mode** pane

This pane's parameters are described below.

Field	Description
-------	-------------

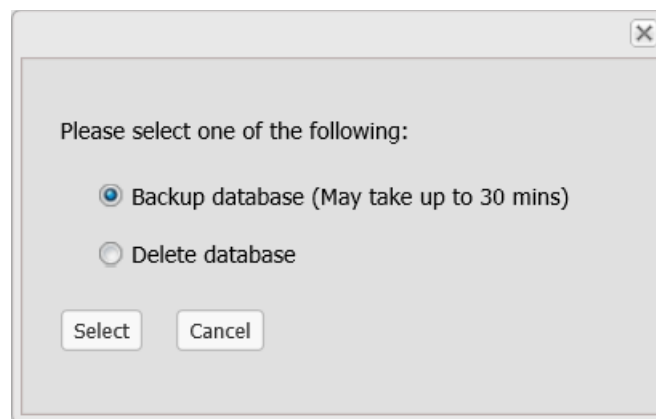
**Operation Mode** can be one of:

- **Training** - Telepath monitors web applications and learns their behavior, but does not alert when it detects anomalous activity. When Telepath is first installed, it remains in **Training** mode for the period specified in the **Training Level** option in the **Settings** tab, measured by either elapsed time or the number of requests processed by Telepath.
- **Production** - Telepath monitors web applications and alerts when it detects anomalous activity.
- **Hybrid** - Telepath monitors web applications and alerts when it detects anomalous activity, and in addition, it also continues to learn application behavior during the hours specified under **Hybrid Mode Schedule**.

### Operation Mode

Field	Description
<b>Hybrid Mode schedule</b>	In Hybrid mode, Telepath monitors traffic while continuing to learn. You can specify during which days and hours the learning will take place.
<b>Stop Learning when number of requests reaches</b>	(Relevant for Hybrid and Training mode) The number of requests Telepath processes before it switches to production mode.

If you change **Operation Mode** to **Training** from **Production** or **Hybrid**, you will be asked to choose whether to save the knowledge database or to delete it, that is, to forget everything that Telepath has learned by monitoring your site's traffic.



Backup or delete database

To save the database, click **Backup database**. This may take some time to complete.

If you click **Delete database**, Telepath will forget everything it has learned and will begin learning from scratch.



You should delete the database only in exceptional circumstances. Once deleted, the database cannot be easily restored.



## Reports

The Report Format pane defines the parameters related to the reports periodically generated by Telepath.

The screenshot shows the 'Reports' tab in the Telepath interface. At the top, there is a navigation bar with buttons for Administration, Save, Cancel, Network, Operation Mode, Advanced Settings, and Reports. Below the navigation bar, there are two radio buttons: 'On' (selected) and 'Off'. The main area is titled 'Report Settings' and contains the following controls:

- Report Frequency:** A numeric input set to '1' and a unit dropdown menu set to 'Hours'.
- Maximum Event:** A numeric input set to '50'.
- Time Window Back:** A numeric input set to '1' and a unit dropdown menu set to 'Hours'.
- By Saved Filter:** An unchecked checkbox and an empty dropdown menu.
- Rule Group:** A checked checkbox and a dropdown menu set to 'multiple\_searches'.
- All Events:** A checked checkbox.
- Configure Schedule:** A button at the bottom left of the settings panel.

**Report Format** pane

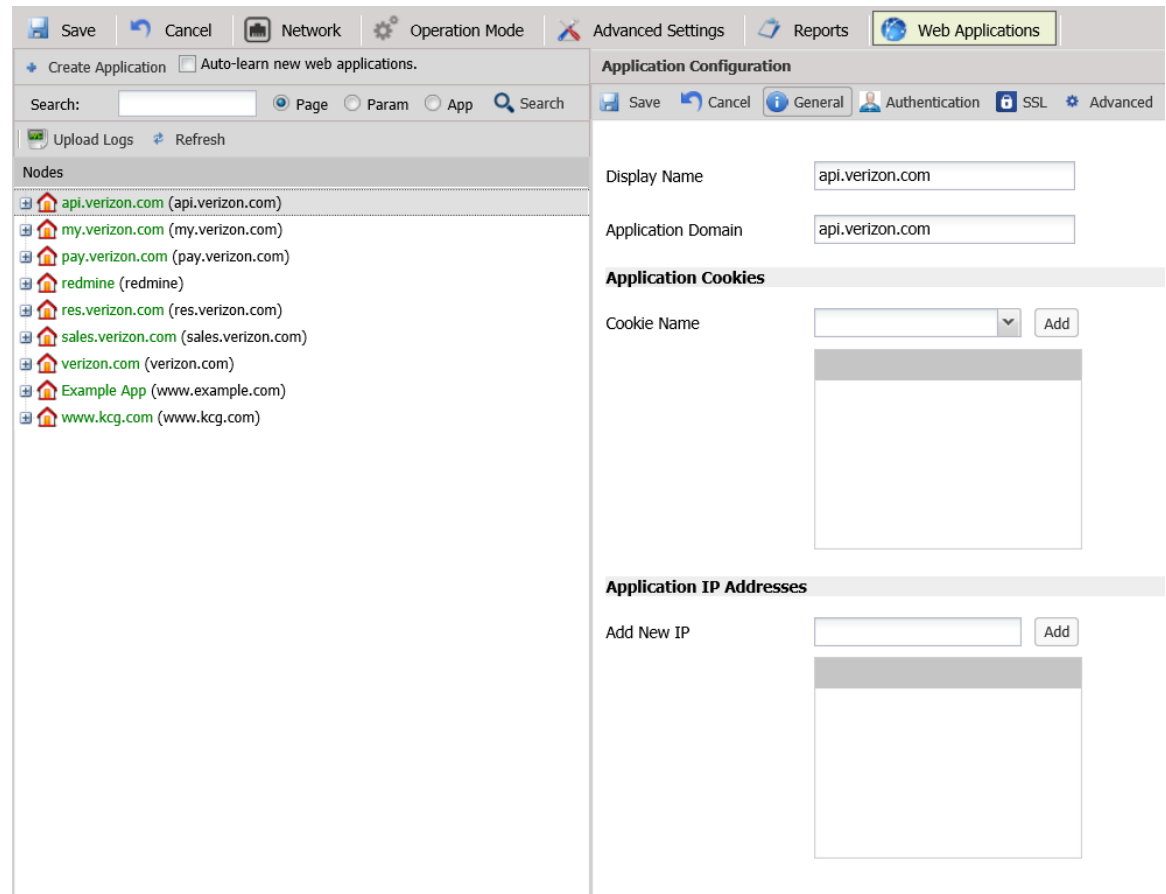
This pane's parameters are described below.

Field	Description
<b>On / Off</b>	<b>On</b> means that Telepath generates reports. <b>Off</b> means Telepath does not generate reports.
<b>Report Frequency</b>	How frequently to produce the report.
<b>Maximum Events</b>	The maximum number of alerts to be included in each report.
<b>Time Window Back</b>	The report will include alerts from the time of the report and the specified prior period.
<b>By Saved Filter</b>	Select <b>By Saved Filter</b> if the report is to include only alerts specified by the selected filter.
<b>Rules tree</b>	Select a rule or set of rules if the report is to include only events in which the anomaly belongs to the selected rule(s).
<b>All Events</b>	Select <b>All Events</b> if the report is to include all alerts during the specified period.
<b>Configure Schedule</b>	Specify the days of the week and hours during which to produce the report.

# Web Applications

The **Web Applications** window specifies information about the web applications monitored by Telepath, and consists of the following panes:

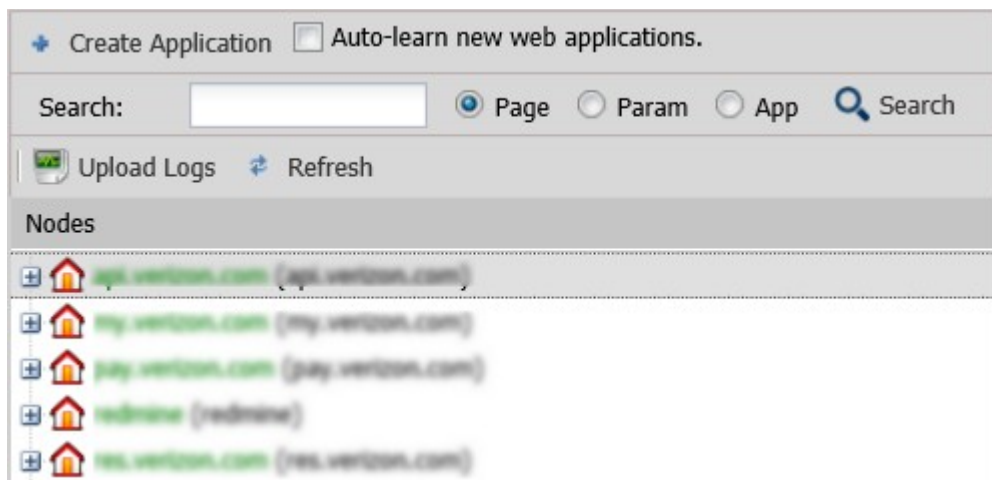
Field	For more information, see
Web Application List	
Web Application General	
Web Application Authentication	
Web Application SSL	
Web Application Advanced	Error: Reference source not found



Web Applications window

## Web Application - Nodes List






The left pane of the **Web Applications** window displays a list of the web applications Telepath has learned by monitoring web traffic.



### Web Applications - List pane


If you select an application from the list, its details are displayed in the **Web Application General** pane on the right.

This pane's parameters are described below.

Field	Description
	Add a new application to Telepath.
<input type="checkbox"/> Auto-learn new web applications	Set Telepath to learn new applications automatically when in Hybrid mode.
 Search	Search the Nodes list for an application, page or parameter.
	Upload Apache or IIS logs to speed up the training process.
	Delete the selected application from Telepath.
	Refresh the Nodes list.

## Creating applications

### To create a new application:

1. Click  **Create Application**. The Add Application dialog is displayed in the General tab.

The screenshot shows a window titled "Add Application" with a close button in the top right corner. The window contains three main sections: "General", "Application Cookies", and "Application IP Addresses".

- General**: Contains two text input fields labeled "Display Name" and "Application Domain".
- Application Cookies**: Contains a "Cookie Name" label, a text input field with a dropdown arrow, and an "Add" button. Below this is a large empty rectangular area.
- Application IP Addresses**: Contains an "Add New IP" label, a text input field, and an "Add" button. Below this is a large empty rectangular area.

At the bottom of the window is a row of five buttons: "Save" (with a floppy disk icon), "General" (with an information icon), "Authentication" (with a user icon), "SSL" (with a lock icon), and "Advanced" (with a gear icon). The "General" button is currently selected.

2. Fill in the application's General details. For more information, see .
3. Click **Authentication** at the bottom to fill in the application's authentication details. For more information, see .
4. Click **SSL** at the bottom to fill in the application's SSL details. For more information, see .
5. Click **Advanced** to fill in the application's advanced details. For more information, see Error: Reference source not found.
6. Click **Save**.
7. Click **OK** in the confirmation message that appears.


## Editing Applications

### To edit an existing application's settings:

1. Select the application from the Nodes list. The Application Configuration pane opens.
2. Edit the application's settings, as explained in the section above.
3. Click **Save**.

## Searching the Nodes List


### To search for an application, page or parameter:

1. In the  **Search** field, specify all or part of the item's name.
2. Select the type of item you want to find (**Page**, **Param** or **App**).
3. Click **Search**.

## Uploading Application Logs to Telepath

Application log files speed up the training process. After uploading the log file, the system reads (parses) the logs and learns what common web application pages the user is accessing.

### To upload a log file:


1. Click  **Upload Logs**. A browse window is displayed.
2. Browse for the file.
3. Select the appropriate **Log Type**.
4. Click **Start**.

## Deleting Applications



If multiple applications are selected, the one appearing highest in the Nodes list will be deleted.

### To delete an application:

1. Select the application from the Nodes list.
2. Click  **Delete**.
3. Click **OK** in the confirmation message.

## Web Application - General

The **Web Application General** pane displays the details of the application selected in the left pane of the **Web Applications** window.

The screenshot shows the 'Application Configuration' dialog box with the 'General' tab selected. The dialog has a title bar and a toolbar with 'Save', 'Cancel', 'General', 'Authentication', 'SSL', and 'Advanced' buttons. The 'General' tab contains the following fields:

- Display Name:** A text box containing 'api.version.com'.
- Application Domain:** A text box containing 'api.version.com'.
- Application Cookies:** A section header followed by a 'Cookie Name' label, a dropdown menu, and an 'Add' button. Below this is a large empty text area.
- Application IP Addresses:** A section header followed by an 'Add New IP' label, a text box, and an 'Add' button. Below this is a large empty text area.

### Web Applications - General pane

This pane's parameters are described below.

Field	Description
<b>Display Name</b> <b>Application Domain</b>	These fields correspond to the fields with the same names in the left pane.
<b>Cookie Name</b>	Specify the name of a cookie unique to each session. Select a name from the drop down menu or enter a name in the text box, and click <b>Add</b> .
<b>Add New IP</b>	The IP address of the server hosting the application. If there are multiple servers, add them all and click <b>Add</b> .

Field	Description
	If the servers are behind a load balancer, specify the IP address before the load balancer, that is, the IP address to which the <b>Application Domain</b> resolves.

## Web Application - Authentication

**Application Configuration**

Save Cancel General **Authentication** SSL Advanced

**User Identification**

☒ Automatic  
☐ Form  
☐ Basic  
☐ Digest  
☐ NTLM

**Success Criteria**

☐ On
 ☒ Off

---

☐ Cookie
 Name  Value

☒ Above value is missing
 ☐ Above value appears

---

☐ Redirect
 Page

Response Status is between  and

---

☐ Body Value
 Value to search in HTML body

### Web Applications - Authentication pane

The **Web Application - Authentication** pane specifies the user authentication method used by the application and optionally, the success criteria. Telepath needs this information in order to extract the user's name from the web traffic.

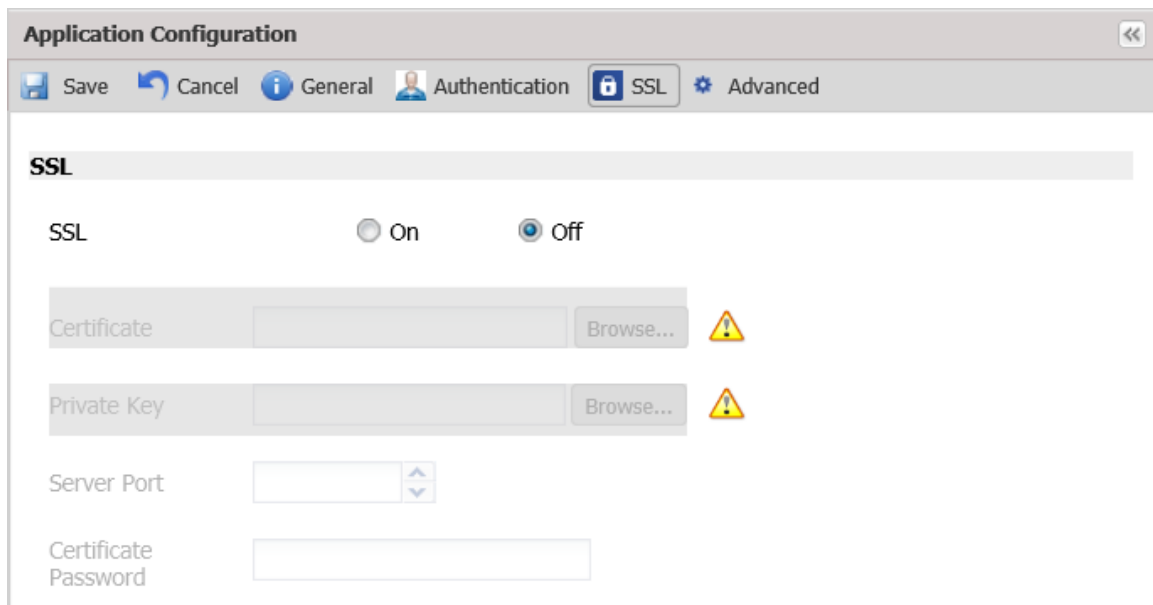
This pane's parameters are described below.

Field	Description
<b>User Identification</b>	Select one of the methods listed.
<b>Success Criteria</b>	Select <b>On</b> or <b>Off</b> and then specify the method for Telepath to use to determine whether authentication was successful. If you can select multiple methods, they are OR'ed. If <b>Cookie</b> is selected, then:
<b>Cookie</b>	<ul style="list-style-type: none"><li>• If <b>Above value appears</b> is checked, authentication is considered to have been successful if the application sets a cookie with the specified <b>Name</b> and <b>Value</b>.</li><li>• If <b>Above value is missing</b> is checked, authentication is considered to have been successful if the application does <i>not</i> set a cookie with the specified <b>Name</b> and <b>Value</b>.</li></ul>
<b>Redirect</b>	If <b>Redirect</b> is selected, authentication is considered to have been successful if the application redirects the client to <b>Page</b> and the response status is between the specified values.
<b>Body Value</b>	If <b>Body Value</b> is selected, authentication is considered to have been successful if the application's specified response contains <b>Value to search in HTML body</b> .



## Web Application - SSL

The **Web Application - SSL** pane specifies the SSL certificate and private key used by the application. Telepath needs this information in order to decrypt the application's traffic.



The screenshot shows the 'Application Configuration' dialog box with the 'SSL' tab selected. The 'SSL' section has a toggle switch set to 'Off'. Below the toggle are fields for 'Certificate' and 'Private Key', each with a 'Browse...' button and a warning icon. There is also a 'Server Port' field with up/down arrows and a 'Certificate Password' field.

### Web Applications - SSL pane

This pane's parameters are described below.

Field	Description
<b>SSL</b>	Specify whether SSL is <b>On</b> or <b>Off</b> .
<b>Certificate</b>	If <b>SSL</b> is <b>On</b> , specify the name of the certificate file and, optionally, the <b>Private Key</b> file in the event that the private key is stored in a different file from the certificate.
<b>Private Key</b>	
<b>Server Port</b>	The port the application server uses for SSL.
<b>Certificate Password</b>	The password required to extract the private key from either the certificate file or the private key file.

# Web Application - Advanced

Application Configuration

Save

Cancel

General

Authentication

SSL

Advanced

Application Global Pages

Regular Expression

Add

Regular Expression		
/b144_sip/members/		
/b144_sip/clients/		
^/(%[a-z0-9]{2}[ ]?)+(.)+[.]aspx\$		
^/products/(%[a-z0-9]{2}[ ]?)+(.)+[.]aspx\$		

API Settings

Injected Header Name

Session Clear Cookie Name

Session Clear Cookie Value

## Web Applications - Advanced pane

The **Web Application - Advanced** pane defines Telepath functionality, and consists of the following sections:

Field	For more information, see
Application Global Pages	
API Settings	

## Application Global Pages


The **Application Global Pages** are defined when the application generates multiple pages with different URLs which should be considered by Telepath to be a single page. For example, an application might generate differently named URLs for each item in the vendor price list, where the URL includes an ISBN number (for books) or an SKU (for catalog items), but from Telepath's point of view, all these pages are functionally identical and there is no need to track each one individually. Instead, all of them are treated by Telepath as if they were the same page.

Field	Description
<b>Regular Expression</b>	A regular expression that describes the variable part of the URL, for example, the catalog number.

## API Settings

The **API Settings** are defined when a Telepath agent installed on the application server which injects a header into the incoming web traffic which the application recognizes as a signal to terminate the session. Communication between the Telepath agent and Telepath is initiated by the agent.

For more information, see .

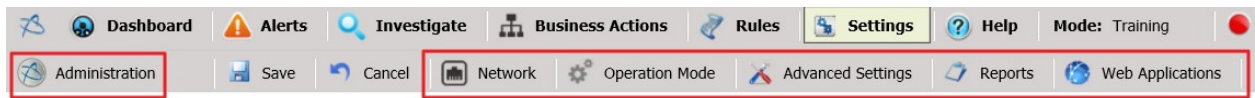
Field	Description
<b>Injected Header Name</b>	The name of the header.
<b>Session Clear Cookie Name</b>	The name of the cookie sent by the web server that indicates the session is to be cleared.
<b>Session Clear Cookie Value</b>	The cookie value that indicates that the session has ended.
 <b>Note</b>	Implementation of this feature requires changes to the web application.

Click the **Settings** tab to display a list of the configuration options:

Option	Description
<b>Administration</b>	
<b>Network</b>	
<b>Operation Mode</b>	
<b>Reports</b>	
<b>Web Applications</b>	

If you change any of the configuration options, remember to click the **Save** button in the **Settings** toolbar.

To display the configuration parameters for any of these options, click the appropriate tab:



**Settings** tab options

# Rule Use Cases

## Parameter rules

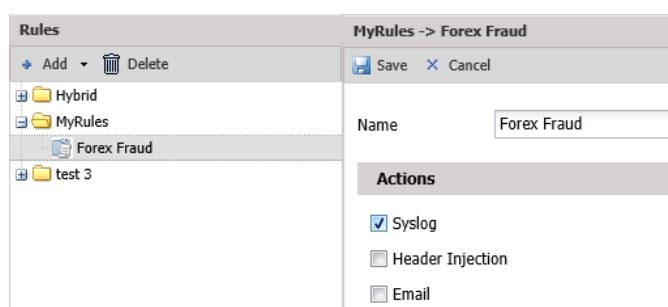
### Forex Fraud

A user attempts to convert the smallest possible amount of a weak currency into a much stronger one. For example, converting 0.01 Russian rubles into British pounds.

Assuming that 0.01 Russian rubles are worth 0.0000199 British pounds, there is no British currency unit that can do this. So in such a situation, the Forex agency might mistakenly exchange 0.01 Russian rubles to 0.01 British pounds (the British currency unit closest to 0.01 Russian rubles), thereby giving the user a 500 % return above the correct amount.

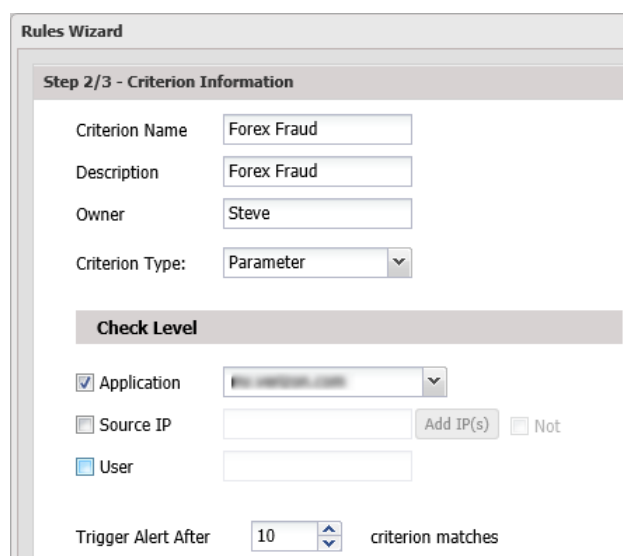
#### To define this rule:

1. Create a rule with a meaningful name (e.g. "Forex Fraud") and set the alert **Action** (e.g. "Syslog").



The screenshot shows a 'Rules' configuration window. On the left, a tree view shows a folder 'MyRules' containing a rule named 'Forex Fraud'. The main area on the right is titled 'MyRules -> Forex Fraud'. It has a 'Name' field with 'Forex Fraud' entered. Below it, under the 'Actions' section, the 'Syslog' checkbox is checked, while 'Header Injection' and 'Email' are unchecked.

2. Add a **Parameter** criterion to the rule.
3. Specify the appropriate **Check Level**(s) (e.g. which application to check this rule against).
4. Set the **Trigger Alert After** field to **10**.



The screenshot shows the 'Rules Wizard' at 'Step 2/3 - Criterion Information'. It contains several input fields: 'Criterion Name' (Forex Fraud), 'Description' (Forex Fraud), 'Owner' (Steve), and 'Criterion Type' (Parameter). Below these is a 'Check Level' section with three options: 'Application' (checked), 'Source IP' (unchecked), and 'User' (unchecked). The 'Application' dropdown is set to 'Web Services'. At the bottom, the 'Trigger Alert After' field is set to '10' with a unit dropdown set to 'criterion matches'.

5. Click **Next**.
6. In the Parameter Criterion screen, do the following:
  - Browse for the appropriate **Page Parameter** (e.g. "exchange-amount").
  - In the **String Inspection** area, make sure **Heuristic** is selected.

Rules Wizard

Step 3/3 - Parameter Criterion

Please select one of the following options:

☒ Page

Parameter

String Inspection

☒ Heuristic

7. Click **Submit**.

## Web Scraping

A business competitor is attempting to copy the website contents record by record (email addresses, phone numbers and prices). The competitor searches for a specific value (e.g. aa) and changes it by one character each time. To avoid detection, the competitor does 10 searches from a different IP address.

For example:

Aa	ba	Ca
Ag	bs	Ct
An	bm	Cn

### To define this rule:

1. Create a rule with a meaningful name and set the alert **Action**.
2. Add a **Parameter** criterion to the rule.
  - a. Set the appropriate **Check Level**.
  - b. Set the **Trigger Alert After** field to **3** (aggregate of events)
  - c. Select the appropriate **Page Parameter** (e.g. "Search").
  - d. In the string Inspection area, select **Parameter values differ by** and set it to **1**.
  - e. Click **Submit**.
3. Add another **Parameter** criterion to this rule with the same **Trigger Alert After** and **Page Parameter** values.
  - a. In the String Inspection area, select **Fuzzy Length** and set it to **Short** (to show that the competitor is searching for short terms, one character apart).
  - b. Click **Submit**.

## Request Tampering

A user has a coupon for a hamburger and a beverage, however this coupon provides a cheap beverage while the user wants to obtain a more expensive one, such as a beer. In the form submission, the user injects a value that is not available in the beverage selection field.

Since Telepath automatically learns the commonly used values for the field, it would render it anomalous.

### To define this rule:

1. Create a rule with a meaningful name and set the alert **Action**.
2. Add a **Parameter** criterion with the appropriate **Check Level(s)**.
  - a. Click **Next**.
  - b. Browse for the appropriate **Page Parameter** (e.g. "Beverage Selection").
  - c. In the String Inspection area, make sure **Heuristic** is selected.
  - d. Click **Submit**.

## Pattern Rules

### Testing stolen credit cards

A fraudster is attempting to "test" credit cards by entering a different credit card each time.

For example:

34960448169330	37834506074161	34477070883291
6	1	3
34164755644706	37074104770964	39856506074161
4	8	1

### To define this rule:

1. Create a rule with a meaningful name and set the alert **Action**.
2. Add a **Pattern** criterion with the appropriate **Check Level(s)**.

Rules Wizard

Step 2/3 - Criterion Information

Criterion Name:

Description:

Owner:

Criterion Type:

Check Level

☒ Application

☐ Source IP  ☐ Not

☐ User

3. Click **Next**.

4. In the Pattern Criterion screen, do the following:

- In the Anchor area, select **IP**.
- Browse for the appropriate **Page** (e.g. "credit-card-number").
- Set **Count** to **5** and **Time Window** to **72 Hours**.

The screenshot shows the 'Rules Wizard' interface at 'Step 3/3 - Pattern Criterion'. Under the 'Anchor' section, 'IP' is selected with a radio button. Below it are options for 'SID', 'Device Fingerprint', 'User', and 'Other'. The 'Page' section has 'credit-card-number' entered in the text box, with 'Browse' and 'Remove' buttons. The 'Changing Parameter' and 'Repeating Action' sections are empty. The 'Count' is set to '5' and the 'Time Window' is set to '72' with a unit dropdown set to 'Hours'.

5. Click **Submit**.

## eCoupon Abuse

A user is attempting to use 10 different coupons in the same session.

### To define this rule:

1. Create a rule with a meaningful name and set the alert **Action**.
2. Add a **Pattern** criterion with the appropriate **Check Level(s)**.
3. Click **Next**.
4. In the Pattern Criterion screen, do the following:
  - In the Anchor area, select **SID** (same session).
  - Browse for the **Page** on which the coupon is entered.
  - Set **Count** to **10** and **Time Window** to **24 Hours**.
5. Click **Submit**.

## Account hijacking: Man-in-the-browser

Multiple rapid money transfers using account takeover.

A fraudster has hijacked a bank account by using stolen credentials or installing a man-in-the-browser Trojan horse and is attempting to make 10 different money transfers from the hijacked account in 15 minutes.



### To define this rule:

1. Create a rule with a meaningful name and set the alert **Action**.
2. Add a **Pattern** criterion with the appropriate **Check Level(s)**.
3. Click **Next**.
4. In the Pattern Criterion screen, do the following:
  - Select the appropriate Anchor.
  - In **Repeating Action**, browse for the appropriate business action (e.g. "Money Transfer" assuming a "Money Transfer" business action has been recorded).
  - Set **Count** to **10** and **Time Window** to **15 Minutes**.
5. Click **Submit**.

## Mass Registration

A fraudster is attempting multiple registrations from the same IP over a short period of time.

### To define this rule:

1. Create a rule with a meaningful name and set the alert **Action**.
2. Add a **Pattern** criterion with the appropriate **Check Level(s)**.
3. Click **Next**.
4. In the Pattern Criterion screen, do the following:
  - In the Anchor area, select **IP**.
  - Browse to the appropriate **Page** (e.g. registration page).
5. Set **Count** to **5** and **Time Window** to **72 Hours**.
6. Click **Submit**.

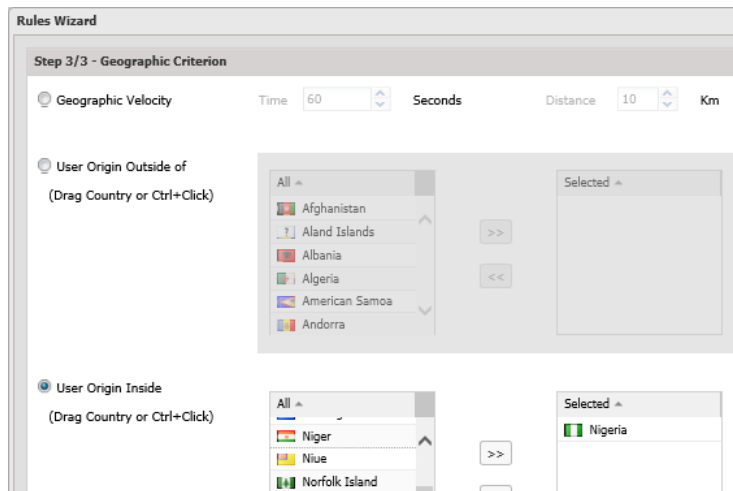
## Geographic Rules

### eFraud Hotspots

Alert when requests originate from countries known to have high levels of fraudulent activity. For example, Nigeria.

### To define this rule:

1. Create a rule with a meaningful name and set the alert **Action**.
2. Add a **Geographic** criterion with the appropriate **Check Level(s)**.
3. Click **Next**.
4. Select **User Origin Inside**, select **Nigeria** and move it into the **Selected** pane.



5. Click **Submit**.

## Session velocity

A fraudster goes online and changes geographic locations in a short period during the same session. This might suggest that either the session being used has been hijacked by a fraudster or the fraudster is attempting to mask his true origin by rapidly changing locations.

### To define this rule:

1. Create a rule with a meaningful name and set the alert **Action**.
2. Add a **Geographic** criterion with the appropriate **Check Level(s)**.
3. Click **Next**.
4. Select **Geographic Velocity**, set **Time** to **60** seconds and **Distance** to **10** km.
5. Click **Submit**.

## Fake Account Registration

Discrepancies between registration details and geographic origin of the IP address: a fraudster is using a British email address (ending with .co.uk) to log in to the application while the login action appears to be originating from a different country (e.g. Nigeria) in the same session.

### To define this rule:

1. Create a rule with a meaningful name and set the alert **Action**.
2. Add a **Parameter** criterion.
  - a. Click **Next**.
  - b. Select the appropriate **Page Parameter** (e.g. "Country").
  - c. In the **String Inspection** area, select **String Contains** and specify "United Kingdom". This will check all requests including the string "United Kingdom".
  - d. Click **Submit**.
3. Add a **Geographic** criterion.

- a. Click **Next**.
- b. Select **User Origin Outside of**, select **United Kingdom** and move it into the **Selected** pane.
- c. Click **Submit**.

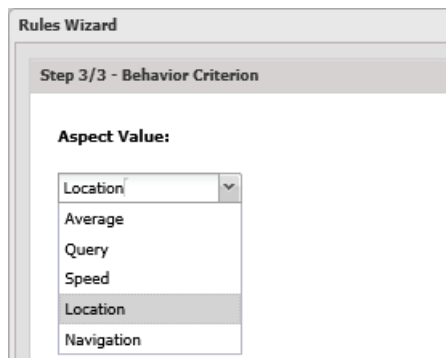
## Behavior Rules

### Unusual Geographic Location

A user of the application who has always logged in from his home in Canada is attempting to log in from Nigeria.

#### To define this rule:

1. Create a rule with a meaningful name and set the alert **Action**.
2. Add a **Behavior** criterion to the rule.
3. In the Score Type area, set a **Numeric** score of **95** (to look for requests with a risk score of 95% or higher).
4. Click **Next**.
5. From the **Aspect Value** drop-down list, select **Location**.



Rules Wizard

Step 3/3 - Behavior Criterion

Aspect Value:

Location

Average

Query

Speed

Location

Navigation

6. Click **Submit**.

### Suspicious User Action

An account holder is attempting to transfer all funds from his bank account to a bank in Nigeria.

#### To define this rule:

1. Create a rule with a meaningful name and set the alert **Action**.
2. Add a **Behavior** criterion to the rule.
3. In the Score Type area, set a **Numeric** score of **95** (to look for requests with a risk score of 95% or higher).
4. Click **Next**.
5. From the **Aspect Value** drop-down list, select **Query**.
6. Click **Submit**.

## Grouping different criterions under one rule

The following rules have multiple criterions. As such, a rule is triggered only if all criterions are matched.

### Suspiciously behaving bots

An IP address has been infected with a spyware program that installed a freeware that transparently installed a toolbar on the system. A user originating from the infected IP address is performing suspicious actions, such as abnormal click speeds and transferring suspicious amounts of money.

Conditions:

- User's click speed is abnormally fast
- User attempts to transfer a suspicious amount of money

Result: Scenarios where both conditions exist suggest that a bot is performing these actions.

#### To define this rule:

1. Create a rule with a meaningful name and set the alert **Action**.
2. Add a **Behavior** criterion to the rule.
  - a. Call it "Click Speed".
  - b. In the Score Type area, set a **Numeric** score of **95** (to look for requests with a risk score of 95% or higher).
  - c. Click **Next**.
  - d. From the **Aspect Value** drop-down list, select **Speed**.
  - e. Click **Submit**.
3. Add a **Parameter** criterion.
  - a. Call it "Suspicious Money Transfer".
  - b. Click **Next**.
  - c. Browse for the appropriate **Page Parameter** (e.g. "Amount").
  - d. Click **Submit**.

### Mass registration attempts directed at one page (layer-7 DoS)

A fraudster is attempting to flood the system with massive amounts of registration requests in order to consume as much of the site's resources as possible so that legitimate users are denied service.

- User performs suspicious actions
- User performs a high number of requests in a short period

#### To define this rule:

1. Create a rule with a meaningful name and set the alert **Action**.
2. Add a **Behavior** criterion to the rule.
  - a. Call it "Suspicious Actions".

- b. In the Score Type area, set a **Numeric** score of **95** (to look for requests with a risk score of 95% or higher).
  - c. Click **Next**.
  - d. From the **Aspect Value** drop-down list, select **Query**.
  - e. Click **Submit**.
- 3. Add a **Pattern** criterion.
  - a. Call it "Requests".
  - b. Click **Next**.
  - c. From the Anchor area, select **IP**.
  - d. Browse for the appropriate **Page** (e.g. "Registration Request").
  - e. Set the **Count** to **50** and **Time Window** to **1 Minute**.
  - f. Click **Submit**.

# Troubleshooting

---

## **Telepath Engine not starting after Telepath installation**

If Telepath Engine doesn't start after installation, (green "On" button on the tab bar), open command-line and run: "Telepath Start"

# Index

---

aspect criteria	32, 48	parameter criteria	30, 47
behavior criteria	32, 48	pattern criteria	32, 49
bot-intelligence criteria	36, 52	production mode	39
criteria		rules	
deleting	37, 53	creating	28, 44
editing	37, 53	scraping attacks	31, 48
dashboard	53	session ID	59
disabling criteria	36, 52	status	38
engine	38	training mode	39
geographic criteria	35, 51		
heuristic algorithms	30, 47		
hot spots	55		
hybrid mode	39		