Plugins

DenyAll

V5.2.0

CONTENTS

CHAPTER

ONE

DENY ALL WAF

Deny All WAF normalizes Deny All WAF events and enables you to analyze Deny All WAF data. LogPoint aggregates and normalizes Deny All WAF logs so you can analyze the information through the *LP_Deny All Web Application Firewall* dashboard. The dashboard provides visualization of incident details for web attack source addresses, countries and other event details detected in your network. You can customize the dashboard to suit your needs and perform in-depth analysis by adjusting the data and searches.

Furthermore, when LogPoint identifies threats, malware, or malicious events with a potential risk, it triggers security alerts based on predetermined rules. The automated alerts enable you to detect potential threats, malware, or malicious events early and take corrective actions against them.

Deny All WAF consists of the following components:

1. **Dashboard Package**
    - LP_Deny All Web Application Firewall
2. **Compiled Normalizer**
    - LP_Deny All Web Application Firewall
3. **Alert Package**
    - LP_DenyAllWAF SQL Injection Attack

CHAPTER

TWO

INSTALLING DENY ALL WAF

Prerequisite

LogPoint v6.7.4 or later

Supported Device

Deny All WAF Server on the Unix environment.

To install Deny All WAF:

1. Download the .pak file from the Help Center.
2. Go to *Settings >> System Settings >> Applications*.
3. Click **Import**.
4. **Browse** to downloaded .pak file.
5. Click **Upload**.

After installing Deny All WAF, you can find it under *Settings >> System Settings >> Plugins*.

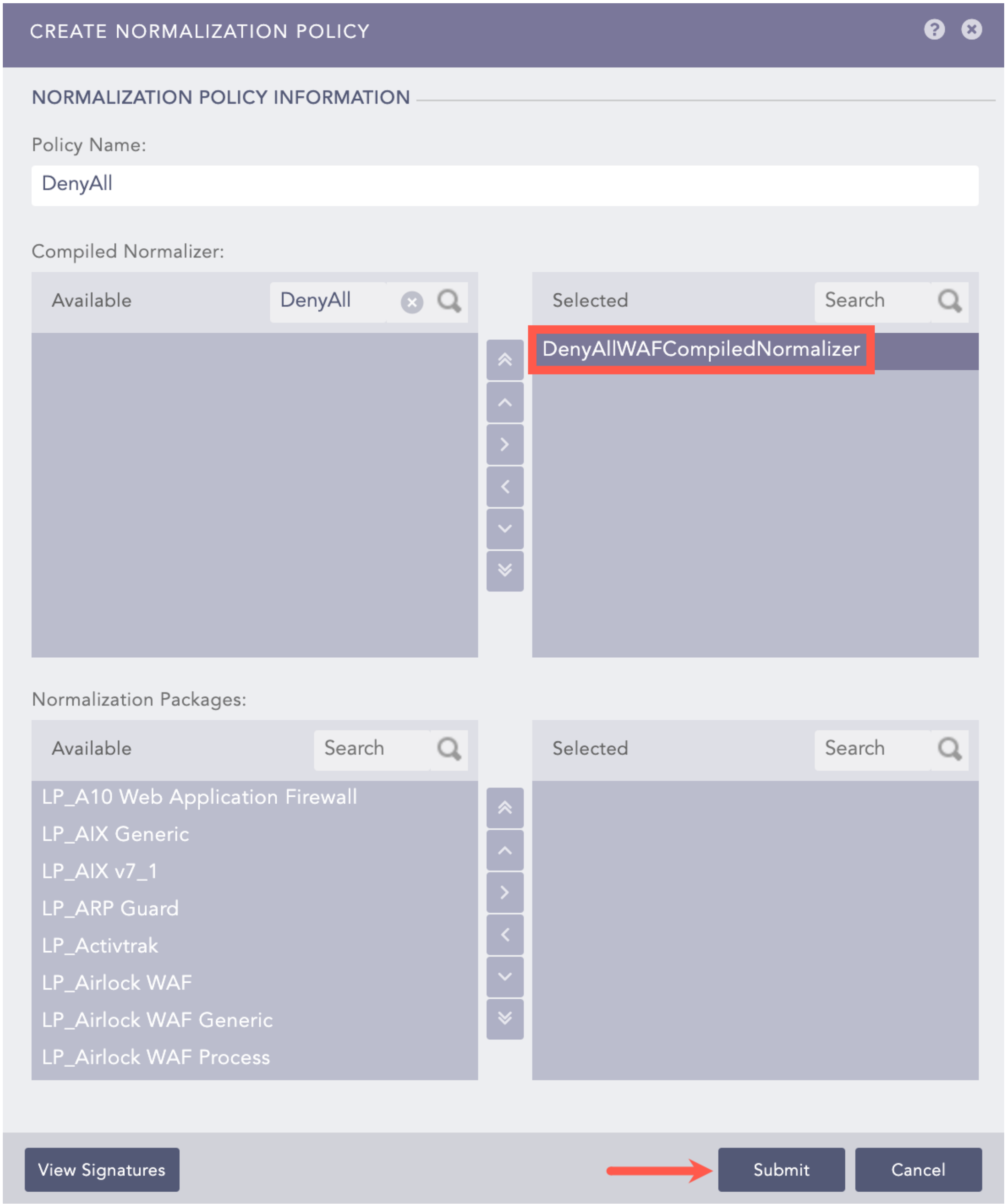
CHAPTER

THREE

CONFIGURING DENY ALL WAF

3.1 Adding a Normalization Policy for Deny All WAF

1. Go to *Settings >> Configuration >> Normalization Policies*.
2. At the top left, click **Add**.
3. Enter a **Policy Name**.
4. In **Compiled Normalizers**, select *Deny All WAF*.
5. Click **Submit**.



CREATE NORMALIZATION POLICY

NORMALIZATION POLICY INFORMATION

Policy Name: DenyAll

Compiled Normalizer:

Available: DenyAll

Selected: DenyAllWAFCompiledNormalizer

Normalization Packages:

Available:

- LP_A10 Web Application Firewall
- LP_AIX Generic
- LP_AIX v7_1
- LP_ARP Guard
- LP_Activtrak
- LP_Airlock WAF
- LP_Airlock WAF Generic
- LP_Airlock WAF Process

Selected:

Fig. 1: Adding a Normalization Policy

3.2 Adding Deny All WAF as a Device in LogPoint

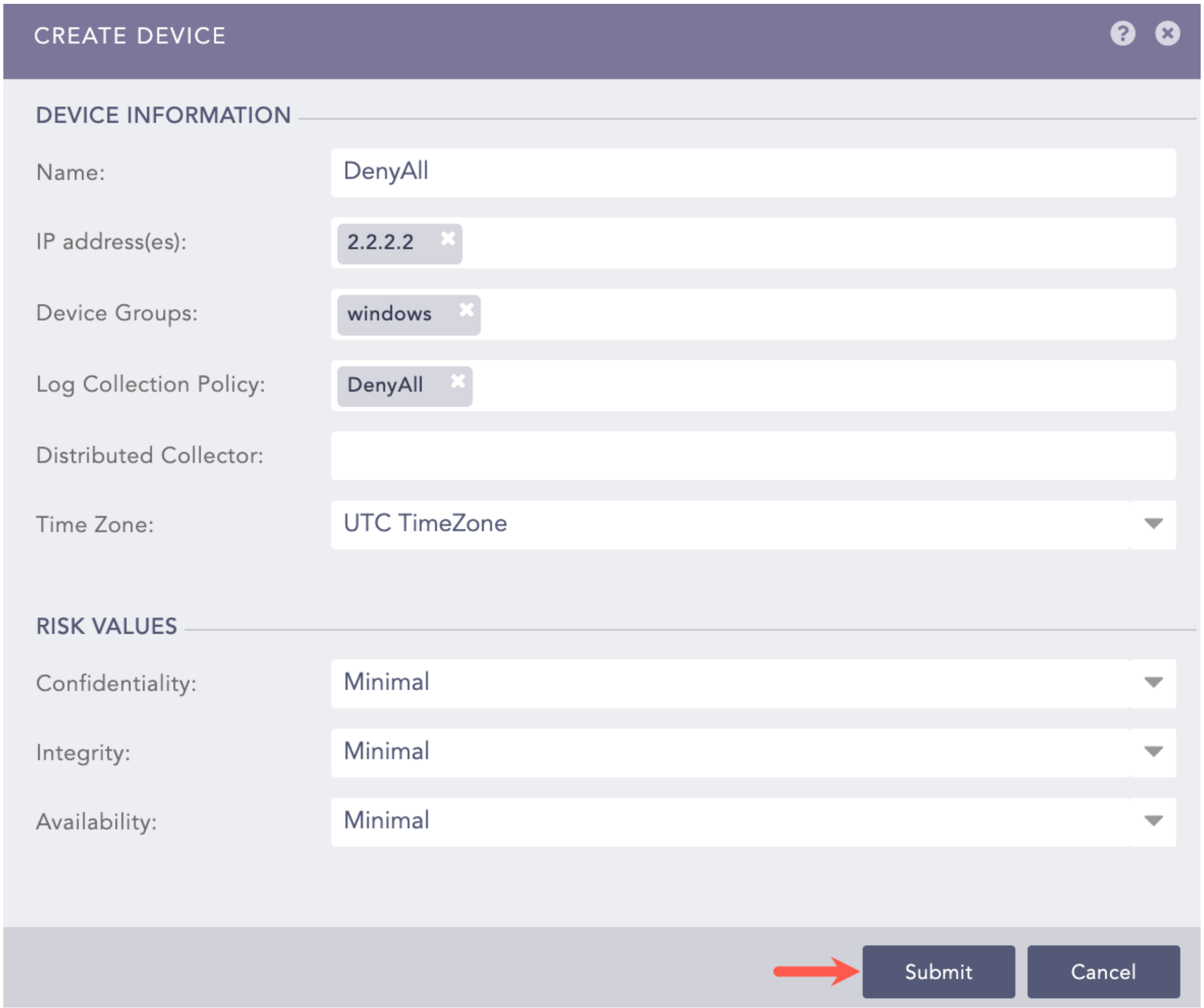
1. Go to *Settings >> Configuration >> Devices*.
2. At the top left, click **Add**.
3. Enter a device **Name**.
4. Enter the **IP address(es)** of the Deny All WAF server.
5. Select the **Device Groups**.
6. Select an appropriate **Log Collection Policy** for the logs.
7. Select a collector or a forwarder from the **Distributed Collector** drop-down menu.

Note: It is optional to select the **Device Groups**, the **Log Collection Policy**, and the **Distributed Collector**.

8. Select a **Time Zone**.

Note: The timezone of the device must be the same as its log source.

9. Configure the **Risk Values** for **Confidentiality**, **Integrity**, and **Availability** used to calculate the risk levels of the alerts generated from the device.
10. Click **Submit**.



DEVICE INFORMATION

Name: DenyAll

IP address(es): 2.2.2.2

Device Groups: windows

Log Collection Policy: DenyAll

Distributed Collector:

Time Zone: UTC TimeZone

RISK VALUES

Confidentiality: Minimal

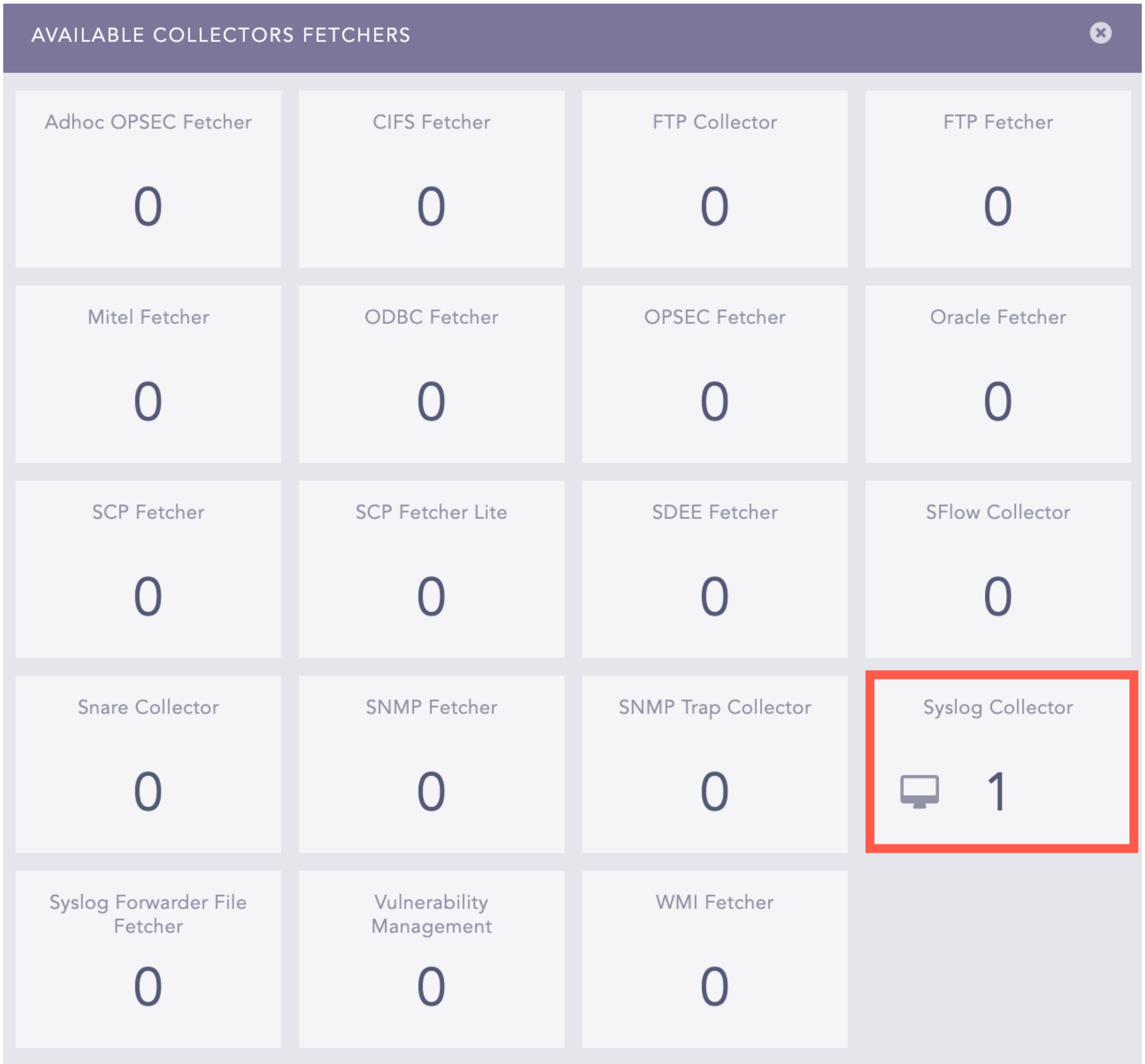
Integrity: Minimal

Availability: Minimal

Fig. 2: Adding Deny All WAF as a Device

3.3 Configuring the Syslog Collector for Deny All WAF

1. Click the **Add** icon from **Actions**.
2. Click **Syslog Collector** on **AVAILABLE COLLECTORS FETCHERS**.

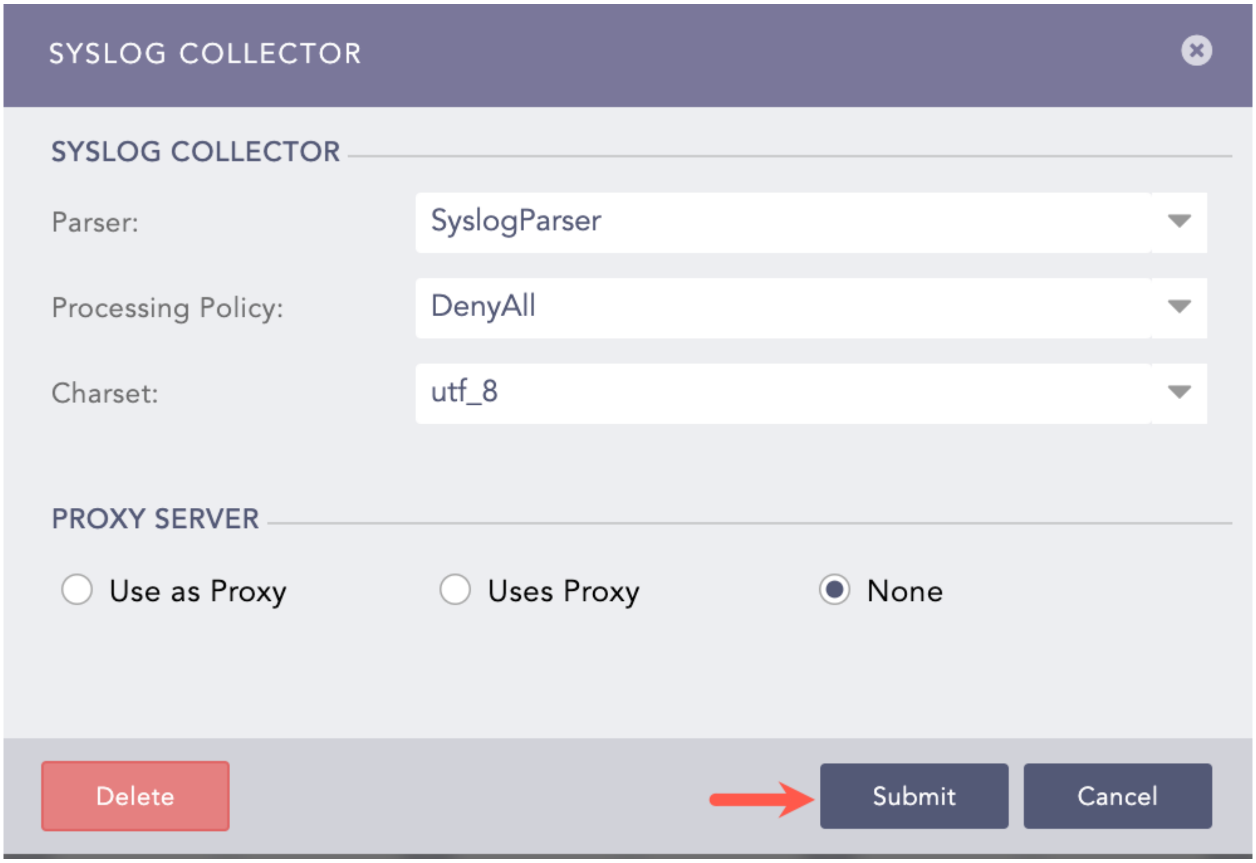


AVAILABLE COLLECTORS FETCHERS

Adhoc OPSEC Fetcher 0	CIFS Fetcher 0	FTP Collector 0	FTP Fetcher 0
Mitel Fetcher 0	ODBC Fetcher 0	OPSEC Fetcher 0	Oracle Fetcher 0
SCP Fetcher 0	SCP Fetcher Lite 0	SDEE Fetcher 0	SFlow Collector 0
Snare Collector 0	SNMP Fetcher 0	SNMP Trap Collector 0	Syslog Collector 1
Syslog Forwarder File Fetcher 0	Vulnerability Management 0	WMI Fetcher 0	

Fig. 3: Configuring Syslog Collector

3. In **Parser**, select **Syslog Parser**.
4. Select the **Processing Policy** which contains the *normalization policy* you added previously.
5. Select the **Charset**. The default value is *utf_8*.
6. In **PROXY SERVER**, select **None**.
7. Click **Submit**.



SYSLOG COLLECTOR

SYSLOG COLLECTOR

Parser: SyslogParser

Processing Policy: DenyAll

Charset: utf_8

PROXY SERVER

○ Use as Proxy ○ Uses Proxy ● None

Fig. 4: Configuring Syslog Collector

CHAPTER

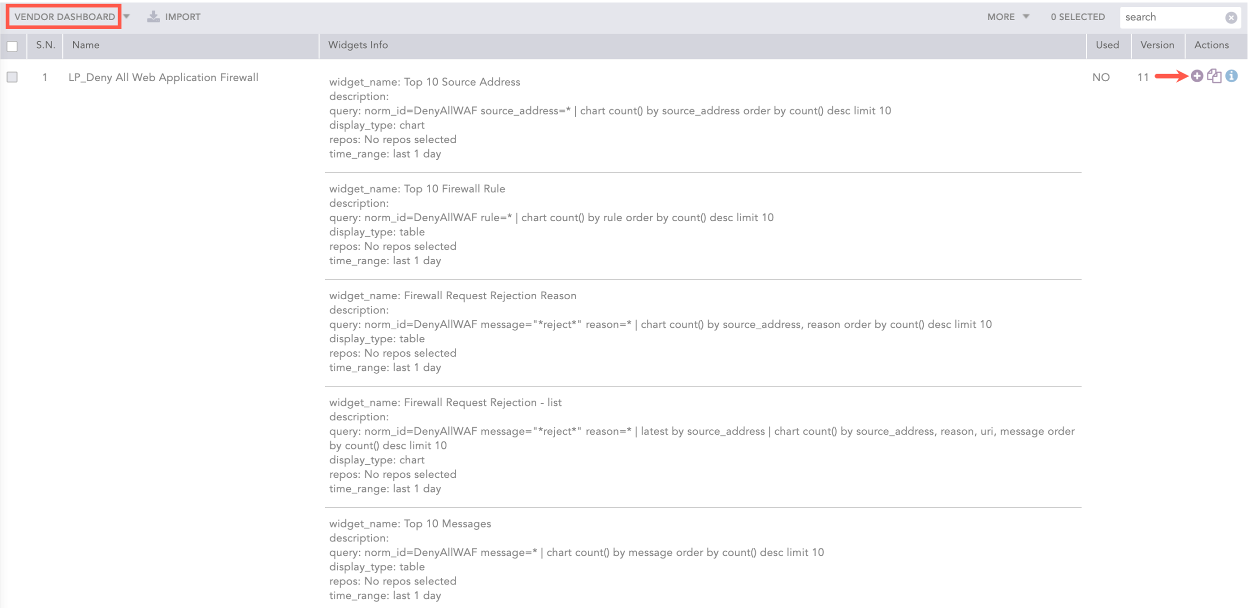
FOUR

DENY ALL WAF ANALYTICS

4.1 Deny All WAF Dashboards

4.1.1 Adding the Deny All WAF Dashboard

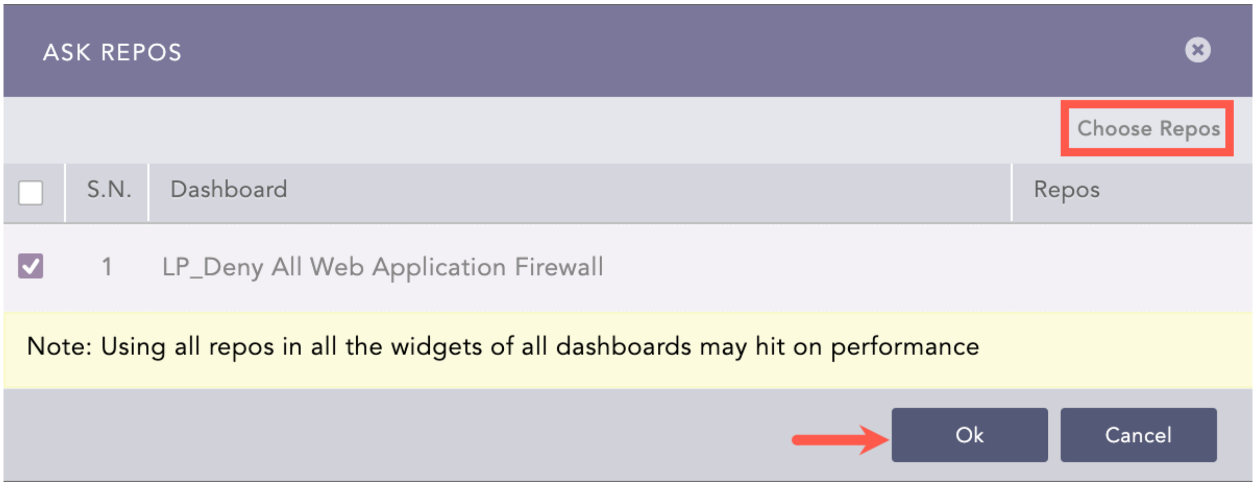
1. Go to *Settings >> Knowledge Base >> Dashboards*.
2. Select **VENDOR DASHBOARD** from the drop-down.
3. Click the **Use** icon from **Actions**.



□	S.N.	Name	Widgets Info	Used	Version	Actions
□	1	LP_Deny All Web Application Firewall	widget_name: Top 10 Source Address description: query: norm_id=DenyAllWAF source_address=* | chart count() by source_address order by count() desc limit 10 display_type: chart repos: No repos selected time_range: last 1 day widget_name: Top 10 Firewall Rule description: query: norm_id=DenyAllWAF rule=* | chart count() by rule order by count() desc limit 10 display_type: table repos: No repos selected time_range: last 1 day widget_name: Firewall Request Rejection Reason description: query: norm_id=DenyAllWAF message="*reject*" reason=* | chart count() by source_address, reason order by count() desc limit 10 display_type: table repos: No repos selected time_range: last 1 day widget_name: Firewall Request Rejection - list description: query: norm_id=DenyAllWAF message="*reject*" reason=* | latest by source_address | chart count() by source_address, reason, uri, message order by count() desc limit 10 display_type: chart repos: No repos selected time_range: last 1 day widget_name: Top 10 Messages description: query: norm_id=DenyAllWAF message=* | chart count() by message order by count() desc limit 10 display_type: table repos: No repos selected time_range: last 1 day	NO	11	⊕

Fig. 1: Adding the Deny All WAF Dashboard

4. Click **Choose Repos**.

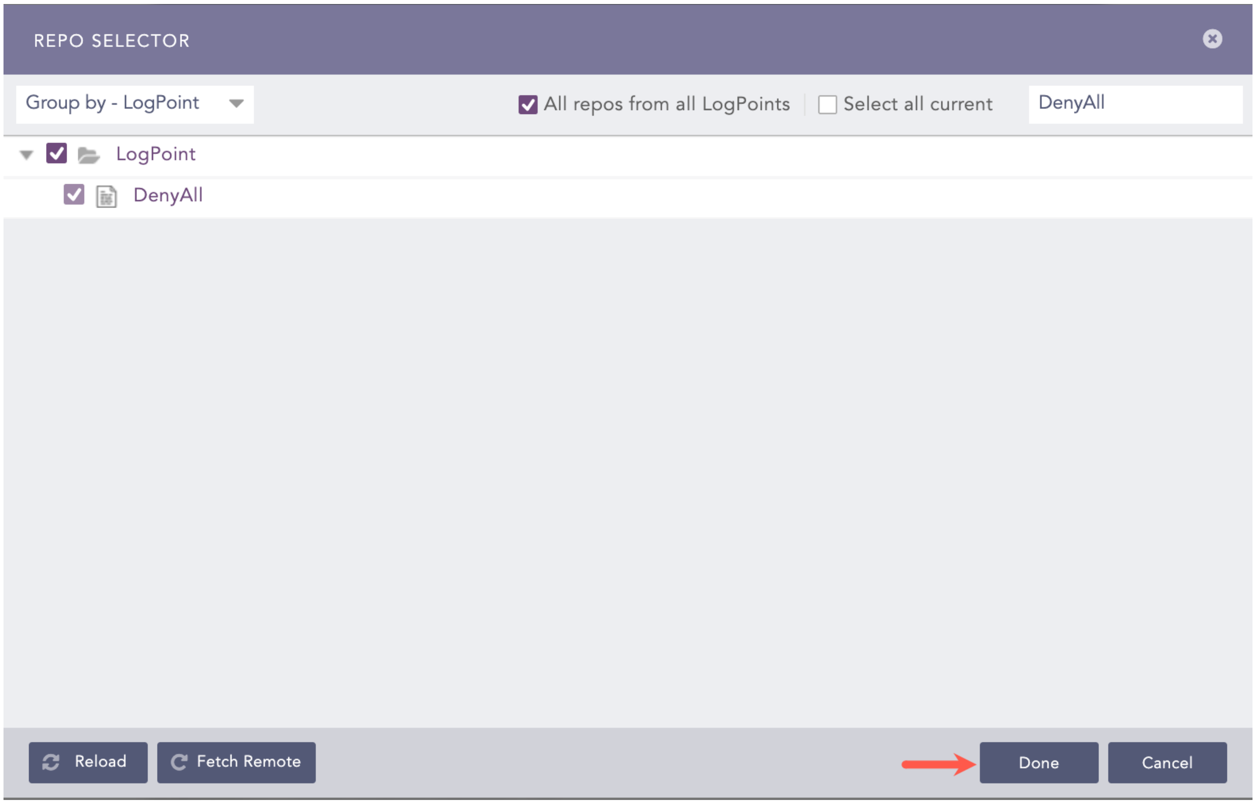


□	S.N.	Dashboard	Repos
☑	1	LP_Deny All Web Application Firewall	

Note: Using all repos in all the widgets of all dashboards may hit on performance

Fig. 2: Selecting Repos

5. Select the repo and click **Done**.



Group by - LogPoint

☑ All repos from all LogPoints

□ Select all current

DenyAll

☑ LogPoint

☑ DenyAll

Fig. 3: Selecting Repos

6. Click **Ok**.

You can find the *LP_Deny All Web Application Firewall* dashboard under *Dashboard*.

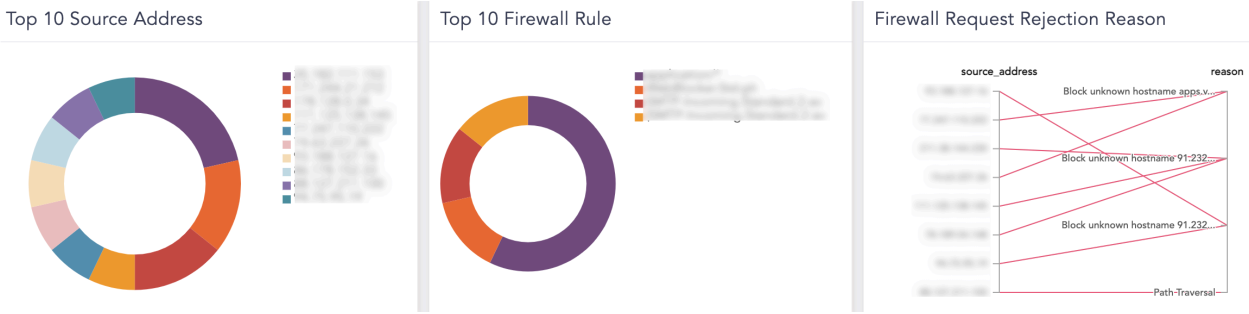

Top 10 Source Address
Top 10 Firewall Rule
Firewall Request Rejection Reason
source_address
reason
Block unknown hostname apps.v...
Block unknown hostname 91.232....
Block unknown hostname 91.232....
Path-Traversal

Fig. 4: Deny All WAF Dashboard

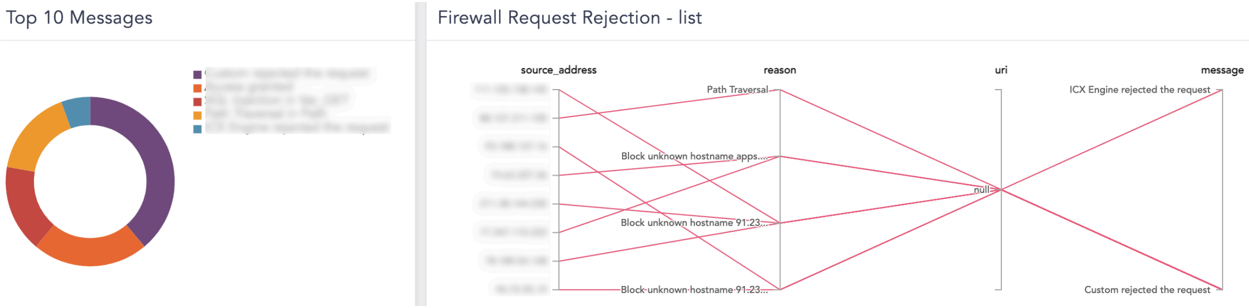

Top 10 Messages
Firewall Request Rejection - list
source_address
reason
uri
message
Path Traversal
Block unknown hostname apps....
Block unknown hostname 91:23....
Block-unknown-hostname-91:23...
null
ICX Engine rejected the request
Custom rejected the request

Fig. 5: Deny All WAF Dashboard

4.1.2 LP_Deny All Web Application Firewall Dashboard

Widgets available in the dashboard *LP_Deny All Web Application Firewall* provide:

Widget Name	Description
Top 10 Source Address	An overview of the top 10 source addresses detected by Deny All WAF.
Top 10 Firewall Rule	An overview of the top 10 firewall rules included in Deny All WAF.
Firewall Request Rejection Reason	An overview of the reasons for firewall requests rejection by Deny All WAF.
Firewall Request Rejection - list	An overview of the lists of reasons to reject firewall requests.
Top 10 Messages	An overview of the top 10 messages detected by Deny All WAF.
Top 10 Sources in SQL Injection Attack	An overview of the top 10 SQL Injection attack source addresses detected by Deny All WAF.
Top 10 Countries in SQL Injection Attack	An overview of the top 10 countries from where the SQL Injection Attack originated.

Continued on next page

Table 1 – continued from previous page

Widget Name	Description
SQL Injection Details	An overview of the SQL Injection attack details (sources, type of threats, country).

4.2 Deny All WAF Alerts

Alerts available in the *LP_Deny All WAF* are:

4.2.1 DenyAllWAF SQL Injection Attack

- **Trigger condition:** A SQL injection attack is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** DenyAll WAF
- **Query:**

```
norm_id=DenyAllWAF label=SQL label=Injection
```

CHAPTER

FIVE

SUPPORTED LOG SOURCES

5.1 Deny All WAF

Supported Version: DenyAll Web Application Firewall v6.x

CHAPTER

SIX

UNINSTALLING DENY ALL WAF

You must remove the **Deny All WAF** configurations to delete it.

1. Go to *Settings >> System Settings >> Applications*.
2. Click the **Uninstall** icon from **Actions**.
3. Click **Yes**.

CHAPTER

SEVEN

EXPECTED LOG SAMPLES

7.1 Deny All WAF

Shellcode

```
"<5>1 2020-01-07T09:17:08.732356+01:00 Management - - - - {"logAlertUid":
↪"bb45b96adbb6a6216981645d5","@timestamp":"1578385028731","timestamp":
↪"1578385028731","_type_":"Controller_Business_Log_SecurityLog","request":{"body":"",
↪"cookies":[],"headers":[{"key":"Host","value":"admin.logpointnp.np"},{"key":"User-Agent",
↪"value":"check_ssl_cert/1.76.0"},{"key":"Connection","value":"close"}],"hostname":"admin.
↪logpoint.np","ipDst":"10.20.69.101","ipSrc":"10.2.1.31","method":"HEAD","path":"/",
↪"portDst":443,"protocol":"HTTP/1.1","query":"","requestUid":
↪"XhQ@hL3oLmW@9nUuvpOS@AAM0"},"context":{"tags":"","applianceName":
↪"Management","applianceUid":"fefaab9235ab42dbb5c4","backendHost":"10.100.1.1",
↪"backendPort":443,"reverseProxyName":"LOG123","reverseProxyUid":
↪"aaaaaad1cba28f9564840e0f774","tunnelName":"CD84-V-zyx","tunnelUid":
↪"661985yyyyyde9402cb00bc72af","workflowName":"WAF xxx-V-PORTACRM","workflowUid":
↪"xxxxx3b35b4c60a766801d0"},"events":[{"eventUid":"74c816c3e280a53df9c203ba05","tokens
↪":{"date":15783850287320003,"eventType":"security","engineUid":"custom","engineName":
↪"Custom","attackFamily":"No Attack Family","riskLevel":50,"riskLevelOWASP":0.0,"cwe":"-",
↪"severity":5,"resolveType":"No Resolve","part":"No Part","customMessage":"URL non□
↪autorisee","reason":"Custom: URL non autorisee"}}]}"
```

```
"<5>1 2020-01-06T23:33:23.889229+01:00 Management - - - - {"logAlertUid":
↪"3820d6a0997f4444b5b6a3369b7053a3","@timestamp":"1578350003887","timestamp":
↪"1578350003887","_type_":"Controller_Business_Log_SecurityLog","request":{"body":"",
↪"cookies":[{"key":"PHPSESSID","value":"PHPSESSID=5g2r3dg3ka59f6vrvujb2mds53"}],
↪"headers":[{"key":"Accept-Encoding","value":"gzip,deflate"},{"key":"From","value":
↪"robot@seokicks.de"},{"key":"Connection","value":"Close"},{"key":"Referer","value":
↪"https://maps.vaucluse.fr/"},{"key":"Accept","value":"text/html,text/plain"},{"key":"Host",
↪"value":"maps.vaucluse.fr"},{"key":"User-Agent","value":"Mozilla/5.0 (compatible; SEOkicks;
↪ +https://www.seokicks.de/robot.html)"}],"hostname":"maps.vaucluse.fr","ipDst":"10.100.19.
↪46","ipSrc":"95.216.96.244","method":"GET","path":"/admin.php/auth/login/","portDst
↪":443,"protocol":"HTTP/1.1","query":"auth_url_return=%2Findex.php%2Fview%2F",
↪"requestUid":"XhO1s0rlt2PSlyBTRXMJ7AAAAWs"},"context":{"tags":"","applianceName""
```