HP Network Protector SDN Application - 1.3 Administrator Guide

Abstract

This guide provides information about the HP Network Protector SDN Application V1.3 administration procedures. This guide is intended for the person who installs and administers this software.

HP Part Number: 5998-7323a
Published: May 2015
Edition: 2

© Copyright 2014, 2015 Hewlett-Packard Development Company, L.P.
Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.
The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.
Links to third-party websites take you outside the HP website. HP has no control over and is not responsible for information outside HP.com.

Warranty

For the software end user license agreement and warranty information for HP Networking products, see http://www.hp.com/networking/support.

Contents

1 HP Network Protector Solution Overview....7
1.1 HP VAN SDN Controller....8
1.2 OpenFlow enabled switches....8
1.3 Service Insertion....9
1.4 Link aggregation....9
1.5 HP TippingPoint RepDV Cloud Service....9
1.6 ArcSight CEF Logger....10
1.7 HP Intelligent Management Center....10
2 Deployment examples....11
2.1 Instance approach to DNS inspection....11
2.2 Aggregate approach to DNS inspection....12
2.3 Fuzzy edge approach to DNS inspection....14
2.4 Edge routing approach to DNS inspection....15
2.5 DNS inspection at HTTP Proxy....16
2.6 MSM wireless deployment....17
2.7 Single switch connected through OOBM port....18
2.8 Stacked switch deployment....18
2.8.1 Stacked switches connected through OOBM port....19
2.8.2 Stacked switches connected through data ports....19
3 Licensing....20
3.1 Overview....20
3.2 Grace allowance....21
3.3 Using Evaluation Licenses....21
3.4 Obtaining product license keys....21
3.5 Registering and activating the HP Network Protector base license....21
3.5.1 Prerequisites....21
3.5.2 Registering an HP Network Protector base license....21
3.6 Registering and activating an HP Network Protector RepDV subscription license....24
3.7 Licensing compliance and alerts....25
3.8 Transferring licenses....25
3.8.1 Deactivating licenses to prepare for transfer....26
3.8.2 Transferring licenses....27
4 Understanding the application console....31
4.1 About the console....31
4.2 Initial configuration tasks....31
4.3 Logging into the console....32
4.4 Displaying the application user window....32
4.5 Adding a user....33
4.6 Verifying license compliance....33
4.7 Viewing alerts....33
4.8 Disabling the application....34
5 Configuring application components in the controller....35
5.1 Descriptions of the configurable components....35
5.1.1 Rule refresher....35
5.1.2 Tunnel heartbeat manager....35
5.1.3 Log config service....36
5.1.4 Service manager....36
5.1.5 Throttle manager....36
5.1.6 Transport manager....37

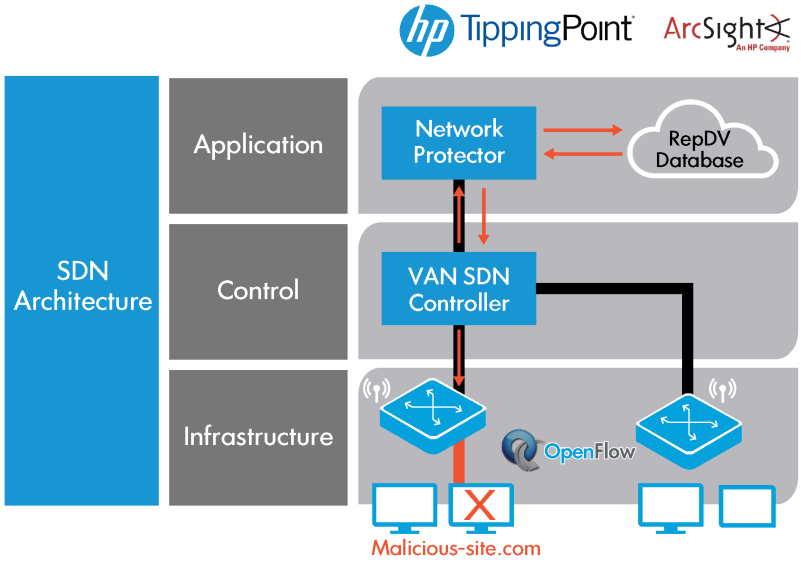
5.2 Accessing the configurable components....37
5.3 Configuring link aggregation....38
5.3.1 Configuring the switch NICs....38
5.3.2 Configuration the controller NICs....38
5.3.3 Verifying link aggregation status....39
5.4 Regulating DNS traffic to the application....40
5.4.1 Setting the DNS packet limit for switches....40
6 Working with Profiles....41
6.1 VLAN groups....41
6.1.1 Creating a new VLAN group....41
6.2 About custom lists....41
6.2.1 Whitelist....41
6.2.2 Adding entries to the whitelist....42
6.2.3 Priority whitelist....42
6.2.4 Blacklist....42
6.2.5 Greylist....42
6.2.6 Rules for creating whitelist and custom list entries....42
6.2.7 Creating priority whitelist, blacklist, or greylist....43
6.2.8 Loading the priority whitelist, blacklist, or greylist from external file....43
6.3 About RepDV Filters....43
6.3.1 Creating a new RepDV filter....44
6.4 About schedules....45
6.4.1 Creating a schedule....45
7 Setting Policies....46
7.1 About default policy....46
7.2 About threshold policies....46
7.2.1 Setting threshold policies....47
7.3 About priority whitelist policy....47
7.3.1 Creating a priority whitelist policy....47
7.4 About inspection policy....48
7.4.1 Creating an inspection policy....48
8 TippingPoint Reputation Digital Vaccine (RepDV) and ACL Manager....50
8.1 About the RepDV database....50
8.1.1 About the custom lists and RepDV search order....50
8.2 Searching for a domain name....50
8.2.1 Rules for a successful search....50
8.3 ACL Manager overview....51
8.3.1 Adding an ACL rule....51
8.3.2 Editing an ACL rule....51
9 Monitoring....53
9.1 HP Network Protector panels....53
9.1.1 System status panel....53
9.1.2 Device status panel....53
9.1.3 Checking VLAN status....54
9.1.4 VLAN status....55
9.1.5 Enabling and disabling a VLAN....56
9.2 Reports....57
9.2.1 Type of reports....57
9.2.2 Generating reports....57
9.3 Alerts....58
9.3.1 Refresh the Alert Listing....58
9.3.2 Changing the Display and Alert Listing Order....59
9.3.3 Acknowledge Alerts....59

9.4 Audit Log....59
9.4.1 Manage the Audit Log Display....60
9.4.2 Setting Audit Log policy....60
9.4.3 Archiving Audit Log Data outside of the HP Network Protector....60
9.5 Support Logs....60
9.5.1 Log Message Levels....61
9.5.2 Logs and log locations....61
9.5.3 Exporting the Support Logs....62
9.6 Viewing throttler statistics....63
9.7 About policy enforcement settings....63
9.7.1 Configuring the web server....63
9.7.2 Configuring policy enforcement settings....64
9.7.3 Time To Live (TTL) value....65
9.7.4 Adding hosts to the ACL....65
9.7.5 Adding hosts to the exception list....65
9.7.6 Deleting hosts from the exception list....65
9.8 Releasing quarantined clients....65
9.9 Exporting quarantined clients report....66
9.10 Notifications....66
9.10.1 Configuring email notifications....66
9.10.2 Configuring the HP ArcSight server....67
9.10.3 Configuring HP Intelligent Management Center....67
9.10.4 Generating license compliance report....67
9.10.5 Enable or disable Service Insertion globally....68
9.10.6 Enabling or disabling Service Insertion globally....68
9.10.7 Selecting the controller NIC....68
9.10.8 Enable or disable Service Insertion on a device....69
10 Backing up and restoring the application....71
10.1 Backup process....71
10.2 Restoring the application....71
10.3 Saving the application configuration settings....71
10.3.1 Prerequisites....71
10.3.2 Running the npConfig script....72
10.4 Restoring the application configuration settings....72
11 Troubleshooting the application....73
11.1 Basic troubleshooting techniques....73
11.2 Service Insertion tunnels are down....73
11.3 npwebserver process fails to start during installation....73
11.4 Application is not monitoring the DNS traffic....74
11.5 I can access a website even when it is on the blacklist....74
11.6 Disabling HP Network Protector SDN Application....75
11.7 Disabling the application for a specific VLAN or device....75
11.8 Troubleshooting user accounts....75
11.8.1 Cannot log on to the application....75
11.9 Troubleshooting licensing....76
11.9.1 Licensing numbers appear to be inaccurate....76
11.10 Troubleshooting RepDV database issues....76
11.11 Troubleshooting switch connection issues....78
11.11.1 Switch connection is not showing as registered in the HP VAN SDN Controller....78
11.11.2 Switching off V1 module in a mix of V1 and V2 modules on Provision OS....80
11.11.3 Gathering information from switches....80
12 Support and other resources....81
12.1 Gather information before contacting an authorized support representative....81

12.2 How to contact HP....81
12.3 Get connected to the HP SDN online user forum....81
12.4 Software technical support and software updates....81
12.4.1 Care Packs....82
12.4.2 Obtaining software updates....82
12.4.3 Warranty....82
12.5 Related information....82
13 Documentation feedback....83
Glossary....84
Index....85

1 HP Network Protector Solution Overview

HP Network Protector SDN Application

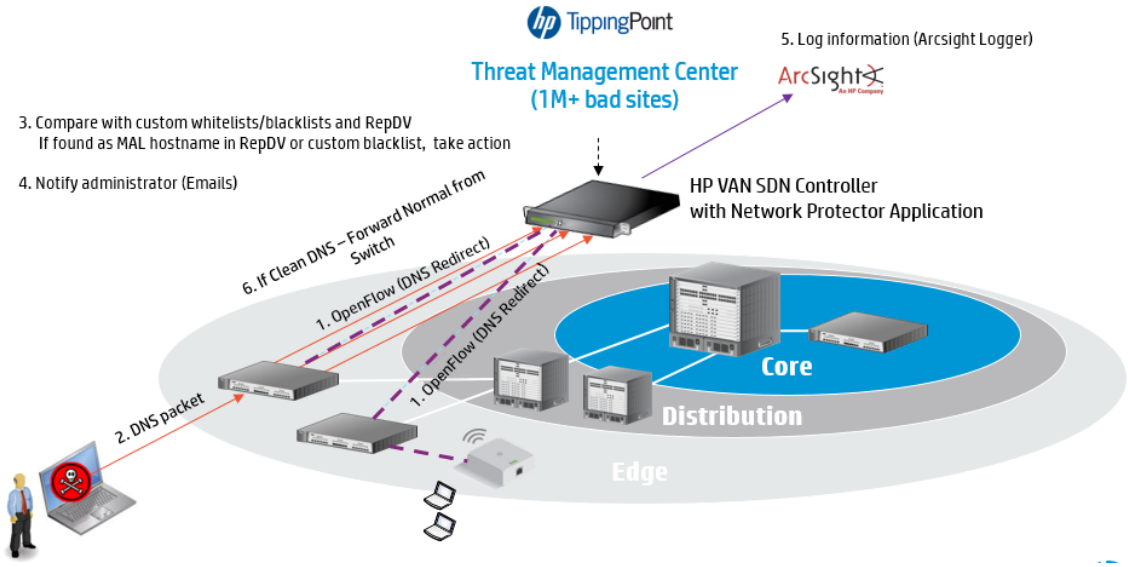


The HP Network Protector SDN Application leverages HP Networking, TippingPoint, and ArcSight products to deliver a converged solution that addresses security threats in a completely new way by leveraging the network itself. The HP Network Protector enables network intelligence on network infrastructure devices. The application uses the HP VAN SDN (Virtual Application Network Software-Defined Networking) Controller and OpenFlow to program the network infrastructure with security intelligence from the HP TippingPoint Reputation Digital Vaccine (RepDV). This turns the entire network infrastructure into security-enforcement devices, providing visibility and threat protection against more than one million malicious botnets, malware, and spyware sites.

Some of the key features of the solution include:

- Runs on HP VAN SDN Controller
- Complimentary to TippingPoint IPS solutions
- Delivers real-time threat characterization with HP TippingPoint DVLabs Database
- Protects from over 1,000,000+ botnet, malware, spyware, and malicious sites
- OpenFlow enabled switches gain ability to detect malware, botnets, and other threats
- Ability to create whitelist and blacklist
- Improves visibility and accuracy with Arcsight Integration
- Dynamic switch learning with HPN OpenFlow enabled switches distributes detection into switch infrastructure

Figure 1 High Level HP Network Protector Architecture



Click here to view a video of the HP Network Protector SDN Application overview.

1.1 HP VAN SDN Controller

The HP Network Protector is deployed as an application that runs on top of the HP VAN SDN Controller. As a stand-alone application bundled with the controller, it leverages several controller features and subsystems like Application Manager, Pipeline Manager, Licensing infrastructure, Cassandra Database, SKI UI framework, REST API framework, Audit, Alert, Support logs, and others.

For information about the controller, see the *HP VAN SDN Controller Administrator Guide* in the SDN information library at http://www.hp.com/go/sdn/infolib.

1.2 OpenFlow enabled switches

One of the basic requirements for the application is the OpenFlow enabled switches. OpenFlow is the mechanism by which the application instructs the discovered switches to redirect all DNS traffic towards itself. There are several security policies supported in the application, which are implemented by using the OpenFlow protocol to push desired flows on the switches. Currently, OpenFlow 1.0 and OpenFlow 1.3 versions are supported.

The switch firmware plays an important role in the proper functioning of the application. Provision switch firmware version 15.15 and above support an additional switch feature called *Service Insertion*, which helps send DNS data traffic to the switch using switch hardware, bypassing the switch CPU, thereby enhancing performance. Packet processing using the switch CPU is slower than the packet processing using switch hardware.

Switch capabilities and extensions or lack thereof have significant impact on how much actual packet processing needs to be handled by the application. The base level OpenFlow switch with no Service Insertion is the most rudimentary environment and all inspected traffic and control is shared on the OpenFlow interface port. Best performance is achieved with switches that support OpenFlow and Service Insertion.

The application scalability and performance also depends on the hardware and software specifications on the server on which it is deployed. For more information about the OpenFlow and switch configuration setting for OpenFlow, see the *HP OpenFlow 1.3 Administrator Guide* in the SDN information library.

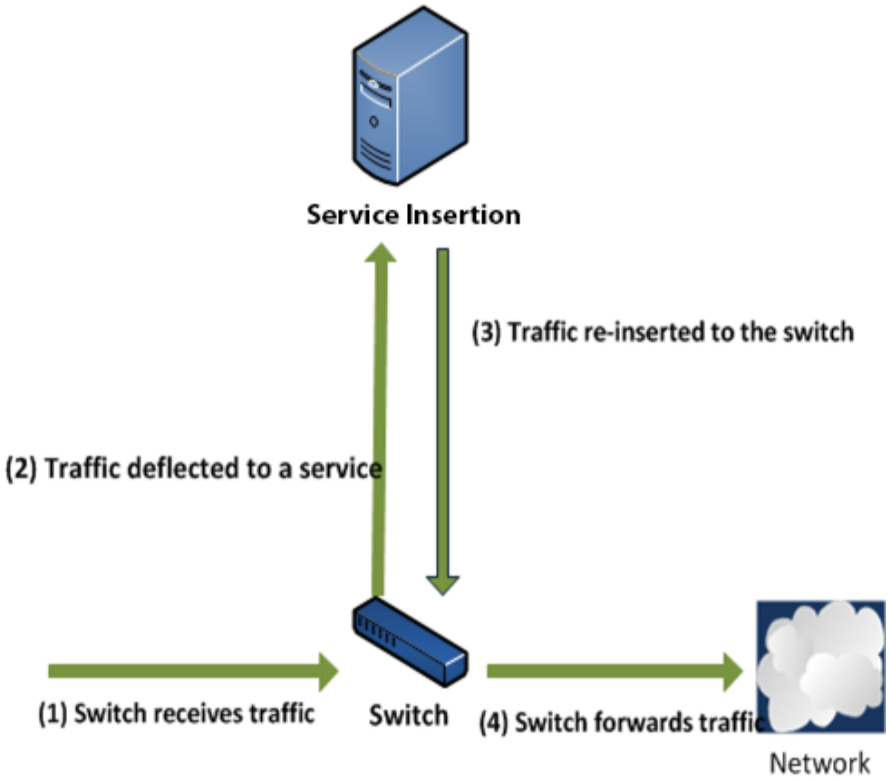
For more information about supported switch matrix information, see the *HP VAN SDN Controller and Applications Support Matrix* in the SDN information library.

1.3 Service Insertion

The application uses OpenFlow protocol to redirect DNS traffic from the switch to the application and compares it against TippingPoint RepDV to make forwarding or blocking decisions. However, packets of new flows need to be copied to switch CPU for processing and then redirected to the application, limiting performance in the range of tens of megabits per second. To maximize the performance and keep the switch to what it does best, packets switching, the switch hardware is used to pipe traffic directly to application, yielding potential performance improvement in the gigabits per second range or line rate. In other words, packets are forwarded by switch hardware instead by switch CPU through a Service Insertion tunnel. The desired best performance for application is achieved with switches that support OpenFlow and tunnel technology for Service Insertion.

For more information about Service Insertion, see the *HP Service Insertion Guide Wired Switches K/KA/WB 15.15* in the SDN information library.

Figure 2 Service insertion mechanism



1.4 Link aggregation

The application supports link aggregation, in which multiple links between the switches and the controller are combined to:

- Increase throughput beyond what a single connection can provide.
- Provide redundant connections to the controller in case of a single link failure.

To implement link aggregation, all the links must have the same bandwidth.

For more information

"Configuring link aggregation" (page 38)

1.5 HP TippingPoint RepDV Cloud Service

TippingPoint Reputation Digital Vaccine (RepDV) is a subscription service that enables organizations to monitor and block inbound and outbound communications with known malicious and undesirable

hosts. RepDV is a robust security intelligence feed powered by advanced analytics and a global reputation database of IPv4, IPv6, and DNS names.

The RepDV database includes more than a million known malicious or undesirable hosts collected from HP TippingPoint ThreatLinQ global intelligence network, DVLabs malware repository and honeypot network, third-party commercial sources, and open source blacklists. A threat score of 1 to 100 is assigned to each entry based on DVLabs analysis of the activity, source, category, and threat. Customers can tune RepDV policies based on reputation score, category, or geolocation to meet custom security requirements. RepDV is updated multiple times a day to stay ahead of emerging threats and reduce customers' security risk.

The application interfaces with the RepDV Cloud service to download the RepDV database and update its local copy of the same. This database forms the basis of DNS hostname comparisons after being filtered based on policies defined within the application. The application polls for updates every two hours (adjustable from the GUI) from the service to keep itself updated of new threats.

1.6 ArcSight CEF Logger

ArcSight is the universal log management solution to unify logs across the IT to collect, store, and search. HP ArcSight Logger can improve compliance, risk management, security intelligence, IT operations, and efforts that prevent insider and advanced persistent threats. This universal log management solution collects machine data from any log-generating source and unifies the data for searching, indexing, reporting, analysis, and retention. And in the age of BYOD and mobility, it enables comprehensive management of increasing volume of log data from an increasing number of sources.

The HP Network Protector supports ArcSight CEF syslog output so events can be sent directly to ArcSight Logger for enterprise visibility. ArcSight CEF is compatible with many generic syslog servers and supports all standard syslog servers.

1.7 HP Intelligent Management Center

The HP Network Protector exposes REST interface which IMC can use to get information about the policies and statistics. The application can also use IMC UAM module's REST API for getting the end user correlation using the IP and MAC address of the end point as collected from the DNS packets received in the application.

2 Deployment examples

This chapter contains a few approaches to deploy HP Network Protector that were implemented during the development, testing, and deployment phases. Use this section to understand certain important aspects before deploying the application in your network.

NOTE: You cannot deploy the application on a HP VAN SDN Controller teamed installation.

2.1 Instance approach to DNS inspection

Instance mode allows production (non-OpenFlow) VLANs and VLANs that belong to OpenFlow instances to be configured on the switch. Each OpenFlow instance is independent and has its own OpenFlow configuration and OpenFlow controller connection. An OpenFlow instance must have a VLAN associated as a member VLAN. This example uses a simpler configuration than other examples.

Figure 3 (page 12) illustrates this example.

In this example:

- Each edge device, such as an HP 2920 switch or an HP 3800 series switch, is connected to the HP VAN SDN Controller and is configured to use OpenFlow.
- The L2 aggregation switch, such as an HP 5406 switch, is not configured to use OpenFlow and is not connected to the controller in this example.
- The application performs inspection and control on VLAN 20 and VLAN 30 but not on VLAN 10 or 40.
- Every VLAN on every device has an OpenFlow instance.
- DNS inspection is automatic when endpoints are browsing because of the transparent proxy configuration at the firewall. In a transparent proxy deployment, HTTP requests are automatically directed to a Proxy server without requiring manual browser configuration.
- There is no wireless controller. Traffic is inspected when it arrives on VLAN 20.

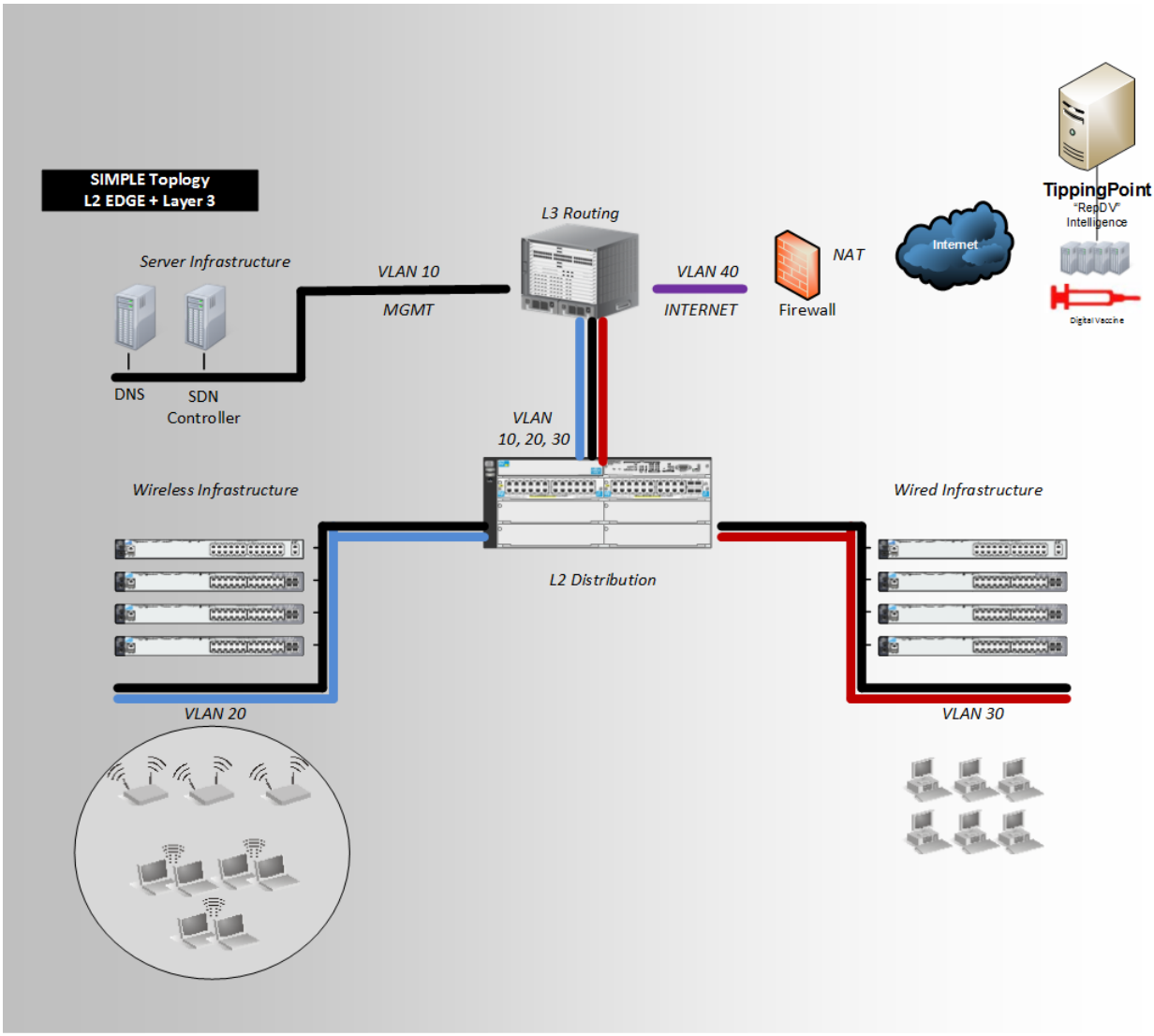
Example configuration file to use OpenFlow 1.3 in instance mode.

```
controller-id 8 ip 15.146.194.104 controller-interface vlan
1
instance "office13"
member vlan 4
controller-id 8
version 1.3 only
mode passive
enable
exit
```

Example configuration file to use OpenFlow 1.0 in instance mode.

```
controller-id 8 ip 15.146.194.104 controller-interface vlan
1
instance "office10"
member vlan 4
controller-id 8
mode passive
enable
exit
```

Figure 3 DNS inspection using an instance approach



2.2 Aggregate approach to DNS inspection

In Aggregation mode, all VLANs in the switch are part of an OpenFlow instance. The exception is the management VLAN and a VLAN that communicates to the controller. Similar to a lab environment the OpenFlow controller manages all the switching and routing for the switch. This example shows the aggregate mode configuration on the EDGE switches. This example has similar advantages and disadvantages as the instance approach (see "Instance approach to DNS inspection" (page 11)), but does not require you to configure as many OpenFlow instances.

Figure 4 (page 14) illustrates this example.

In this example:

- Each edge device, such as an HP 2920 switch or an HP 3800 series switch, is connected to the HP VAN SDN Controller and is configured to use OpenFlow.
- The L2 aggregation switch, such as an HP 5406 switch, is not configured to use OpenFlow and is not connected to the HP VAN SDN Controller.
- The application performs inspection and control on VLAN 20, 30, 40, 50, 60, and 70.

- Each device has a single OpenFlow instance that is configured to include all VLANs except the controller VLAN.
- DNS inspection is automatic when endpoints are browsing because the transparent proxy deployment is used. In a transparent proxy deployment, HTTP requests are automatically directed to a Proxy server without requiring manual browser configuration.

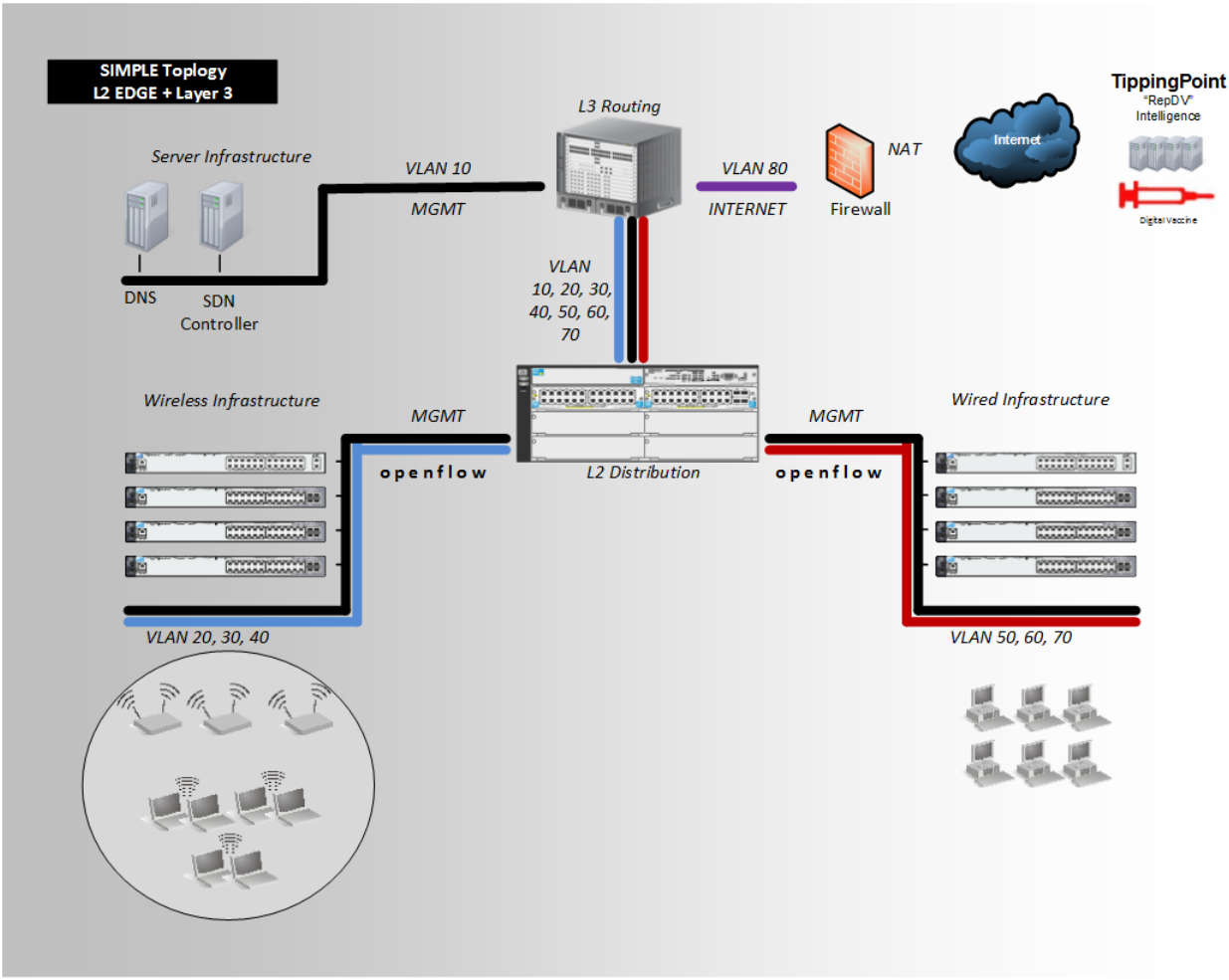
Example configuration file to use OpenFlow 1.3 in aggregate mode.

```
controller-id 8 ip 15.146.194.104 controller-interface vlan
1
instance aggregate
controller-id 8
version 1.3 only
mode passive
enable
exit
```

Example configuration file to use OpenFlow 1.0 in aggregate mode.

```
controller-id 8 ip 15.146.194.104 controller-interface vlan
1
instance aggregate
controller-id 8
mode passive
enable
exit
```

Figure 4 DNS inspection using an aggregate approach



2.3 Fuzzy edge approach to DNS inspection

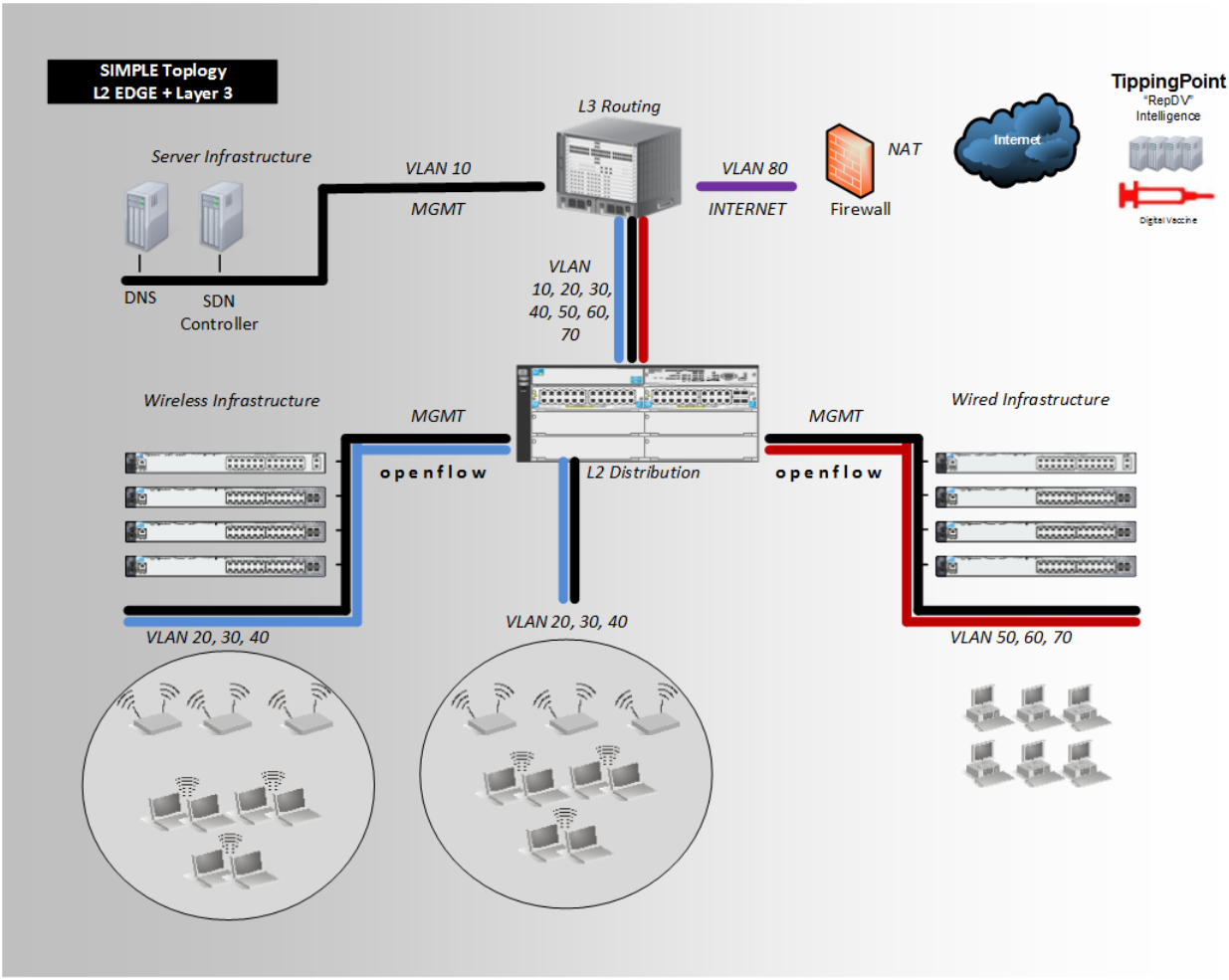
In the fuzzy edge approach, the endpoints are connected to the edge switches but there are also endpoints connected to the distribution switch. In this example, you choose to inspect DNS requests at the distribution switch in addition to the edge switches. Using this approach allows specify which VLANs you want the application to inspect.

Figure 5 (page 15) illustrates this example.

In this example:

- Each edge device, such as an HP 2920 switch or an HP 3800 series switch, is connected to the HP VAN SDN Controller and configured to use OpenFlow.
- The L2 distribution switch, such as an HP 5406 switch, is also connected to the controller and configured to use OpenFlow.
- The application performs inspection and control on VLAN 20, 30, 40, 50, 60, and 70.
- Each device has a single OpenFlow instance that is configured to include all VLANs except the controller VLAN.
- DNS packets are inspected both at the edge and at the point of aggregation for VLANs 20, 30, and 40.
- DNS inspection is automatic when endpoints are browsing because the transparent proxy deployment is used. In a transparent proxy deployment, HTTP requests are automatically directed to a Proxy server without requiring manual browser configuration.

Figure 5 DNS inspection using a "fuzzy edge" approach



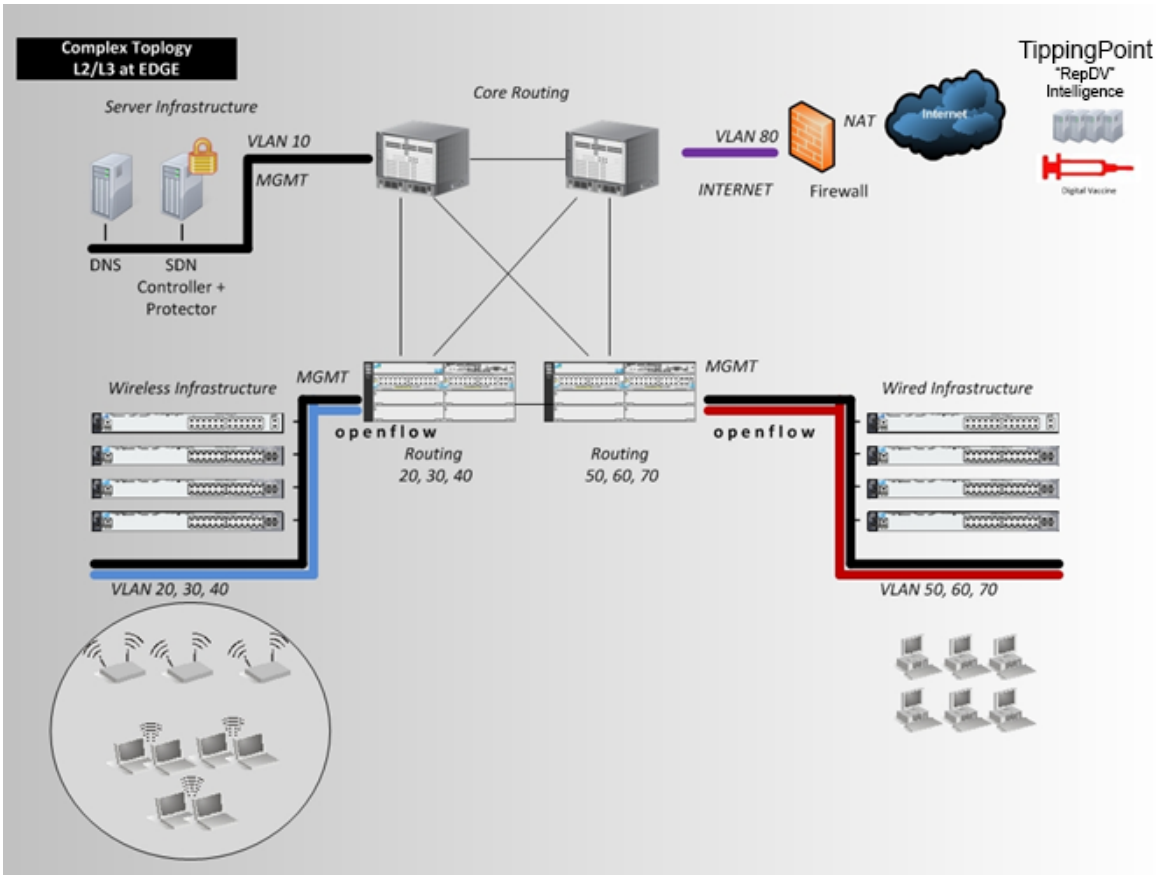
2.4 Edge routing approach to DNS inspection

In this example, you configure the solution to perform DNS inspection at the edge routers. Figure 6 (page 16) illustrates this example.

In this example:

- Each edge router, such as an HP 5406 switch, is connected to the HP VAN SDN Controller, is configured to use OpenFlow, and is routing packets.
- The application performs inspection and control on VLAN 20, 30, 40, 50, 60, and 70.
- An OpenFlow packet out operation is not supported for the routers in this configuration.
- If you want inspection to occur on a device that is routing, that device must support Service Insertion.
- DNS inspection is automatic when endpoints are browsing because the transparent proxy deployment is used. In a transparent proxy deployment, HTTP requests are automatically directed to a Proxy server without requiring manual browser configuration.

Figure 6 DNS inspection at edge routers



2.5 DNS inspection at HTTP Proxy

In this example, HTTP request for hostname **`example.com`** reaches the HTTP Proxy server. This request is an HTTP GET (TCP) instead of DNS UDP (UDP) request and therefore the application does not inspect the request.

The HTTP proxy can be deployed in two ways:

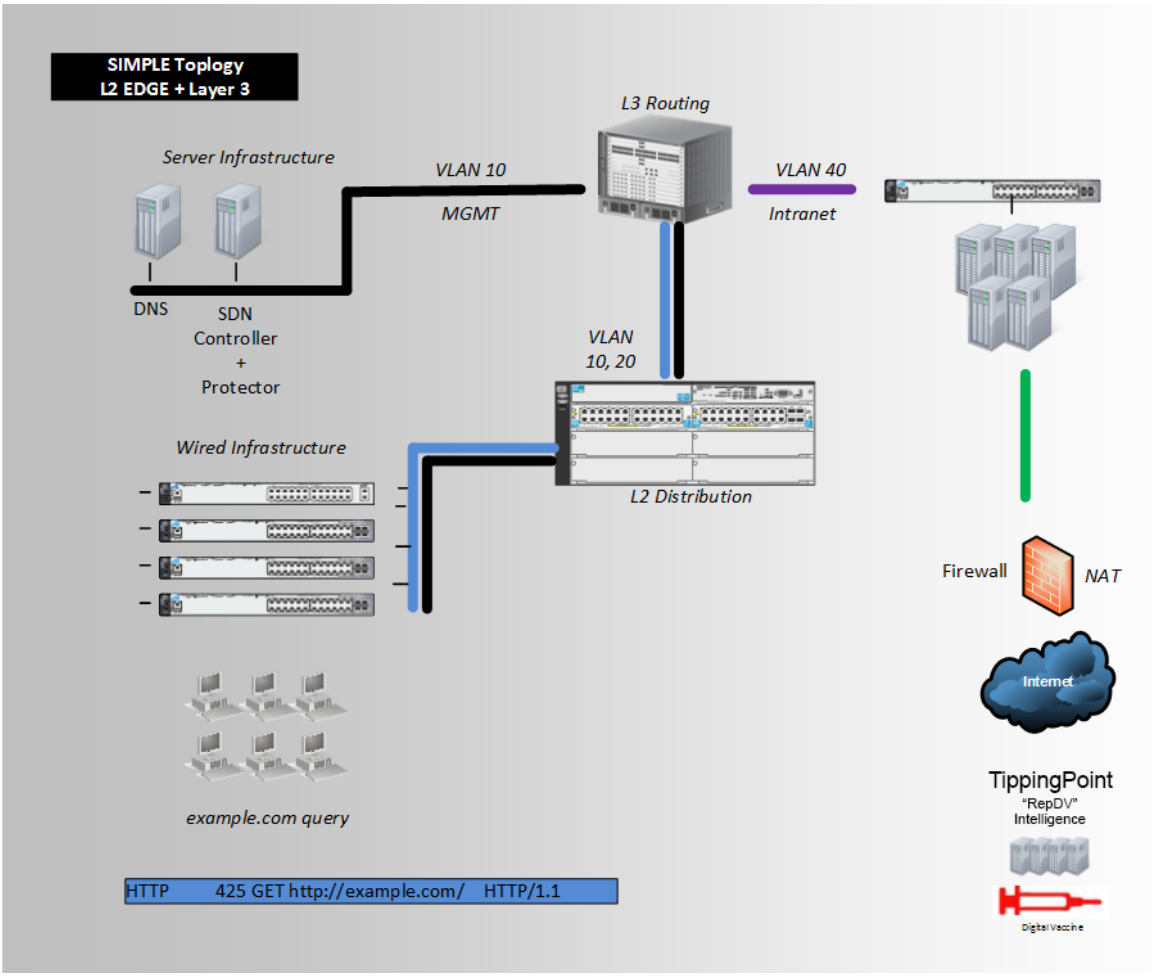
- **Explicit proxy deployment**. In this deployment the browser is explicitly configured to send HTTP requests directly to a proxy server.
- **Transparent proxy deployment**. In this deployment the HTTP requests are directed through a proxy server without any manual browser configuration.

In the case of transparent proxy deployment, the HTTP request results in a DNS request, and therefore the application always inspects the requests. But, in case of explicit proxy deployment, with DNS caching options, every HTTP request does not necessarily result in a DNS request sent to the DNS server, thereby bypassing the application.

You can however ensure the DNS lookups happen, in which case inspection could occur with VLAN 40 shown in figure. For cases where you want to ensure the DNS request is generated, a PAC (Proxy Auto Config) file can be configured to work with the proxy server. The PAC file, for example proxy.pac, can be configured to direct end clients to behave as follows:

1. Set proxy.pac to direct client to send DNS request. If DNS request returns valid, then proceed to send HTTP GET request to web proxy.
2. If DNS address comes back with redirect to a specific IP of a remediation site, set proxy.pac to query for direct query site.

Figure 7 HTTP proxy configuration



For more information about how to configure the Proxy Access Control (PAC) file to direct the HTTP requests from the web browsers to the DNS server, see "I can access a website even when it is on the blacklist" (page 74)

2.6 MSM wireless deployment

This example shows an MSM (MultiService Mobility Controller) wireless deployment comprising of Non-Access Controlled Virtual Service Communities (VSCs) and Mobility Traffic Manager (MTM) with the application. The MTM feature provides for seamless roaming of wireless users, while at the same time giving the administrator the complete control over how wireless user traffic is distributed onto the wired networking infrastructure.

In this example:

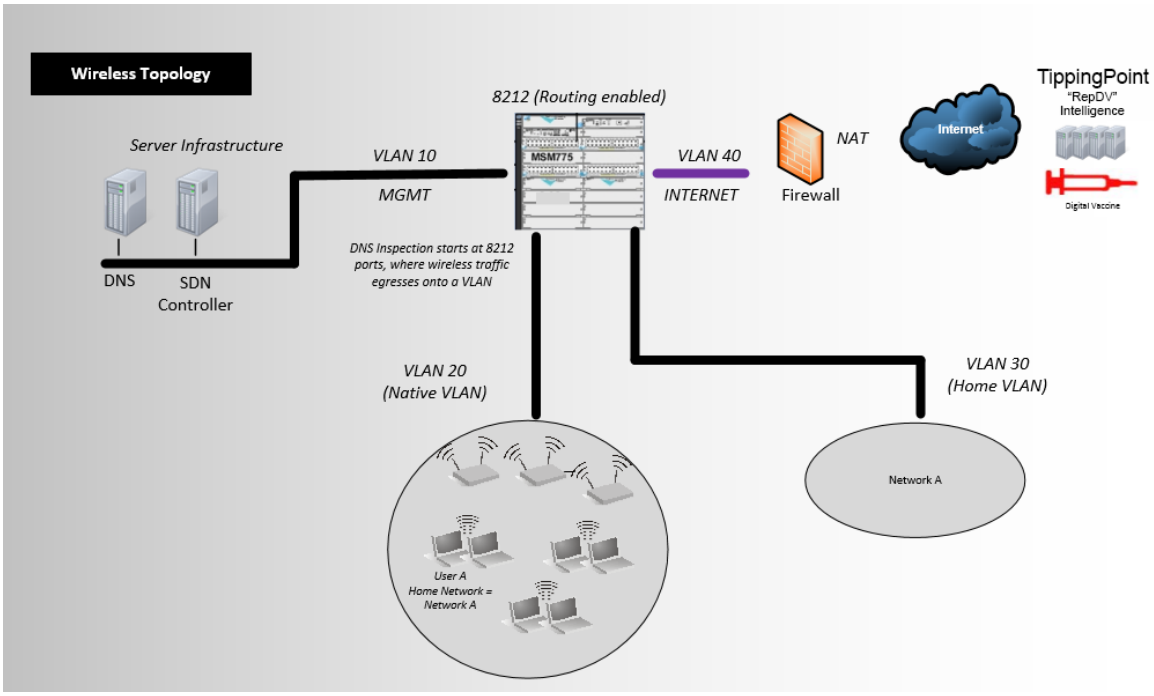
- If the DNS Intercept feature is turned off, inspection by the application can occur anywhere the wireless traffic egresses onto a VLAN, including:
  - Non-access-controlled VSCs (virtual service communities)
  - Mobility Traffic Manager (MTM)

  When MTM is used, inspection can occur on either home or native VLANs.
- The block and quarantine actions of the application are based on the MAC address and IP address of the source as received by the application.

- Service Insertion is required in situations where the egress VLAN is inspected and the device is routing. This situation is depicted in Figure 8 (page 18) with the Core 8212 switch.
  - DNS inspection is occurring on the 8212 device and redirected out to the SDN Controller.
  - Pure OpenFlow configuration on 8212 will not work in this scenario as packet-out normal cannot be performed by the 8212 switch when it is routing.
  - In this scenario, Service Insertion configuration on 8212 and MTM will work with all supported application features.
- Configurations in which the application cannot inspect the original source MAC and IP address are not supported. This restriction includes access-controlled VSCs.

Figure 8 (page 18) illustrates this example.

Figure 8 MSM wireless deployment



2.7 Single switch connected through OOBM port

You can configure the OOBM port on a single switch to provision DNS traffic between the controller and the switch. You can connect the Pro-visions switch series such as HP 3800, HP 2920, and HP 5400R and the controller via the OOBM port. Service Insertion tunnels are not supported on OOBM ports even though the switch by itself is supporting Service Insertion tunnels. When you connect the switch and the controller through the OOBM port, you are providing separate paths for management traffic and data traffic. The OOBM port can be used to handle only management traffic instead of using a data port for both management and data DNS traffic.

2.8 Stacked switch deployment

Pro-visions switch series such as HP 3800 and HP 2920 support stacking. Stacking of switches consists of 3, 5, or 7 switches stacked together. After the switches are stacked, the switches are automatically synced to have the same configuration and firmware as of the master switch. The stacked switches can be managed under a single IP address through either OOBM port or the Data port. DNS traffic between the application and switch is through one of the ports.

2.8.1 Stacked switches connected through OOBM port

The stacked switches connected to the controller through the OOBM port work similar to the stand-alone switches connected through OOBM port. For stacked switches connected through OOBM port, the DNS traffic between the application and switch is through Openflow channel. Service Insertion is not supported on OOBM ports, even if the switch supports Service Insertion on 1G/10G NICs on HP 3800 switch with KA.15.15 firmware version. Service Insertion tunnels are not created and the application provisions OpenFlow channel for the stacked device's datapaths.

OOBM redirection occurs when one of the OOBM ports in the management module of the switch is down then the OOBM port in another management module within the same chassis handles all the incoming traffic. OOBM redirection is supported on HP 5412R switch and is not supported on HP 3800 switch series.

NOTE: For switches connected through OOBM ports, OpenFlow is the best possible mode and the device health status will be **Green** in the application.

2.8.2 Stacked switches connected through data ports

When the stacked switches and the controller are connected through a data port, then the DNS traffic between the application and switch is provisioned through Service Insertion tunnels. The stacked switches and its firmware must support Service Insertion to connect through data port. When one Service Insertion tunnel is created between the controller and the stacked devices (usually between master switch and controller), then all the switches use the same tunnel to communicate with the controller. HP 5400R zl2 Switch Series support Service Insertion during stacked mode.

Example 1 Managing stacked switches through data port

Configure a group of 3 switches is a stacked mode. Configure one data port from each switch as a LACP (Link Aggregation Control Protocol) trunk. The LACP trunk is used to connect the stacked switches with the controller. Service Insertion tunnel is created between the stacked switches and the controller. All the datapaths are provisioned through the Service Insertion tunnel.

3 Licensing

3.1 Overview

The HP Network Protector uses electronic licenses. Each electronic license is an SKU (Storage Keeping Unit) on the HP CPL (Corporate Price List) that you can purchase from HP through resellers. You can purchase electronic licenses at different times and from different resellers. You must have the HP VAN SDN Controller licenses installed before you can install the HP Network Protector licenses.

The following table lists the license SKUs for the application:

Table 1 License SKUs

Product number	Product description	Validity
JL004AAE	HP Network Protector SDN Application 250 Concurrent Users E-LTU	Perpetual
JL005AAE	HP Network Protector RepDV Subscription 250 Concurrent Users 1 Year E-LTU	1 year
JL006AAE	HP Network Protector RepDV Subscription 1000 Concurrent Users 1 Year E-LTU	1 year
JL007AAE	HP Network Protector RepDV Subscription 2000 Concurrent Users 1 Year E-LTU	1 year
JL008AAE	HP Network Protector RepDV Subscription 4000 Concurrent Users 1 Year E-LTU	1 year
JL092AAE	HP Network Protector RepDV Subscription 8000 Concurrent Users 1 Year E-LTU	1 year
JL093AAE	HP Network Protector RepDV Subscription 20,000 Concurrent Users 1 Year E-LTU	1 year
JL094AAE	HP Network Protector RepDV Subscription 40,000 Concurrent Users 1 Year E-LTU	1 year

The application electronic licenses are of two types:

- **HP Net Protector SDN App 250 User E-LTU**

JL004AAE HP Net Protector SDN App 250 User E-LTU is an HP Network Protector base license. The application base license that you purchase never expires. You need to purchase at least one application base license. The number of base licenses you need is determined by the maximum number of concurrent users using the application in an active session. The duration of each active session is 15 minutes.

For example, if you buy four 250–user HP Network Protector SDN Application base licenses, the maximum number of users with the application in an active session is 1,000 (4×250).

NOTE: The HP Network Protector SDN Application user is a unique pair of a MAC and an IP address.

- **HP Net Protector RepDV subscription license**

Use the HP Net Protector RepDV licenses to subscribe to the RepDV database. The HP Network Protector RepDV subscription licenses expire after a period of one year. There are four HP Network Protector RepDV subscription licenses, which cater to 250, 1,000, 2,000, and 4,000 users. The HP Network Protector RepDV subscription license you need is determined by the number of users using the application base licenses.

For example, if you buy four 250–user HP Network Protector base licenses (1,000 users), then you purchase the HP Network Protector RepDV subscription licenses for 1,000 or more than 1,000 users.

If you do not buy HP Network Protector RepDV subscription license, you can use the application with your own custom lists such as blacklist or whitelist entries. However, you will not be able to access the TippingPoint RepDV database. If you do not renew your HP Network Protector RepDV subscription licenses after expiry, you can access the RepDV database, but you will not receive the RepDV updates from the TippingPoint server.

During the course of the RepDV subscription, users can access RepDV subscription license count greater than the HP Network Protector base license count. After the RepDV subscription expires, a higher RepDV license subscription is required to match the base license count.

3.2 Grace allowance

The HP Network Protector controls the number of users by licenses and provides a grace allowance for the application users. There is no grace time allowance for the HP Network Protector RepDV subscription licenses.

3.3 Using Evaluation Licenses

You can use the evaluation license to install HP Network Protector and use and evaluate the product. If you are using the AppStore, install the Trial Mode SDN applications.

1. Install the application.
2. Log on to **My Networking Portal** (MPN) at http://hp.com/networking/mynetworking and select SDN Evaluation Licenses.
3. Enter your install-id.
4. MNP generates evaluation license for that install id.
5. Apply the relevant licenses to the application.

3.4 Obtaining product license keys

You can obtain your product license keys from MNP (**My Networking** portal). After purchasing the HP Network Protector electronic licenses, you can register them on MNP by using the HP VAN SDN Controller Install ID and obtain the application product license keys. You can use MNP to transfer the application licenses from one machine to another.

3.5 Registering and activating the HP Network Protector base license

3.5.1 Prerequisites

To register an HP Network Protector base license from MNP, you must already have an HP VAN SDN Controller base license registered and activated (in Table 2 (page 21) below, **J9863AAE**). For information about registering and activating a license for the HP VAN SDN Controller, see the *HP VAN SDN Controller Administrator Guide* in the SDN information library.

Table 2 (page 21) below presents information on the application prerequisite license.

Table 2 Prerequisite license details

Product number	Product description	Prerequisite product number	Prerequisite product description
JL004AAE	HP Net Protector SDN App 250 User E-LTU	J9863AAE	HP VAN SDN Ctrl Base SW w/50–node E-LTU

3.5.2 Registering an HP Network Protector base license

To register an HP Network Protector base license and obtain a license key:

1. Log on to **My Networking** portal at http://hp.com/networking/mynetworking.
2. Select **My Licenses**.

   The Register license screen appears, as shown in Figure 9 (page 22).

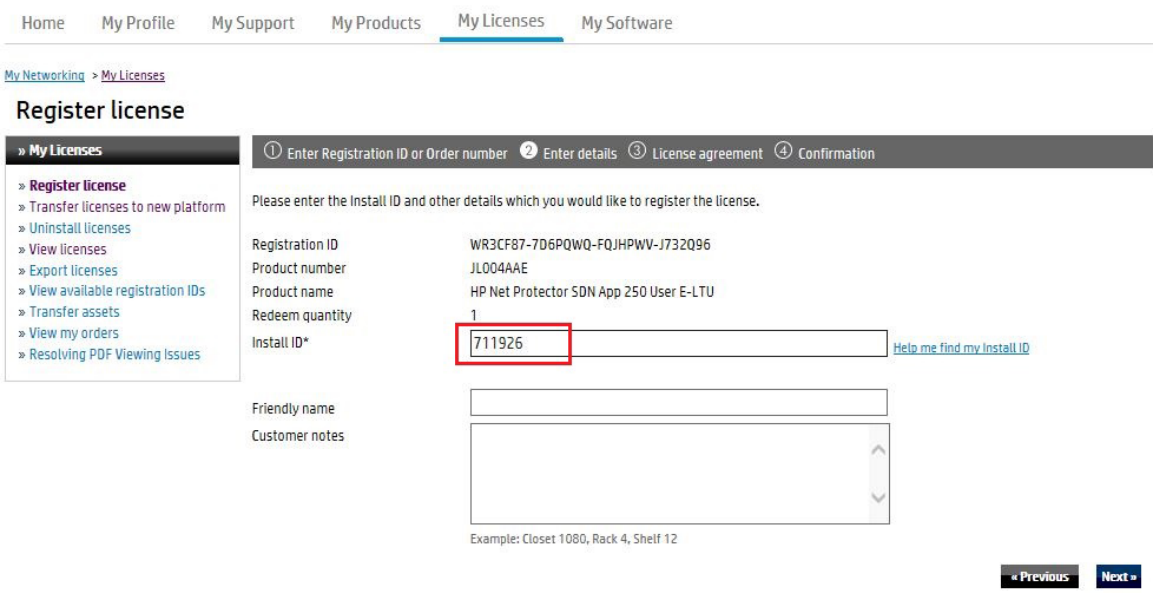
Figure 9 Entering order number or registration ID



3. Enter your application base license order number or registration ID in the field provided, and then click **Next**.

   The registration details screen appears, as shown in Figure 10 (page 22).

Figure 10 Entering the Install ID

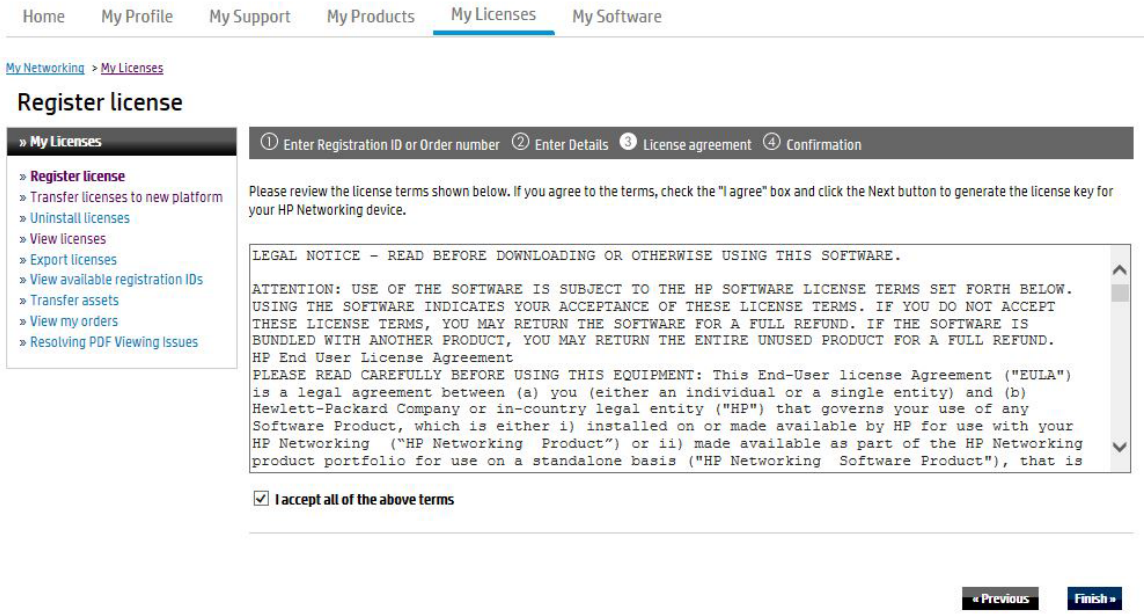


4. In the **Install ID** field, enter your HP VAN SDN Controller Install ID number.

   You can find the Install ID on the HP VAN SDN Controller under **General→Licenses**.
5. Optional: Enter a **Friendly name** and **Customer notes** for this license.
6. Click **Next**.

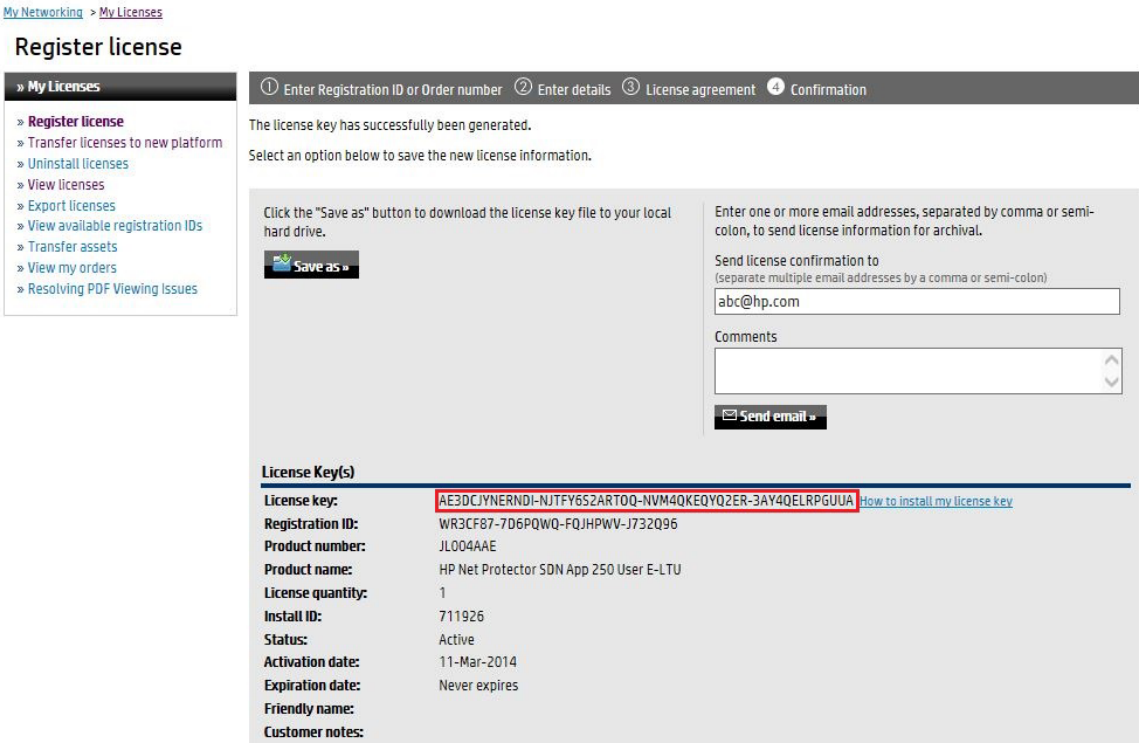
   The end user software license agreement screen appears, as shown in Figure 11 (page 23).

Figure 11 Accepting the license agreement



7. Select **I accept all of the above terms**, and then click **Finish**.
   The confirmation screen appears, as shown in Figure 12 (page 23).

Figure 12 Reviewing your registration



8. Review your license registration details, and record the **License key** listed.
9. Optional: To download the license key file, click **Save as**, and then save it to your local hard drive.

10. Optional: To e-mail the registration details:
    a. Enter one or more email addresses, separated by a comma or semicolon in the field provided.
    b. Optional: Enter **Comments** about this license.
    c. Click **Send email**.
11. Optional: If you want to register additional HP Network Protector base licenses:
    a. Click **Register more for this order**.
    b. Repeat steps 4 through 11 until you have registered all the application base licenses.

3.6 Registering and activating an HP Network Protector RepDV subscription license

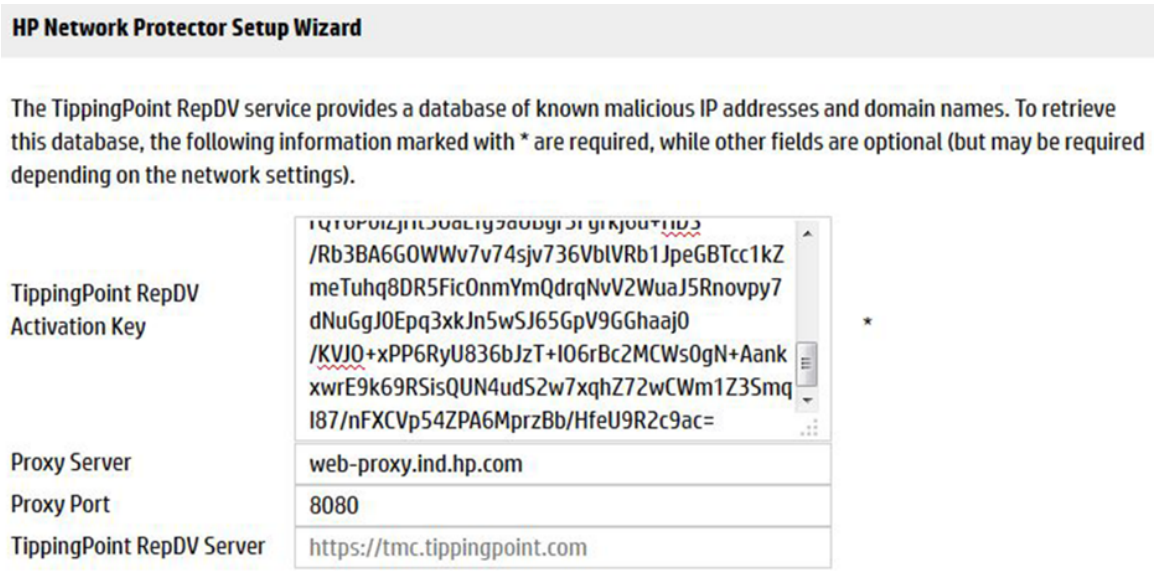
Before registering the HP Network Protector RepDV subscription license, ensure that you have registered and activated the HP Network Protector base license.

1. Register the HP Network Protector RepDV subscription license you purchased on the **My Networking** portal and obtain the RepDV activation key.
2. Install the RepDV activation key on the application. To install the RepDV activation key:
    a. Log into the HP Network Protector.

       The **Network Protector Login Console** appears when you are logging into the application for the first time.

    b. Enter the user name and password and click **Login**.
    c. On successful login, the **Network Protector Setup Wizard** appears. Click **Next**.
    d. Enter the RepDV activation key and other details, as shown in Figure 13 (page 24). Click **Next**.

Figure 13 Adding RepDV activation key

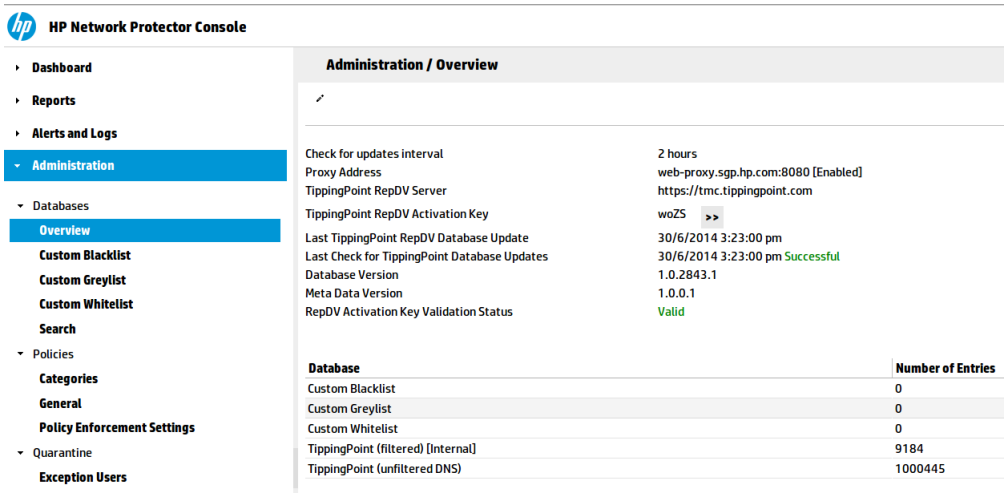


    e. Enter the SNMP credentials and click **Finish**.

3. To verify whether the activation of the HP Network Protector RepDV subscription license is successful:
   a. On the application UI, navigate to **Administration**+**Databases**→**Overview**.
   b. Press **F5** to refresh the page.

   If the license is successfully activated, the **RepDV Activation Key Validation Status** is **Valid**. See Figure 14 (page 25).

Figure 14 RepDV Activation Key Validation Status



NOTE: After you enter the RepDV activation key, the application connects to the TippingPoint database and verifies the RepDV status. However, after entering the RepDV activation key for the first time, it takes some time for the application to connect to the TippingPoint database and download the entire database.

4. You can modify your RepDV activation key settings on the application UI. For more information, see "Initial configuration tasks" (page 31).

IMPORTANT: When upgrading the HP Network Protector RepDV license, register the new HP Network Protector RepDV license on MNP, and install it on the application after about 15 minutes. After registering the new license on MNP, the old RepDV license is deactivated. Therefore, you must wait for about 15 minutes before proceeding to install the new RepDV product license key on the application.

3.7 Licensing compliance and alerts

The HP Network Protector checks for licensing compliance at an interval of every 15 minutes. When licensing compliance requirements are violated, the application generates alerts and logs. It also send a mail notification to the administrator indicating a license violation has occurred and urges the administrator to verify the compliance reports. The mail is sent once in every 24 hours.

The application generates alerts, email notifications and logs when:

- The application base license is missing.
- The number of concurrent users in active sessions exceeds the grace license limits.

IMPORTANT: HP reserves the right to strictly enforce licensing compliance in future releases.

3.8 Transferring licenses

You can transfer your HP Network Protector license from one machine to another. To transfer, you must first deactivate your application and the controller base licenses on the HP VAN SDN

Controller. For transferring the HP Network Protector RepDV subscription license, deactivation is not required. You can transfer it directly.

IMPORTANT: To transfer the HP Network Protector licenses, you must transfer all the application licenses associated with the controller. Partial transfer of licenses is not permitted.

3.8.1 Deactivating licenses to prepare for transfer

Deactivate your HP Network Protector license only if you want to the transfer the license or uninstall the application. You will receive an uninstallation key when you deactivate the license. Note down the uninstallation key number for your records.

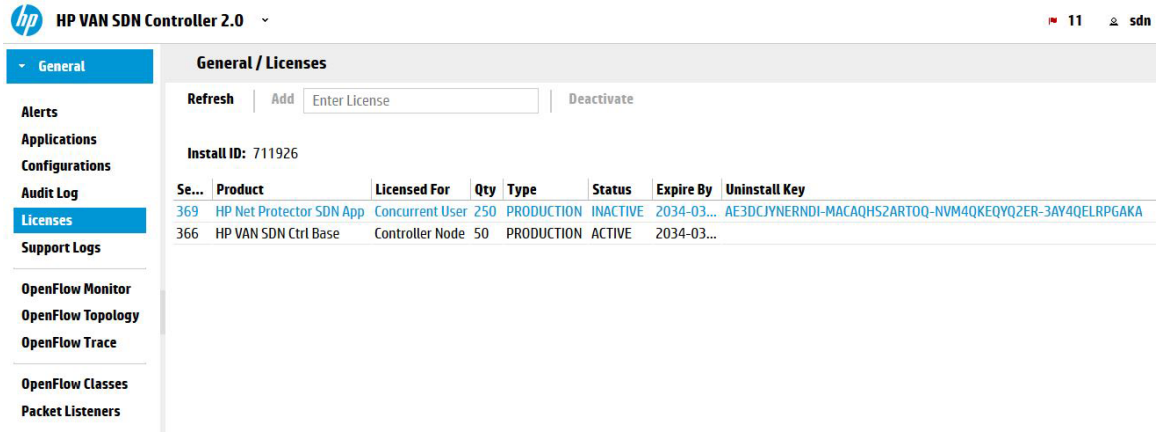
CAUTION: Do not deactivate your HP Network Protector license for any other reason.

To deactivate licenses to prepare for transfer:

1. Log into the HP VAN SDN Controller.
2. Navigate to **General→Licenses**.
3. First, select the HP Network Protector base license that you want to deactivate.
4. Click **Deactivate**.

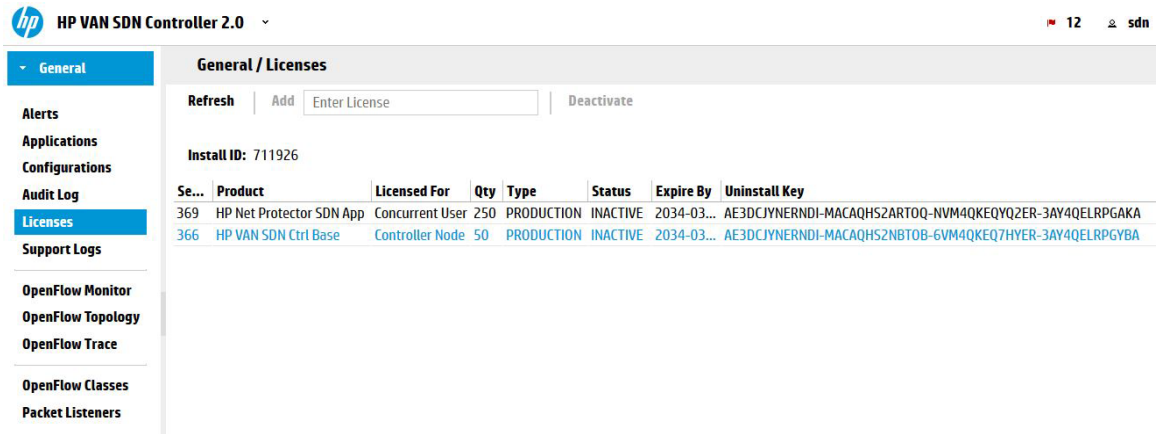
   An uninstallation key appears, note down the uninstallation key number. See Figure 15 (page 26).

Figure 15 HP Network Protector SDN Application base license deactivation



5. Next, select the HP VAN SDN Controller base license that you want to deactive.
6. Click **Deactivate**.
7. Note down the uninstallation key number. See Figure 16 (page 26).

Figure 16 HP VAN SDN Controller base license deactivation



3.8.2 Transferring licenses

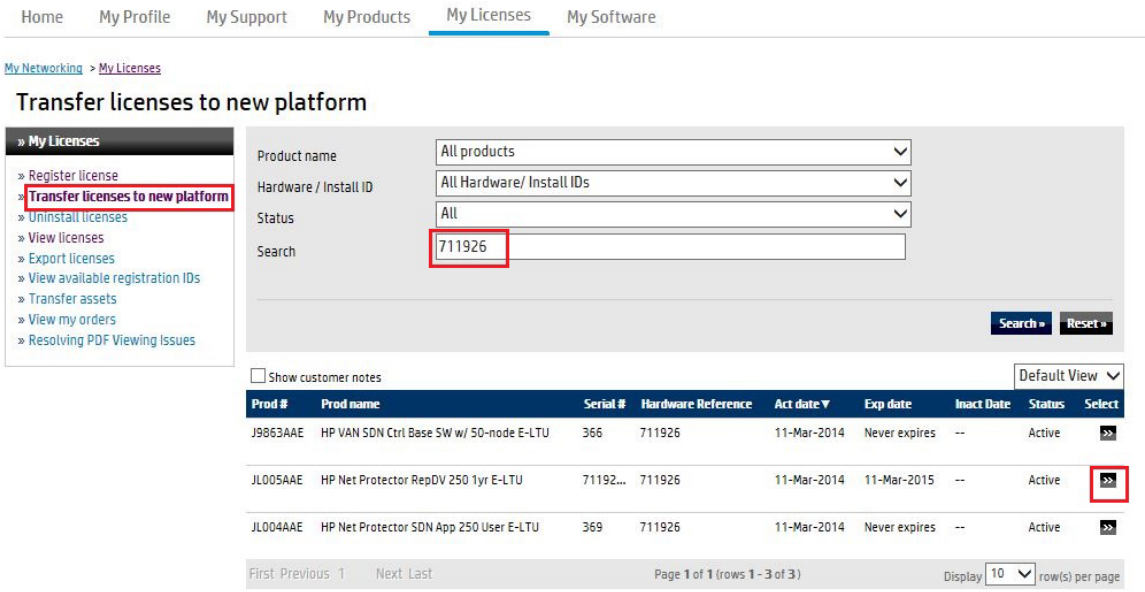
After you deactivate your HP Network Protector and HP VAN SDN Controller base licenses, you can transfer them.

To transfer licenses:

1. Log on to **My Networking** portal.
2. From the **My Licenses** section, select **Transfer licenses to new platform**.
3. In the **Search** field, enter the Install ID for the license you want to transfer, and then click **Search**.

   The transfer license screen displays a list of associated licenses, as shown in Figure 17 (page 27).

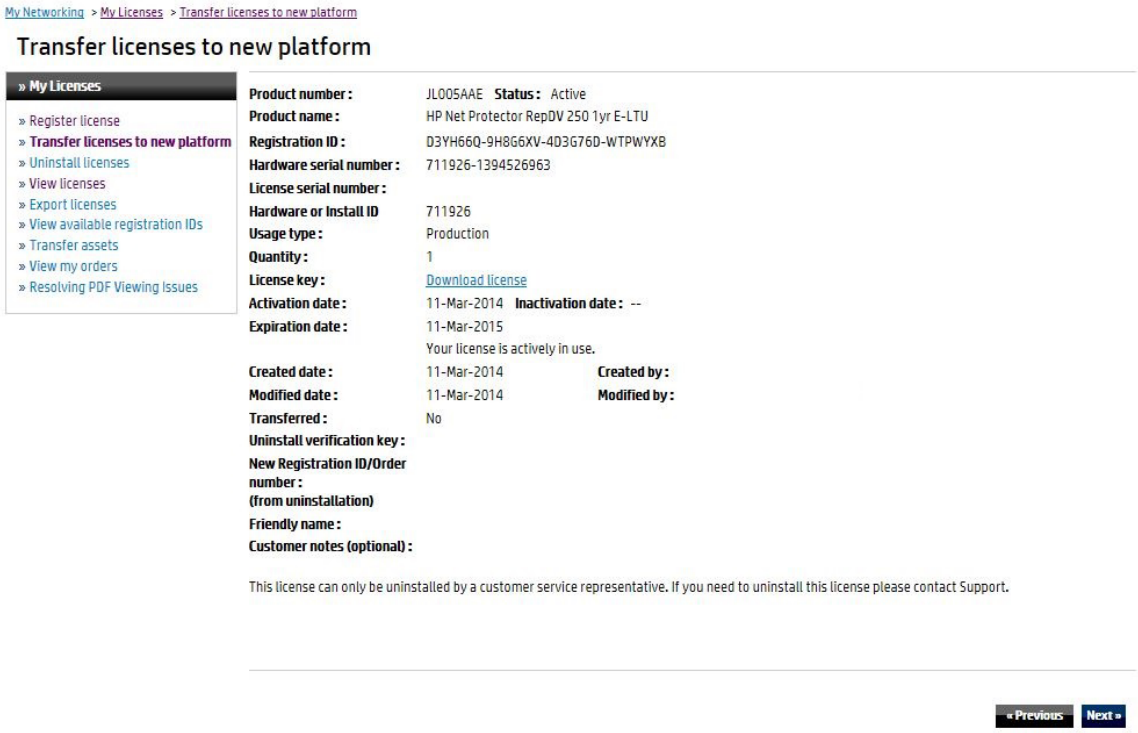
Figure 17 Selecting licenses to transfer



4. Click the **Select** icon next to the license to be transferred.

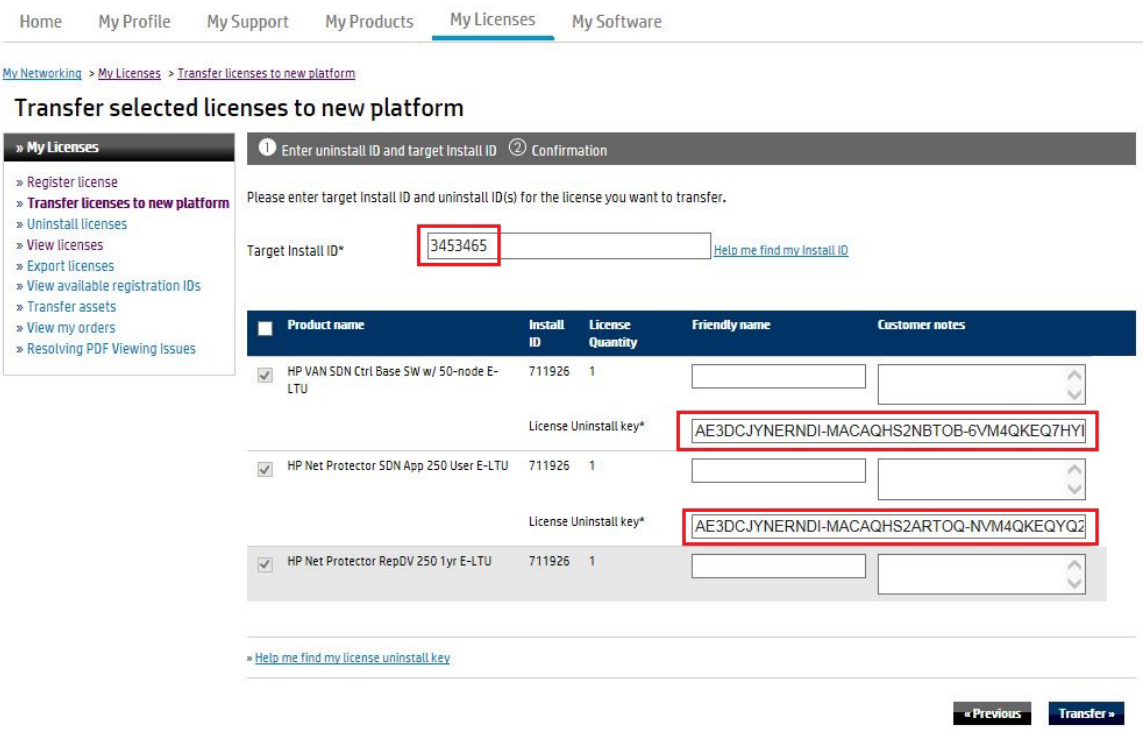
   The license details screen appears, as shown in Figure 18 (page 28).

Figure 18 Reviewing details before transfer



5. Verify that this is the license you want to transfer, and then click **Next**.
The target install ID screen appears, as shown in Figure 19 (page 28).

Figure 19 Entering target install and uninstall IDs

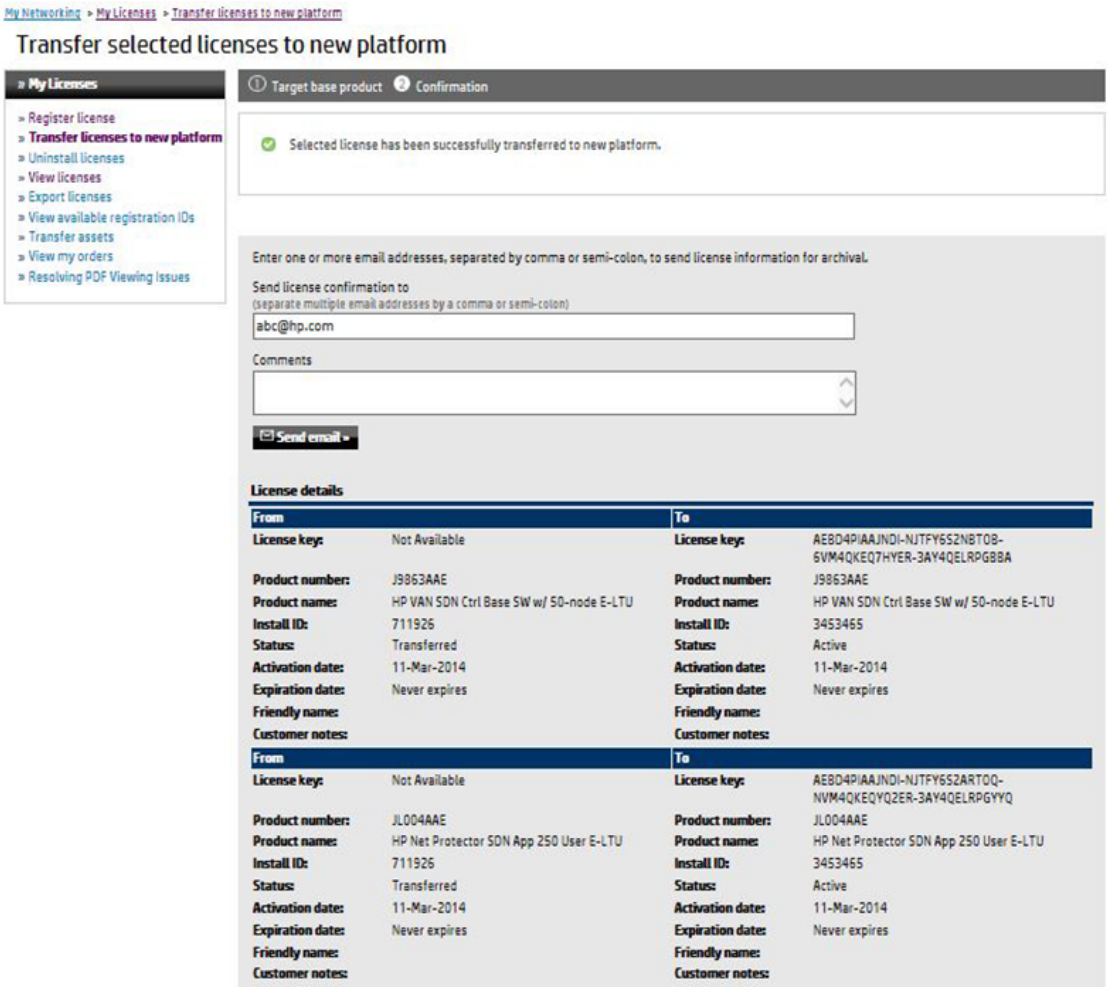


6. Enter the Install ID in the **Target Install ID** field and a license uninstall key in each **Uninstall** field, and then click **Transfer**.

NOTE: For the transfer process to succeed, you must enter an **Uninstall** value for every registered license, except for the HP Network Protector RepDV subscription license. For the transfer of the HP Network Protector RepDV subscription license, uninstall value is not required to be entered.

New license registration information appears on the license transfer confirmation and license details screens, as shown in Figure 20 (page 29).

Figure 20 Viewing license transfer confirmation and details



7. Review the confirmation screen details.

8. Optional: To email transferred license details:
   a. Enter one or more email addresses, separated by a comma or semicolon in the field provided.
   b. Optional: Enter comments about this license transfer in the **Comments** field.
   c. Click **Send email**.

   The license screen displays the status of the original licenses as **Transferred**, and the new Install IDs as **Active**, as shown in Figure 21 (page 30).

Figure 21 Reviewing transferred license status screens

Prod #	Prod name	Serial #	Hardware Reference	Act date▼	Exp date	Inact Date	Status	Select
JL004AAE	HP Net Protector SDN App 250 User E-LTU	369	711926	11-Mar-2014	Never expires	11-Mar-2014	Transferred	>>
JL005AAE	HP Net Protector RepDV 250 1yr E-LTU	71192...	711926	11-Mar-2014	11-Mar-2015	11-Mar-2014	Transferred	>>
J9863AAE	HP VAN SDN Ctrl Base SW w/ 50-node E-LTU	366	711926	11-Mar-2014	Never expires	11-Mar-2014	Transferred	>>

Prod #	Prod name	Serial #	Hardware Reference	Act date▼	Exp date	Inact Date	Status	Select
JL004AAE	HP Net Protector SDN App 250 User E-LTU	369	3453465	11-Mar-2014	Never expires	--	Active	>>
JL005AAE	HP Net Protector RepDV 250 1yr E-LTU	34534...	3453465	11-Mar-2014	11-Mar-2015	--	Active	>>
J9863AAE	HP VAN SDN Ctrl Base SW w/ 50-node E-LTU	366	3453465	11-Mar-2014	Never expires	--	Active	>>

4 Understanding the application console

4.1 About the console

The HP Network Protector console provides at-a-glance insight into your network security status with charts and graphs that continuously update to reflect the health, status, and events related to your network traffic. The console also provides the status of all the switches and the VLANs communicating with the application. This overview, composed of configurable color-coded charts and tables, is the starting point for:

- Monitoring the health and status of the devices and VLANs.
- Monitoring security alerts or issues.
- Troubleshooting events and issues on your network.

4.2 Initial configuration tasks

To set up the application, you will need the RepDV license key and the SNMPv3 credentials of at least one switch on your network. You can enter the SNMPv3 credentials of up to three switches on your network. The application uses the credentials to communicate with the switch and extract the switch details. It uses these details to configure Service Insertion tunnels.

If you do not provide the SNMPv3 credentials, then the application communicates with the switch through the OpenFlow channel.

1. Use a supported browser to access the application user interface at the following IP address:

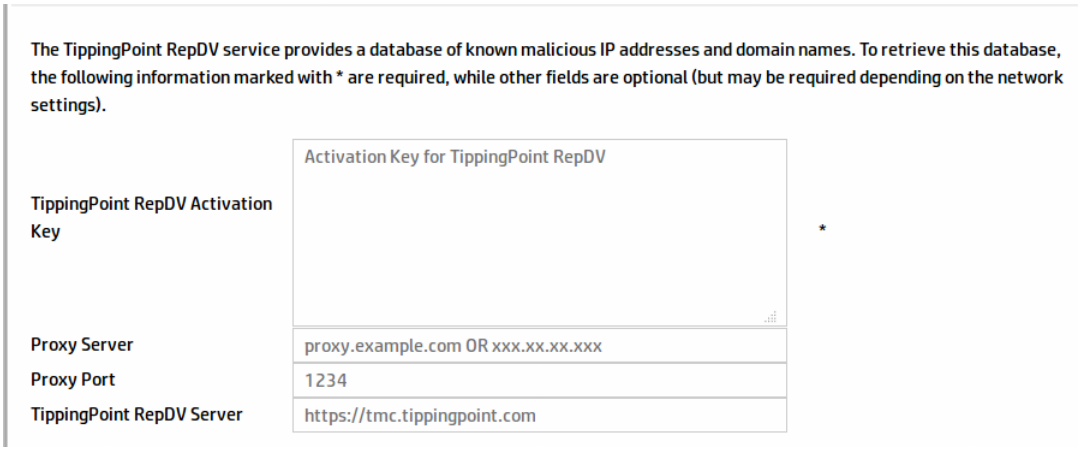
   `https://ip_addr:8443/networkprotector/ui`

   Where *ip_addr* is the IP address of the system on which you have installed the application.

   For example:

   `https://127.0.0.1:8443/networkprotector/ui`

   A setup wizard appears when you log in to the application for the first time.



2. Enter the RepDV license key in the **TippingPoint RepDV Activation Key** field.

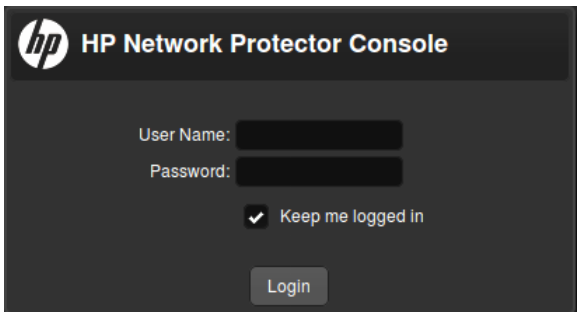
   NOTE: For more information about RepDV license key, see "Licensing" (page 20).

3. Enter the proxy server and proxy port details if required.
4. Click **Next**.
5. Enter SNMPv3 credentials of at least one switch.
6. Click **Finish**.

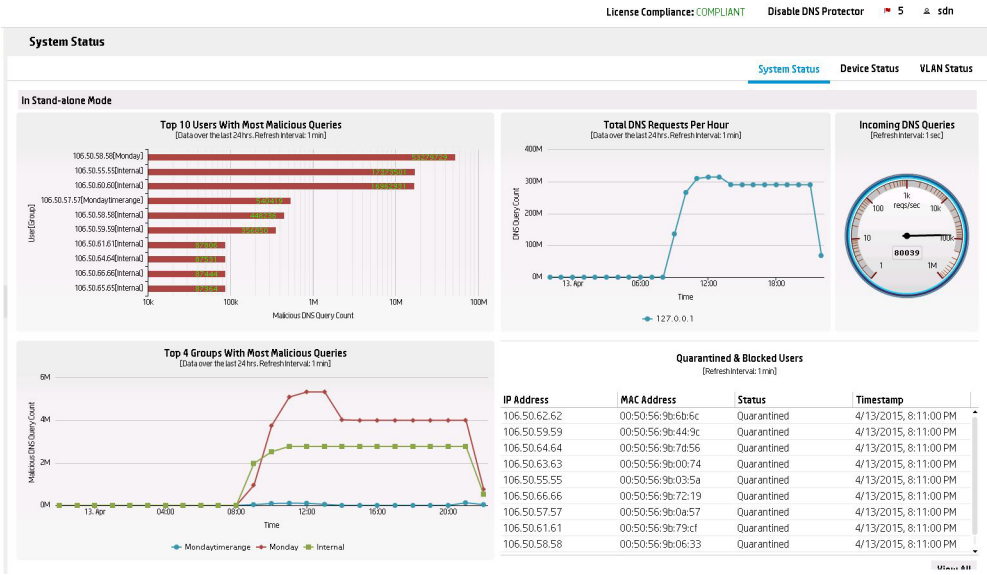
The main application Console page appears.

4.3 Logging into the console

1. Use a supported browser to access the application user interface at the following IP address:
   `https://ip_addr:8443/networkprotector/ui`
   Where *ip_addr* is the IP address of the system on which you have installed the application.
   For example:
   `https://127.0.0.1:8443/networkprotector/ui`
2. Enter user name and password credentials, then click **Login**.



The main application page appears:

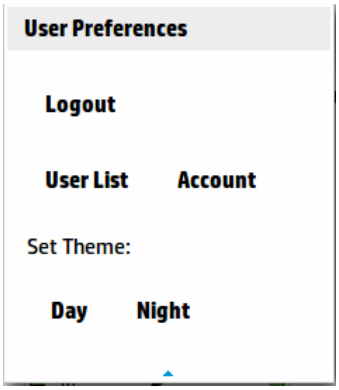


For more information about the supported web browsers see the *HP Network Protector SDN Application Support Matrix Guide* in the SDN information library.

4.4 Displaying the application user window

To display the application User Window, click sdn icon.

The **User Preferences** dialog box appears:



4.5 Adding a user

The login credentials to the application is the same as the controller credentials. After the controller user logs into the application, the user has access to all the features of the application.

For more information about the user management, see the *HP VAN SDN Controller Administrator Guide* in the SDN information library at http://www.hp.com/go/sdn/infolib.

4.6 Verifying license compliance

You can view the **License Compliance** status to check if the number of concurrent users connected to the application is compatible with the license policy. The application controls the number of concurrent users by licenses and provides a grace allowance for the application users. The status also reflects if you have not added the license to the application or if the license has expired. The application checks for license compliance at an interval of one minute and provides the status in the form of color code as listed in the table.

Table 3 License compliance status

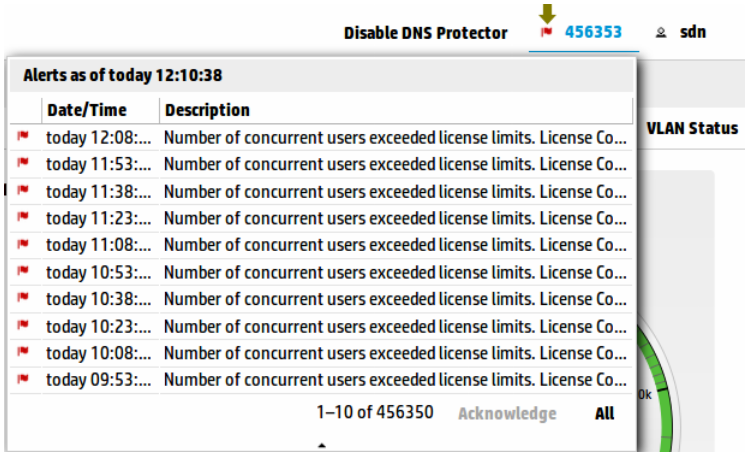
Color	Status	Description
Green	Compliant	The application is licensed and concurrent users connected to the application are within the grace allowance license limits.
Red	Non-compliant	The application is licensed but the concurrent users connected to the application are beyond the grace allowance license limits.
Red	Not Licensed	The application is not licensed, deactivated, or the license has expired.

For more information

"Generating license compliance report" (page 67)

4.7 Viewing alerts

View the number of critical alerts generated by the application next to the alert symbol on the console. To view the last 10 alerts generated by the application for quick reference and action, click the alert symbol .



You can perform the following actions on the Alert dialog box.

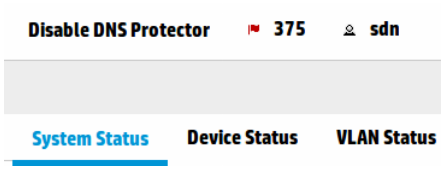
- Select an alert and click the **Acknowledge** button to acknowledge the alert.
- To view all the alerts, click the **All** button and navigate to the **Alerts** page.

For more information

"Alerts" (page 58)

4.8 Disabling the application

You can choose to disable application on your network by clicking **Disable DNS Protector**



on the application console.

When you disable the application on your network:

- The DNS traffic is not monitored by application
- The traffic flows normally
- The configuration and operation of the network is not affected

You can enable the application on your network to start monitoring the DNS traffic again. You can disable and enable the application on your network without making any changes to the network configurations or other settings.

5 Configuring application components in the controller

Log into the controller to configure components of the application.

5.1 Descriptions of the configurable components

5.1.1 Rule refresher

The application provides a rule refresher mechanism to refresh the DNS redirect rule pushed down by the application. It may be configured within the base controller configurations section and the default interval of 3 seconds is enabled when the application is installed.

The purpose of this rule refresher is to age out the DNS Divert rule on all the controlled switches in the event that the application becomes unavailable. A failure to refresh the rule effectively disables DNS inspection after 8 seconds, at which time the DNS traffic would be forwarded directly to the DNS server.

NOTE: You cannot change the values in the rule refresher configuration section. These values can be changed only by the HP support personnel for troubleshooting purposes.

Component	Description
`hard.timeout`	Time interval until which the switch will wait for the refresher signal from the application. After the lapse of the timeout interval, the switch falls back to the normal working flow and the data is not monitored by the application. The default value is 8 seconds.
`refresh.interval`	Intervals in seconds at which the application will refresh the DNS redirect and normal rule on the switch. The default value is 3 seconds.
`rule.refresher.enabled`	You can enable or disable the rule refresher. By default the rule refresher is enabled.

5.1.2 Tunnel heartbeat manager

NOTE: You cannot change the values in the tunnel heartbeat manager configuration section. These values can be changed only by the HP support personnel for troubleshooting purposes.

Component	Description
`tunnel.heartbeat.interval`	Intervals in millisecond at which heartbeat signals are sent to the monitored tunnels. The default value is 1000 milliseconds.
`tunnel.heartbeat.receive.queue`	The length of the heartbeat receiving queue. The default value is 200.
`tunnel.heartbeat.retry`	The number of times the application sends heartbeat signals to the tunnel without receiving the reciprocating heartbeat signal from the tunnel before the application declares it as down. The default value is 5.
`tunnel.heartbeat.timeout`	Interval at which the heartbeat checker thread monitors the received queue to pull out the heart beat packet if any and compare them against the sent heartbeat signal. This value must be less than the `tunnel.heartbeat.interval` value.

5.1.3 Log config service

Component	Description
`startup.debug.enabled`	Set this value to true to enable debug log when the application starts. By default, this value is not enabled.

5.1.4 Service manager

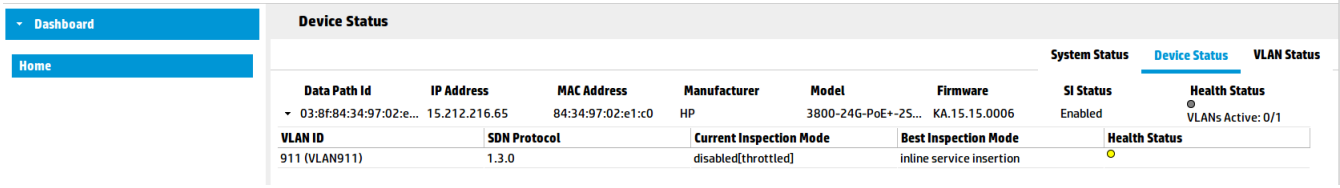
Component	Description
`stat.cache.enabled`	Enables or disables caching of data retrieved from CSD (Cassandra Statistics Database) in memory for faster user interface responsiveness. If disabled, each web client and each UI graph on the application console issues separate request to CSD.
`stat.cleanup.time`	The time of day to run periodic cleanup of the CSD. This specifies a time of day to perform the periodic cleanup task. Local controller's time in 24 hours format.
`stat.enabled`	Enables or disables the collection of statistics that are persistently stored in the CSD.
`stat.flush.interval`	Specifies the time interval in seconds between flushes of the in-memory write-cache to the persistent CSD.
`stat.limit`	The maximum number of records that are requested in a single query to the CSD.
`stat.retention.day`	The data retention interval (in days) for day-granularity data in the CSD.
`stat.retention.hour`	The data retention interval (in days) for hour-granularity data in the CSD.
`stat.retention.min`	The data retention interval (in days) for minute-granularity data in the CSD.

5.1.5 Throttle manager

The HP Network Protector throttles or disables the top 3 switches when their DNS traffic increases above a set threshold limit. The DNS OpenFlow rules are removed from these switches to reduce the incoming traffic to the controller. The application sends an email to the configured administrators providing the IP address of the devices disabled from inspection. The devices are a disabled for a period of 5 minutes by default and are then re-enabled for inspection.

To view the status of the throttled or disabled switches, from the HP Network Protector UI, navigate to **Dashboard** +**Home** +**Device Status**.

Figure 22 Throttled or disabled switch status



The **Health Status** of the switch is grey indicating that one or more DataPaths of the switch has been disabled. The **Current Inspection Mode** shows that the DataPath has been disabled due to throttling.

From the controller UI, the values throttling components can be modified. You cannot change the values in the throttle configuration section. These values can be changed only by the HP support personnel for troubleshooting purposes.

Component	Description
`cooldown.interval`	The interval in millisecond after which the throttled datapaths are enabled. Default value is 300000 milliseconds (5 minutes).
`rate.monitor.interval`	The time interval in milliseconds at which the incoming packet rate counter is sampled by the application. Default value is 500 milliseconds.
`rate.threshold`	The threshold value for incoming packet rate, which when breached the application throttles the switch. Default value is 0. When the value is 0 the threshold is calculated based on the number of CPUs available on the system.
`tolerance.threshold`	This value controls the throttling sensitivity. The number of consecutive times the threshold has to be breached before throttling is initiated. Default value is 2.
`throttle.disabled`	Setting this variable to true disables throttling. Default value is false.

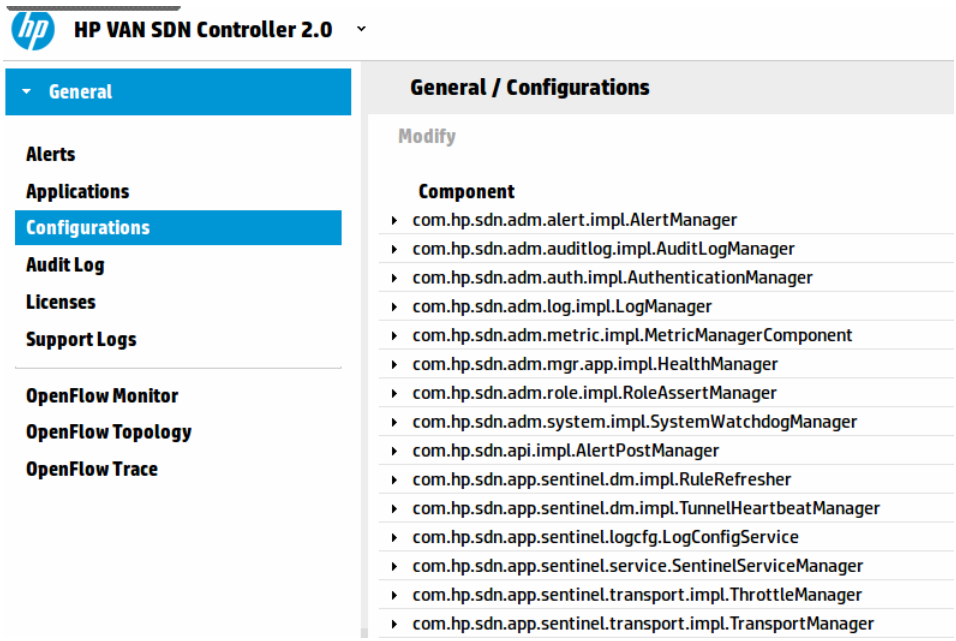
5.1.6 Transport manager

You cannot change the values in the transport manager configuration section. These values can be changed only by the HP support personnel for troubleshooting purposes.

Component	Description
`inspect.queue.size`	Intervals in millisecond when the application inspects the internal queue size.
`num.worker.threads`	Number of worker threads for both inspect and audit pools.
`socket.receive.buffer`	Socket receive buffer size in bytes.
`socket.send.buffer`	Socket send buffer size in bytes.

5.2 Accessing the configurable components

The default values set in the controller are sufficient for the optimal functioning of the application. You can configure some of the application components on the controller. You can enable or disable the components for testing and troubleshooting purposes. The **Configurations** enable access to the configurable components in the controller.



5.3 Configuring link aggregation

The links are created with one terminating end at the switch and the other terminating end at the controller's NIC. You must configure the switch and the controller NICs to implement link aggregation. You can aggregate the links for load balancing and redundancy. The switches support following link aggregation methods on the server:

Table 4

Configuration method	Mode	Description
Round robin method	(bond_mode 0)	Transmits packets in sequential order from the first available (NIC) slave through the last. This mode provides load balancing and redundancy.
Active backup method	(bond_mode 1)	Only one NIC slave in the bond is active at a given time. A different slave becomes active only if the active slave fails. This mode provides only redundancy.

IMPORTANT:

- Before you implement link aggregation, create the backup of the `/etc/network/interfaces` file.
- Ensure you always have a way to connect to or reach the server, if you are configuring NIC aggregation over ssh. When you restart the network manager, if there are configuration errors, you might lose connections to the server.

5.3.1 Configuring the switch NICs

1. Configure LACP (Link Aggregation Control Protocol) on the switch with the ports the ports that you want to use for link aggregation.
   ```
   trunk B1-B3 trk10 lacp
   ```

5.3.2 Configuration the controller NICs

1. Stop all the controller NICs that you want to configure as slaves in the aggregated link (bond0)..
2. Assign the NIC roles such as master and slaves in `/etc/network/interface` file.

Example 2 Sample network interface file

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
          address 1.1.1.135
          netmask 255.255.255.0
          broadcast 1.1.1.255
          gateway 1.1.1.1
          network 1.1.1.0
          dns-domain ind.hp.com
          nameserver 192.0.2.0/24

auto eth1
iface eth1 inet manual
bond_master bond0
bond_primary eth1

auto eth2
iface eth2 inet manual
bond_master bond0

auto eth3
iface eth3 inet manual
bond_master bond0

auto bond0
iface bond0 inet static
          address 172.16.22.10
          netmask 255.255.255.0
          network 172.16.22.0
          gateway 1.1.1.1
          bond_mode 1
          bond_miimon 100
          bond_slaves eth1 eth2 eth3
          bond_primary eth1
<comment>Sets a controller NIC to act as a master.<comment>
          bond_updelay 200
          bond_downdelay 200
```

3. Load the Linux aggregation bonding module into the Linux kernel using the following command:
   `sudo modprobe bonding`
4. Configure other controller NICs as slaves to the master NIC using the `ifenslave` Linux utility.
   `ifenslave bond0 eth, eth2, ...ethn`
5. Restart network-manager service for the configuration to take effect.
   `sudo service network-manager restart`

5.3.3 Verifying link aggregation status

On the machine you have installed the controller, execute the `ifconfig` utility to verify the following parameters:

- The bond interface (bond0) with the configured switch IP has started.
- The bond interface status is displayed as `MASTER`.
- The slave interfaces (eth1, eth2...) have started.
- The slave interfaces are displayed as `SLAVE`.

5.4 Regulating DNS traffic to the application

When the DNS traffic to the switch is high, the switch cannot take up the extra load of sending the DNS packets to the application for inspection. You can configure the application to stop inspecting the DNS packets from the switch during peak DNS traffic. You can set the DNS packet limit for switches configured for OpenFlow channel. The DNS packet limit cannot be configured on switches that support Service Insertion. When the switch reaches the DNS packet limit, then the application stops capturing the DNS packets for a few seconds and then resumes capturing the packets again.

The default value can be set based on the following switch criteria:

- Switch manufacturer, for example HP
- Switch family, for example Provision, Comware or
- Switch models, for example 5900, 5920, 5930, 3500, and others

5.4.1 Setting the DNS packet limit for switches

Each switch has a default DNS packet limit set. You can change the default DNS packet limit through REST API. Use RSdoc, an API online documentation tool, to interact with REST APIs on the controller.

1. Use a supported browser to access the RSDoc user interface at the following IP address:

   `https://ip_addr:8443/api`

   Where *ip_addr* is the IP address of the system on which you have installed the controller.

   For example:

   `https://127.0.0.1:8443/api`

   The RSdoc page appears.
2. Select **Magellan API v1.0** from the drop down list.
3. Enter the credentials in the **X-Auth-Token** text box and click **Explore**.

   The **/throttler** page opens.
4. Click **/throttler** to list all the APIs.
5. Click **Get** next to **/throttler/devicelimit**.
6. From the **Response Body**, copy the REST api for the switch you want to change the DNS packet limit.

   Example 3 Sample REST API with DNS limiting value of 4500

   ```
   { "id": "6fd30d7f-8ff5-4db5-8bd7-a0081e1289d2",
   "manufacturer": "HP",
   "family": "PROVISION", "model": "3800",
   "packetInLimit": 4500 },
   ```

7. Click **Put** next to **/throttler/devicelimit**.
8. Paste the Rest API in the **deviceLimit** section and change the DNS packet limit value.
9. Click **Try it out**.

   The new DNS packet limit value is updated for the switch.

6 Working with Profiles

You might want to manage different categories of users, DNS traffic, and VLANs differently or you might want to manage traffic differently during different times of the day or week. For example, you might want to create a policy that allows certain users to access the internet sites needed to do their duties, but block them from sites that might use too much network bandwidth or otherwise might reduce worker productivity. You can use a profile to create a set of policies for a specific VLAN or group of VLANs.

6.1 VLAN groups

You can group the VLANs into logical groups to assign policies. You can create policies for each VLAN group based on the requirement.

For example, in a university campus, you can create two VLAN groups. You can group all the VLANs in the main university campus into one group and all the VLANs in the dormitory as the other group. You can apply customized policies to manage both groups.

6.1.1 Creating a new VLAN group

1. Select **Profiles→VLAN Groups**.
2. Click the **New** button. The **Create new group** page appears.
3. Enter a logical name for the group in the **Group Name** text box.
4. Select the VLANs that you want to group from the list of available VLANs.
5. Click the → to group the VLANs.
6. To add a VLAN that is not listed, enter the VLAN number in the VLAN text box, and click **Add**.
7. Click **Create**. The group is added to the Groups view.

6.2 About custom lists

You can work with four types of custom lists to manage traffic in your network:

- Whitelist
- Priority whitelist
- Blacklist and
- Greylist

6.2.1 Whitelist

You can add host names to the whitelist. The application compares the host names on this list and allows access to the host names without examining the blacklist or the RepDV database. You can add host names to whitelist when you want the application to skip looking for the host names in the blacklist and the RepDV database. You can also override the RepDV database entries with whitelist host name entries. Unlike the blacklist or greylist, where you can set time ranges, the whitelist is always active.

You must edit the default list to add whitelist entries. You cannot delete the default list.

IMPORTANT: The whitelist allows access to the exact matches of domain names listed. It does not recognize fuzzy matches. Use wild card entries to allow access to domain names with fuzzy matches.

6.2.2 Adding entries to the whitelist

1. Select **Profiles** →**List**.

   The **Profiles/List** page appears.
2. Select the **default** list and click **Edit**.

   The whitelist **Edit List** page appears.
3. Click **Add** and enter the domain name in the **Domain Name** text box.
4. Repeat Step 3 to add more whitelist entries.
5. Click **OK** to save the list.

6.2.3 Priority whitelist

All the traffic in the network does not have equal importance or priority. In other words, some traffic is critical to the business, while some are not. But both type of traffic is vying for the same available network bandwidth. To manage critical traffic and provide preferential treatment to it and ensure that it reaches its destination, you can create a whitelist entries and attach the Quality of Service (QoS) and priority to the traffic. Based on the QoS value and the priority, the application treats the various types of data streams that flow across your network traffic differently.

IMPORTANT: You can create a maximum of 20 whitelists and each whitelist can contain up to 10 domain list entries.

6.2.4 Blacklist

In addition to the RepDV database, you can add blacklist entries of host names to restrict access. When a user accesses a domain listed in the blacklist, the application drops the traffic and the statistics of end users trying to access the blacklist sites is updated in the logs.

When you generate reports based on the total number of blocked DNS requests or malicious DNS requests, then the reports contain the blacklist DNS entries along with the RepDV database.

6.2.5 Greylist

You can include host names in the greylist that are not harmful to your network but might be blocked to adhere to business policies. You can add host names to greylist to restrict access to certain sites during specific time of the day. When you add host names to the greylist, the user will not be able to access the host. Unlike a blacklist, the application does not save the statistics of users trying to access greylist entries as malicious DNS requests.

For example, in a university campus, you can set the greylist to restrict access to social media sites which are a distraction during class hours. Restricting access to social media sites encourages the staff and students to engage more with each other, during class hours.

6.2.6 Rules for creating whitelist and custom list entries

The whitelist and custom lists match exact domain names entries in the lists to allow or block access to domain names. They do not recognize fuzzy matches. Use wild card entries to be able to access domain with fuzzy matches.

The host name address must contain at least two levels and you can enter wild cards at third or more levels.

Example 4 Fuzzy match entries

To allow access to a site such as http://www.iboss.com/ and if you provide only www.iboss.com as an entry in the whitelist, then the application allows access to only the exact entry of www.iboss.com and blocks access to the site for any other match to the same sites such as www.iboss.com/solutions/issue and others.

To allow access to all matches to the site, use wild card entries such as *er.iboss.com, *iboss.com. You cannot add whitelist entries like *.com or *.* etc.

6.2.7 Creating priority whitelist, blacklist, or greylist

You can create multiple priority whitelist, blacklists, and greylists. After creating the lists, you can add domain names to each list, with each list containing customized list of domain names. You can add the custom lists to various VLAN groups depending on the requirement. For example, a list of greylist entries for students in a university might not be the same as for the professors.

1. Select **Profiles** →**List**.

   The **Profiles/List** page appears.
2. Click the **Add**.

   The **Create New List** page appears.
3. Enter a name for the list in the **Name** text box.
4. Enter a description for the list in the **Name** text box.
5. From the **Type** drop down list, select **Blacklist**, **Greylist**, or **Priority Whitelist** depending on the type of list you are creating.
6. Click **Add** and enter the domain name in the **Domain Name** text box.
7. Repeat Step 6 to add more domain names.
8. Click **OK**.

   The domain names are added to the custom list.

6.2.8 Loading the priority whitelist, blacklist, or greylist from external file

To load the blacklist or greylist from a file:

1. Select **Profiles** →**List**.

   The **Profiles/List** page appears.
2. Select the list and click **Edit**.

   The **Edit List** page appears.
3. Click **Import**.

   The **Upload Custom list file** page appears.
4. Click **Browse** and navigate to the blacklist or greylist you want to upload and click **OK**.

   The addresses from the list are added to the custom list.

6.3 About RepDV Filters

The RepDV provides Domain Name System (DNS) security intelligence feeds from a global reputation database so that you can actively enforce and manage reputation security policies. The application uses the reputation scores to inspect traffic in real-time and enforce security policies.

You can customize the reputation scores and apply it to the inspection policy to protect your network. Table 5 (page 44) lists out the various threat types.

Table 5 Threat types

Threat type	Meaning
Botnet	Malicious software is installed on your computer through the Internet without your knowledge and your computer is used to perform repetitive tasks. The tasks can include sending out spam mails, spread malicious software, and perform other illegal activities. When performing these tasks the performance of your computer might slow down.
Malware	Malware is the abbreviation for malicious software. Malware is installed on your computer without your knowledge to disrupt your computer operation or to gather sensitive information. The information gathered can be used to display unsolicited advertisements or redirect affiliate marketing revenues to the malware creator.
Misuse and Abuse	Misuse and abuse of the network resources. This is similar to the peer-to-peer protocols where the network resource and bandwidth are primarily used to share music and video files.
Network Worm	A network worm is a standalone malware computer program that replicates itself to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program.
Peer-to-peer (P2P)	Peer-to-peer protocols are primarily used to share music and video files, and essentially turn a personal computer into a file server which makes its resources and those of its host network available to the peer-to-peer community.
Spam	Electronic spamming is the use of electronic messaging systems to send unsolicited bulk messages (spam), especially advertising, indiscriminately.
Spyware	Spyware is a type of software that transmits information without the user's knowledge or permission. Spyware may be the result of a virus infection or may be installed along with other applications. Spyware often consumes vast resources and can slow systems and, in some cases, cause systems to become unstable or unusable.
Web Application Attackers	Web Application Attackers generally look for vulnerabilities in a network. Writing malicious code, they try to find the weak points in a network security system to bypass filters and reach data and services. These attackers seek to use intrusion methods against areas, such as software back-doors and poorly protected hosts and ports.
Worm	A worm is also a malicious software that spreads from one computer to another, leaving infections as it travels. Worms use either the network vulnerability or social engineering to trick the user to spread. Network worms are capable of damaging data or software and causing denial-of-service (DoS) conditions.

6.3.1 Creating a new RepDV filter

1. To create a new RepDV filter, select **Profiles** +**RepDV Filters**.
2. Enter a logical name for the filter in the **Name** text box.
3. Select the **Threat Type** you want to edit and click **Edit**.

   The **Edit a Threat Entry** page appears.
4. Set the required reputation score for the threat.

5. Select the source location of the threat. The source of the threat can be any location or specific geographical locations.
6. Repeat Step 3 to Step 5 to set the reputation score of other threat types.
7. [Select a threat type and click **Disable** to disable the threat based on your requirements.]
8. Click **OK**.

   A new RepDV profile is created.

6.4 About schedules

You can create schedules to apply to the priority whitelist, greylist, and the blacklist. The schedules give you the flexibility to allow the users to access the lists during certain times of the day or certain days of the week.

For example, during office hours, you can block employees from accessing video-sharing websites. Restricting access to video-sharing website saves network bandwidth and improves employee productivity. You can allow employees to access the video-sharing sites after office hours and during holidays.

6.4.1 Creating a schedule

1. Select **Profiles→Schedules**.

   The **Profiles/Schedules** page appears.
2. Click **New**.

   The **Create a new Schedule** page appears.
3. Enter a logical name for the schedule in the **Name** text box.
4. Enter a description in the **Description** text box.
5. Select a time range from the **Time** section.
6. Select **Server** or **Browser** option, to set the server or client time zone.
7. Select the days of the week from the **Days of the Week** section.
8. Select **Holidays** to apply this schedule during holidays.
9. Set the start and end dates from the **Range** section and click **OK**.

7 Setting Policies

You can set four types of policies for the traffic on the VLANs. The policies are:

- Default policy
- Threshold policy
- Priority whitelist policy and
- Inspection policy

7.1 About default policy

The default policy is similar to the inspection policy except that it is active all the time. You can apply the default policy only to Internal (Default) VLAN group. No other VLAN group can be attached to this policy. This policy checks incoming DNS packets to the Default RepDV filter only. You cannot attach any other RepDV filter to it.

You can assign blacklist and greylist to the default policy. All the DNS traffic in the network is continuously compared with the profiles attached to the default policy. If the traffic in the network matches the default policy, then the policy is applied to the DNS network traffic.

Unlike the other policies, where you can assign a schedule to allow or block when users can access the sites, the default policy is always active.

7.2 About threshold policies

You can set general threshold policies for all the hosts in the network to manage and mitigate malicious traffic and host name requests. The general policies prevent the host from acting like a botnet and being controlled by external malicious computers. By default, the general policies are disabled.

You can set the policies for the following network traffic pattern in your system:

- Unique threat – Number of unique threats originating from any host. Unique threats include threats matching RepDV database and blacklist entries.
- DNS requests per second – Total number of DNS requests originating from any host per second.

When network traffic from a host exceeds the policy limits or matches the threshold policy, you can configure application to perform one of the following actions:

Action	Description
Block	When a host breaches the general policies, the application blocks the host from sending current and all subsequent packets. The block on the traffic ensures that the attack never reaches its destination. You can choose to block a host to completely isolate the host from the network.
Block and Notify	Blocks the host from sending current and all subsequent packets and sends a mail notification to the administrator.
Quarantine	When a host breaches the general policies, the application quarantines the host. That is, the host is blocked from accessing any resource on the network except the hosts listed in the ACL (Access Control List) under Policy Enforcement Settings. The host is directed to a known safe site or the DNS is resolved to report that the domain does not exist. For example, when a host is quarantined, all the traffic from that host is blocked, but the host can access the IP phone, if the IP phone server is listed in the ACL.

Action	Description
Quarantine and Notify	The application quarantines the host and sends a mail notification to the administrator.
Notify	The application sends out a notification to the administrator in the form of email if a user accesses a host name that is listed in the blacklist, greylist, or matches the threat profile. The event is logged in the application log. The application does not drop or quarantine the traffic to the domain and the user continues to access the domain.

7.2.1 Setting threshold policies

1. Select **Policies** →**Policies**.

   The **Policies/Policies** page appears.
2. Select the **DNS request per second** or **Unique Threats**.
3. Click **Edit** to edit the general policies.

   The **Edit General Policies** page appears.
4. Enter the threshold value in the **Threshold Value** text box based on the selected policy type.
5. Select one of the actions from the **Action** section:
   - **Block**
   - **Quarantine**
   - **Notify**
6. Enter time in minutes in the **Expiration Time in Minutes** text box to set the time interval for the set action, and click **OK**.

   The **Policies/Policies** page appear.
7. Select the threshold policy you configured and click **Enable**.

For more information

"Adding hosts to the ACL" (page 65)

7.3 About priority whitelist policy

All the safe traffic flowing to and from the whitelist domains in your network competes for bandwidth whether it is of prime importance or negligible importance. Attaching Quality of Service (QoS) marking and assigning a priority to the network traffic enables the application to differentiate traffic based on the DSCP/PCP tag values set in the traffic. QoS functionality differentiates the various types of data streams that flow across your network by tagging DSCP/PCP values to the traffic.

The application differentiates the traffic destined to the domain listed in the priority whitelist by tagging DSCP/PCP value to the traffic flowing in and out of the network from the listed domain. You can configure policy based routing at the WAN based on DSCP/PCP tagging done at the access edge switch. You might configure to provide DSCP/PCP tagging for specific site traffic so that you can route this traffic based on some criteria, such as different ISP or time of day, date, or year.

For example, you might want to tag all social media site traffic with a DSCP/PCP value so that you can direct such traffic to a lower capacity ISP and tag all critical traffic with another set of DSCP/PCP values so that the critical traffic can be directed to the best available ISP.

7.3.1 Creating a priority whitelist policy

After you apply the priority whitelist policy to a priority whitelist, the application tags the network traffic with DSCP/PCP tagging. The application does not perform any routing of the traffic based

on the tagging. Traffic routing on the WAN or edge switches must be implemented by applying the required ACL rules or other methods based on the DSCP/PCP tagging.

1. Select **Policies+Policies**.
2. Click **Add**.

   The **Create new Policy** page appears.
3. Enter a logical name for the priority whitelist policy in the **Name** text box.
4. Enter a description in the **Description** text box.
5. Select **Priority White List Policy** from the **Policy Type** drop down box.
6. Select the VLAN group to which you want to apply the policy from the **VLAN Group** drop down box.
7. Select the priority whitelist for which you want to tag the DSCP/PCP values from **Priority White List** drop down box.
8. Select the duration for which you want to apply the policy to the VLAN group from the **Time Range** drop down box.
9. Enter the IP address of the downstream switch in the **Downstream Switch IP** text box.

   NOTE: The downstream switch tags the downstream traffic coming back to the network from the external world. For example, the ingress traffic from an ISP.
10. Set the Quality of Service (QoS) and L2 priority for the traffic originating on this priority list and click **OK**.

7.4 About inspection policy

You can add customized inspection policy to inspect DNS traffic in your network and take suitable action, such as allow good traffic and block or drop bad DNS traffic. The inspection policy can be applied to VLAN groups in your network. You can apply schedules for the customized inspection policies.

To create an inspection policy to a VLAN, apply a blacklist and greylist to the policy and assign a RepDV profile. When the DNS traffic generated from a VLAN, which is part of the VLAN group associated with the inspection policy and the generated DNS, is listed either in blacklist, greylist or if it matches the RepDv filter that is associated with the policy, then the application performs the specified action such as, drop the DNS traffic, notify the administrator, or both.

7.4.1 Creating an inspection policy

1. Select **Policies+Policies**.
2. Click **Add**.

   The **Create new Policy** page appears.
3. Enter a logical name for the inspection policy in the **Name** text box.
4. Enter a description in the **Description** text box.
5. Select **Inspection Policy** from the **Policy Type** drop down box.
6. Select the VLAN group to which you want to apply the policy from the **VLAN Group** drop down box.
7. Select the blacklist, greylist, and the RepDV profiles for which you want to apply the inspection policy from the profiles section.
8. Select the duration when you want to apply the policy to the VLAN group from the **Time Range** drop down box.

9. Select one of the actions from the **Action** menu:
   - **Drop** – The application drops the DNS traffic when a user accesses a domain name that is listed in the blacklist, greylist, or matches the threat profile.
   - **Notify** – The application sends out a notification to the administrator in the form of email if a user accesses a host name that is listed in the blacklist, greylist, or matches the threat profile. The event is logged in the application log. The application does not drop the traffic to the domain and the user continues to access the domain.
   - **Drop** and **Notify** – The application sends out a notification to the administrator in the form of email if a user accesses a domain name that is listed in the blacklist or matches the threat criteria. The application drops the traffic to the domain.
10. Click **OK** to save the policy.

8 TippingPoint Reputation Digital Vaccine (RepDV) and ACL Manager

8.1 About the RepDV database

RepDV database is a subscription service that enables the application to monitor and block outbound communications with known malicious and undesirable host names. The RepDV database includes hundreds of thousands of known malicious or undesirable hosts. A threat score of 0 to 100 is assigned to each host name based on analysis of the activity, source, category, and threat. The Database overview page provides the high-level details of the RepDV database, such as the RepDV Server address, interval at which RepDV database checks for updates, the date, and time the database was last updated.

8.1.1 About the custom lists and RepDV search order

The application performs a sequential search on the whitelist, the blacklist, and finally the RepDV database before it allows the host to access external host names. When the application finds a domain name in the whitelist, it stops looking for the entry in the blacklist or in the RepDV database and allows the user to access the domain name. If a domain name is listed in the whitelist and the blacklist or the RepDV database, the application allows the user to access the domain name.

For example, if you add example.com in the whitelist and if example.com is listed as a malicious site in the RepDV database, you will still be able to access this site. Whitelist will override the blacklist entries and the RepDV database.

8.2 Searching for a domain name

Use the search field to filter domain name entries in the RepDV database, whitelist, greylist, or the blacklist. When you enter the domain name address in the search field, the domain name along with the database name where the host name is listed is displayed.

1. Select **Administration** →**Tipping Point**→**Search**.

   The **Search** page appears.
2. Enter the domain name in the **Domain Name** text box.
3. From the **Database** list, select all the databases from where you want to search the domain name.
4. Click the  icon.

   The domain name is listed along with the database name.

8.2.1 Rules for a successful search

While searching an entry which is present in custom lists, the search will be successful only if the corresponding custom list is attached to a policy which is active.

For example, if you have created a blacklist `mylist` that contains an entry `example.com`. If `mylist` is not attached to any inspection policy, and you search for `example.com`, then the search does not display any results.

If you attach `mylist` to an inspection policy `mypolicy` and if the policy is disabled, and you search `example.com` the search still does not display any results.

If `mylist` is attached to `mypolicy` and if `mypolicy` is enabled, then searching `example.com` is successful and the search displays the result.

Table 6 Criteria for successful search

Entry is attached to any inspection policy	The policy is enabled	Search result
No	No	Fail
Yes	No	Fail
Yes	Yes	Successful

8.3 ACL Manager overview

ACL Manager leverages five tuple packet attributes and VLAN ID to create access control policies. The five attributes are:

- Source IP address
- Source port (any)
- Destination IP address
- Destination port (80 or 443)
- Destination protocol (typically TCP)

Access control policies are based on packet attributes and enables the application to perform Deep Packet Inspection (DPI). If the incoming packet matches the access control policy, the application either drops the packet or forwards it based on the policy action you have set. You can also use the ACL Manager to apply network masks on source or destination IP addresses.

8.3.1 Adding an ACL rule

You can enter the tuple attributes such as the IP address, subnet address, and the port ID of the source or destination to create the ACL rule. If you set the source or destination subnet IP address, then the application matches the entire subnet for the entered IP address for both source or destination and blocks or allows any traffic for the subnet. If you set only the fields name and action then the rule applies to any IPv4 traffic, by blocking or allowing it depending on the selected action.

1. Select **Administration** →**ACL Manager**.

   The **Administration/ACL Manager** page appears.
2. Click **Add**.

   The **Add ACL Rule** page appears.
3. Enter a logical name for the rule in the **Name** text box.
4. Enter any or all the tuple attributes and the VLAN ID for which you want to apply the policy.
5. From the **Action** drop down box, select `Allow` or `Block`.
6. Set the **Bidirectional** property to either `True` or `False`.

Example 5

If you set the rule to block packets from **IP source** 10.0.0.10 and set the **Bidirectional** rule to `TRUE`, then packets to the destination IP address 10.0.0.10 is also blocked.

8.3.2 Editing an ACL rule

1. Select **Administration** →**ACL Manager**.

   The **Administration/ACL Manager** page appears.

2. Select the rule you want to edit and click **Edit**.
   The **Edit ACL Rule** page appears.
3. Edit any of the properties you want to change.
4. Click **OK** to save the rule.

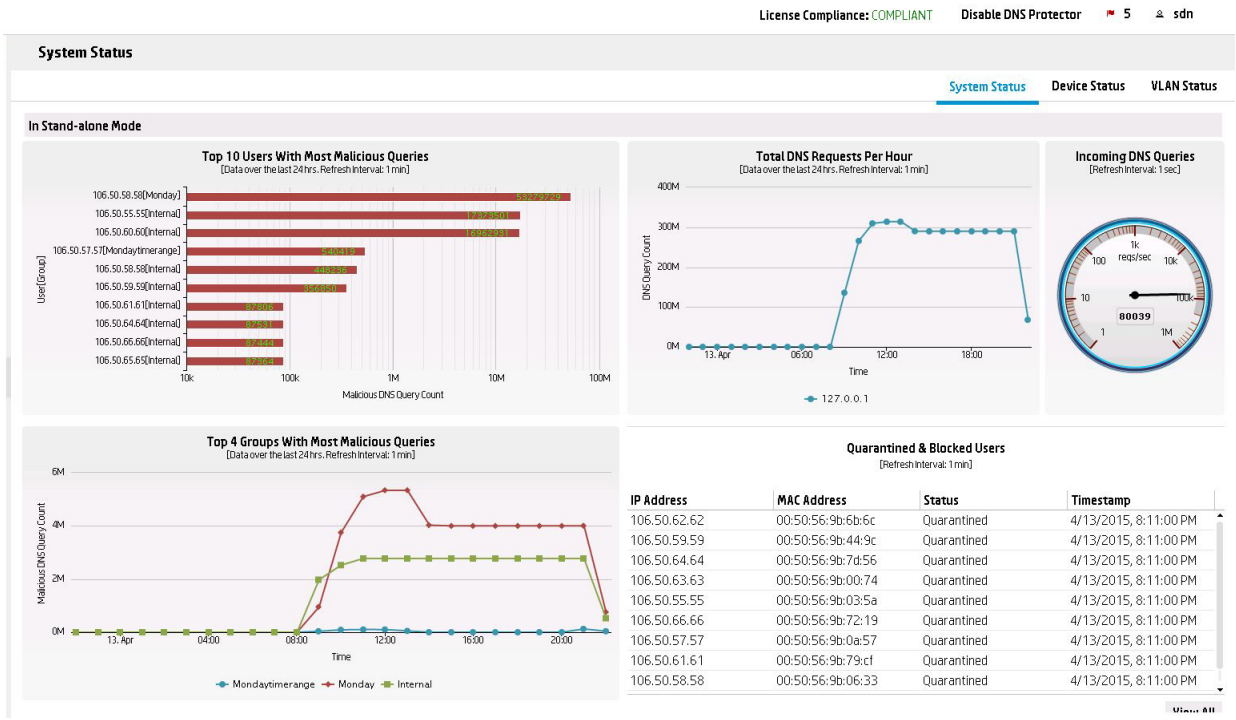
9 Monitoring

9.1 HP Network Protector panels

The application console provides configurable panels that enable you to view, monitor, and analyze health, status, and events at system and switch levels. These panels provide a high-level warning system for potential health and performance problems with your system and devices. The system status tool monitor characteristics of system health and report on the basic health and status of the network. The main focal points of the health and status panels include:

9.1.1 System status panel

Select **System Status** to display the system overview.



The **System Status** panel provides a graphical representation of the following system parameters. This information is refreshed every minute.

- Top 10 users with most malicious queries during the past 24 hours.
- Total DNS requests per hour during the past 24 hours.
- Incoming DNS requests per second.
- Top four VLAN groups with most malicious queries during the past 24 hours.
- The latest 10 blocked or quarantined hosts along with their IP address, MAC address, status, and time stamp.

Click **View All** button to view all quarantined and blocked hosts.

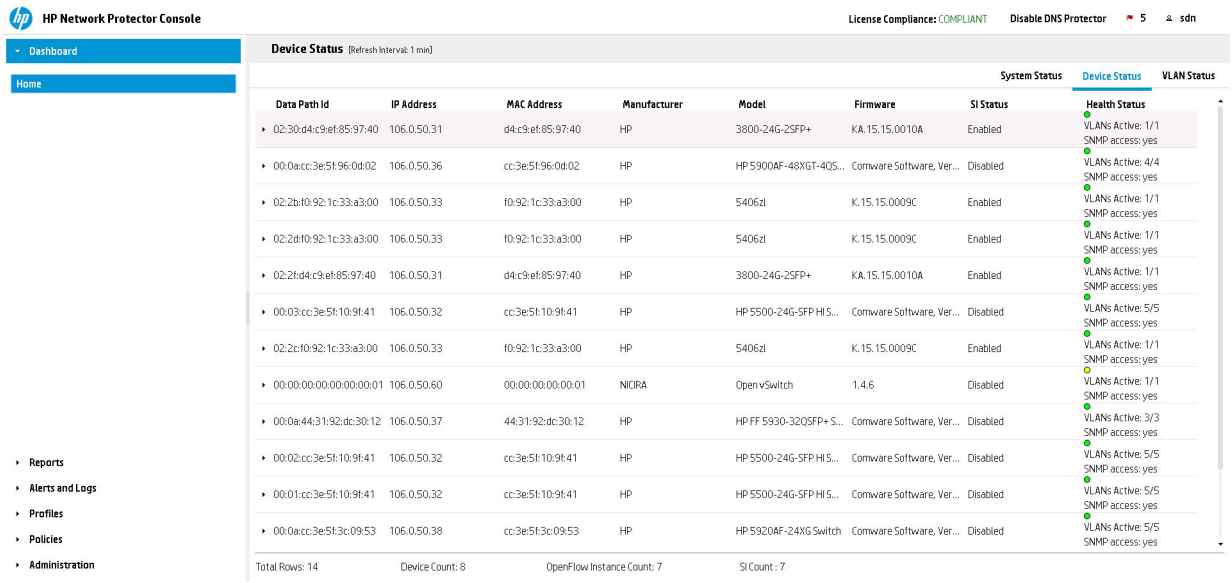
For more information

"Releasing quarantined clients" (page 65)

9.1.2 Device status panel

Select **Device Status** to display details of the switch and the health status of the VLAN configured on the switch.

Figure 23 Example of VLAN health status view



The device status panel displays the details of the switch such as:

- The IP and MAC address of the switch
- The manufacturer and model details of the switch
- The firmware installed on the switch and the SI status of the switch
- Switch connection status on the VLAN

The application uses the switch firmware information to decide if the communication with the switch is through OpenFlow channel or through the application Insertion tunnel. For firmware versions K.15.14 and lower, the application communicates with the switch through OpenFlow channel. For firmware versions KA.15.15.0015 and greater, the application can communicate with the switch either through OpenFlow channel or Service Insertion tunnels.

Health status	Description
Green	Any one of the conditions is true: • The status of all the VLANs configured on the switch is green
Yellow	• The status of one or more VLANs configured on the switch is not green • One of the VLANs configured on the switch has been disabled from DNS inspection
Grey	• The status of all the VLANs configured on the switch is grey or if the switch is throttled

9.1.3 Checking VLAN status

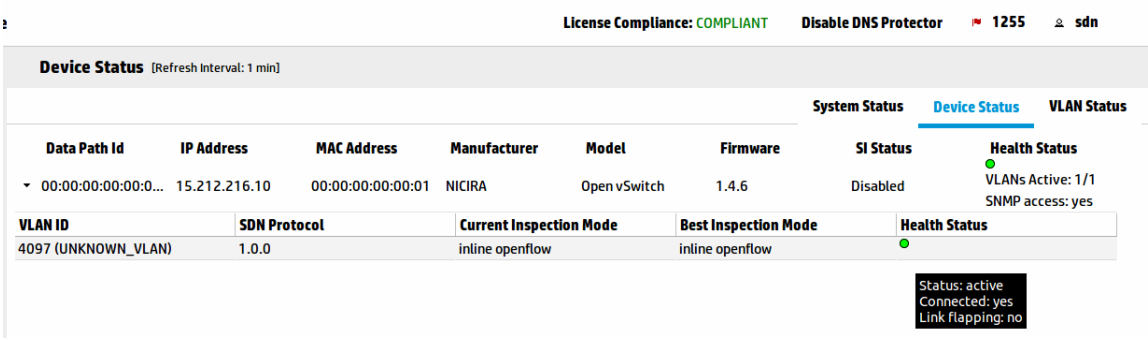
To check the health status of the VLANs configured on the switch, select **Device Status**. Four colors green, red, yellow, and grey display the health status of the VLANs.

1. Select **Device Status** on the console.

   The **Device Status** page displays the list of switches configured.

2. Click the ▸ icon next to the IP address of the switch.

   The list of all the VLANs configured on the switch appears.



3. Hover over the **Health Status** of the switch connection to view the health status of the switch connections configured on the VLAN.

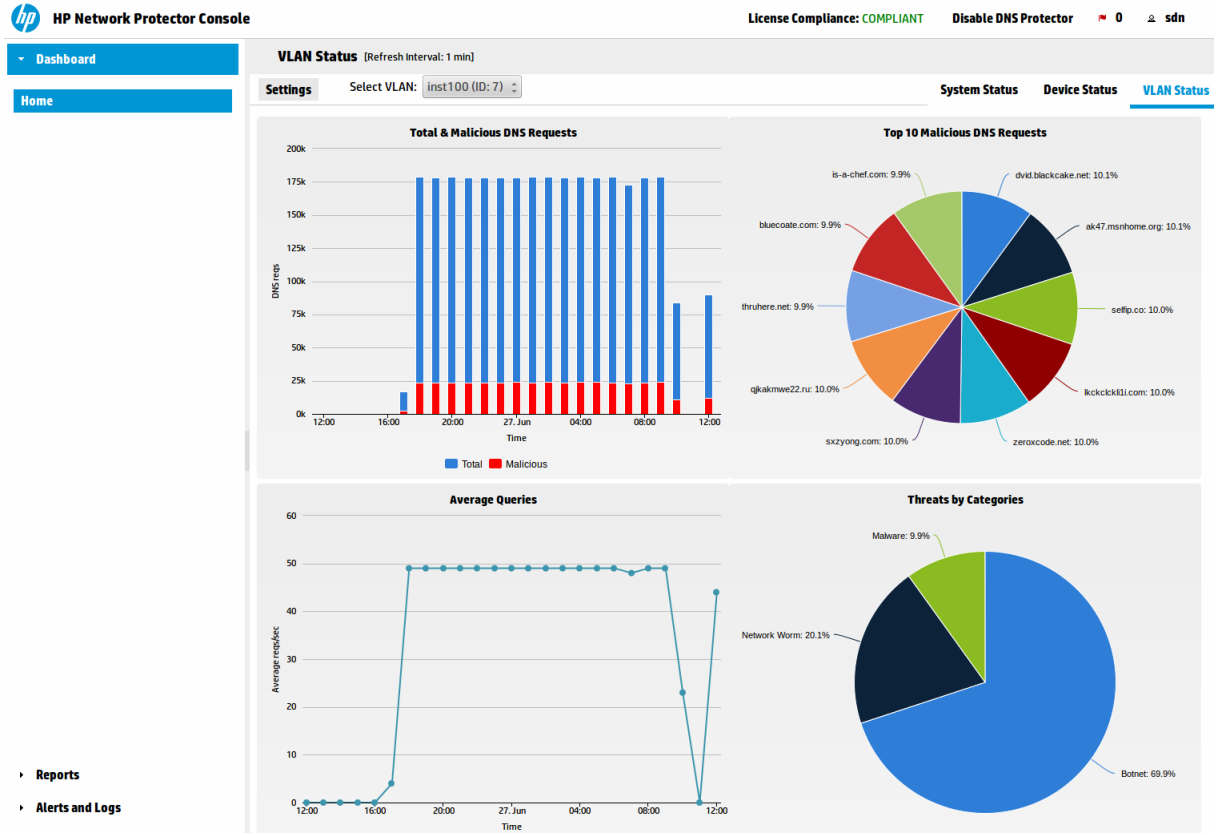
Table 7 Health status of VLANs

Color	Description
Green	All the conditions are true: • The VLAN is active • The VLAN instance is connected • The SNMPv3 credentials to the switch are correct • The VLAN link is stable • The current mode is reported as the maximum mode
Red	Any one of the conditions is true: • The VLAN instance is not active • The VLAN instance is active but not connected • The SNMPv3 credentials to the switch are incorrect or not working
Yellow	Generally indicates Service Insertion tunnel issues and any one of the conditions is true: • The VLAN instance is not active • The link is unstable • The current inspection mode is not the best inspection mode for the connection
Grey	• VLAN has been disabled from DNS inspection

9.1.4 VLAN status

Click **VLAN Status** to view the details of the DNS requests originating from each VLAN.

Figure 24 Example of VLAN status view



The DNS details are represented graphically and provide the details of DNS requests originating from each VLAN configured in the network. You can tune the policies for each VLAN based on the following reports and threat types:

- Total and malicious DNS requests
- The average DNS requests
- The top malicious DNS requests

NOTE: For OVS (Open Virtual Switch) discovered in the application, the VLAN is captured as UNKNOWN_VLAN (4097). No statistics are captured by application for this UNKNOWN_VLAN and the VLAN Status page will not display this VLAN in the VLAN drop down list.

9.1.5 Enabling and disabling a VLAN

You can choose to enable or disable the application on VLANs. When you disable the application on a VLAN, the DNS traffic on the VLAN is not monitored by the application and the traffic flows normally. Disabling the application on VLAN does not affect the configuration and operation of VLAN on the connected switches.

1. Click **VLAN Status** on console page.

   The **VLAN Status** page appears.
2. Click **Select VLAN** drop down list and select the VLAN for which you want to change the status.
3. Select **Device** and select the DPID from the drop down list to disable the selected DPID.

   Or
4. Select **Entire VLAN** to disable the VLAN.
5. Click **Disable** to disable application on the VLAN.

   When the application is disabled on the VLAN, it does not monitor traffic on the VLAN.

9.2 Reports

You can generate reports from the network traffic generated in the system and compiled by the application. These reports detail the total network traffic generated, the threats encountered by the system, and the traffic trends. The application console provides real-time graphical representation of the DNS network statistics. You can use these reports to know the health status of your network and identify the threat perception to the network. You can use the reports to identify any unusual network traffic patterns in the network and take appropriate action.

9.2.1 Type of reports

When you create a report, you select a template and modify its settings. These report templates track all issues, specific threat types, blocked DNS requests, and the top ten malicious DNS requests encountered.

Report type	Description
Total DNS requests	Total number of DNS requests report displays all the DNS requests generated by all the hosts in the network during a particular time interval. This helps you understand the DNS traffic patterns in the network and manage the network traffic based on this report. When the total number of requests is beyond the threshold limit, you can disable application.
Total blocked DNS requests	Total number of DNS requests report displays all the blocked DNS requests by application per unit time.
Top 10 malicious DNS requests	The Top 10 malicious DNS requests report displays information about the most frequent malicious attacks that target your network. The report enables you to determine the type malicious attacks and the behavior of the traffic during detection and block procedures.
Threat type percentages	Threat type percentages report displays the threat types to the network in the form of a percentage. This report enables you to determine the type of threats to the network.
Total malicious DNS requests	The Total malicious DNS requests report displays information about all the attacks that target your network during a particular time interval. The report enables you to determine the type of malicious attacks and the behavior of the traffic during detection and block procedures.
Total malicious end hosts	Total malicious end hosts report display all the end hosts which are making malicious DNS requests and their count during a particular time interval. This report enables you to identify the hosts making the malicious requests.
Top 100 talkers	Top 100 talkers report display all the hosts with their DNS request count which includes good and malicious for the given time. This report enables you to find out network usage by end hosts. This report can be rendered only for three months window. It can be any three months.

9.2.2 Generating reports

To generate reports complete the following steps:

1. Select **Reports→ System**.

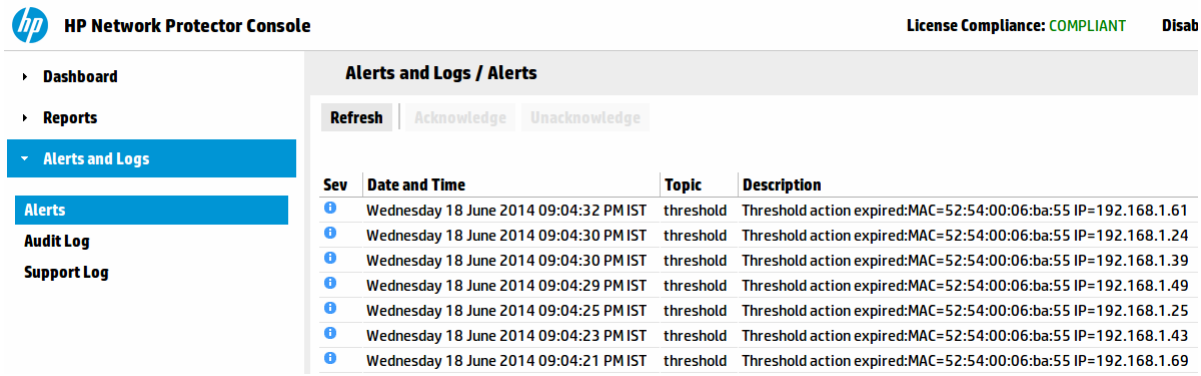
   The **Reports/Systems** page appears.
2. Select the type of report you want to generate from the **Request Category**.
3. From the **Report Type** options, select **Table** or **Graph** option depending on how you want the report rendered.

4. Optional. Select a graph type.
5. Click the **Time Range** to set the duration for which you want to view the reports.
6. Click the **Time Interval** to set the frequency at which you want to generate the reports.
7. Click the **Generate report** to generate the report.
8. Scroll down or click configure **-** icon at the top to view the generated report.

9.3 Alerts

Alerts give notification of internal events that affect the application operation, and in some cases indicate that some action is needed to correct a condition. Alerts also indicate any policy breach or malicious DNS requests from end hosts. The Alerts generated by the administrator, user, or an event are visible in the **Alerts** display.

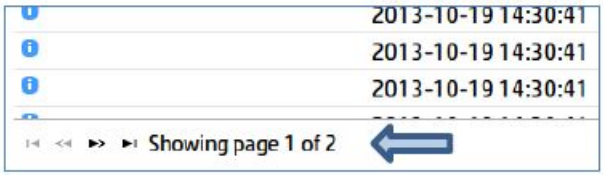
Figure 25 Alerts View

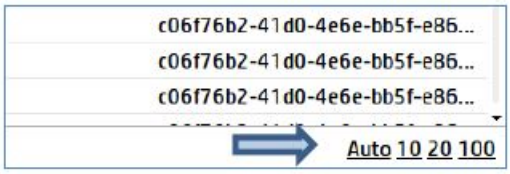


The three alert levels are:

- Informational
- Warning
- Critical

To navigate through the alert listings, use the arrow keys of the alert display. To select the number of alerts to display in a single view, use the options of the alert display. (For listings exceeding the length of the alert display, you can also use the scroll bar on the right side of the view.)





9.3.1 Refresh the Alert Listing

The alert page is a static display and the new alerts do not automatically appear in the **Alerts** view. When you click **Refresh** to refresh the alert page, new alerts appear on the **Alerts** view.

9.3.2 Changing the Display and Alert Listing Order

In the default display shown in Figure 25, alerts are displayed in descending order from newest to oldest, based on the alert date and time. You can change the display order in any of the following ways by clicking on the appropriate column heading:

Column heading	Description
Severity	Groups alerts by alert level; to or the reverse.
Date/Time	Oldest to newest (the default) or the reverse.
Description	Alphabetical or the reverse, by the description of the alert.
Topic	Alphabetical or the reverse, by application function type. Shows the category under which this alert should be considered. Multiple origins can contribute alerts to the same topic.

9.3.3 Acknowledge Alerts

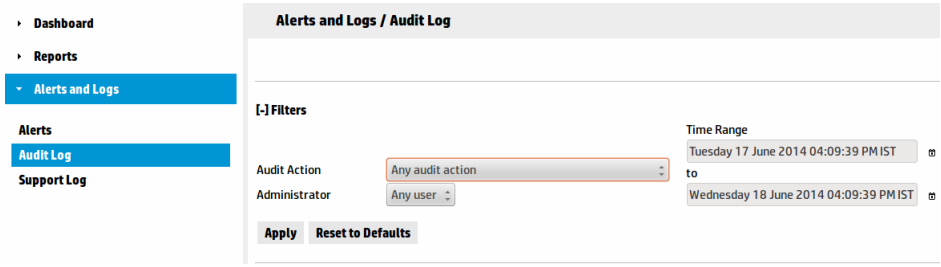
When the application creates an alert, it appears in an unacknowledged state. To acknowledge an alert, click **Acknowledge**. Acknowledged alerts appear greyed-out in the Alerts view. If you want an acknowledged alert to retain prominent visibility, select the alert and click the **Unacknowledge** button to return the alert to an unacknowledged state.

9.4 Audit Log

The audit log records events related to activities, operations, and configuration changes initiated by an authorized user. This includes activities such as:

- Managing users such as creating, deleting, or modifying user privileges.
- Adding, deleting or modifying various Network Protector configurations such as schedules, holidays, SNMP settings, etc.

Figure 26 Selecting the Audit Log

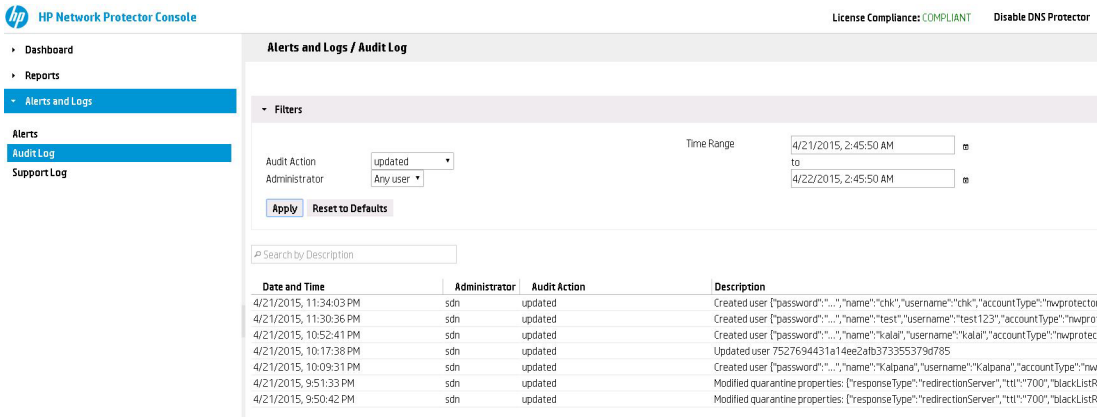


Audit Log data fields include the following:

- **Timestamp**: A time stamp (in UTC format) marking when the controller created the audit log entry.
- **Administrator**: A string representing the user that performed the operation that triggered the log entry.
- **Audit Action**: A string description providing detail about the audit log entry.
- **Description**: A string describing any additional description of the audit action.

For example, the audit log displays modified activity:

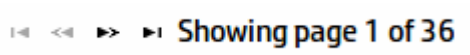
Figure 27 Example of audit log showing modified activity



9.4.1 Manage the Audit Log Display

You can manage the log to analyze the logs better. Use the filters to filter the logs based on the type of action or the user who initiated the action. You can also filter logs generated at a time interval. Filtering the logs helps you narrow down the log entries to manageable numbers to help you analyze the logs for any potential threats and take preventive actions.

The paging information display indicates which page of the log is visible and how many pages of Audit Log entries currently exist.



9.4.2 Setting Audit Log policy

An audit log entry may not be modified or selectively deleted. Entries are removed only as a result of the default age-out policy which is set to 40 days.

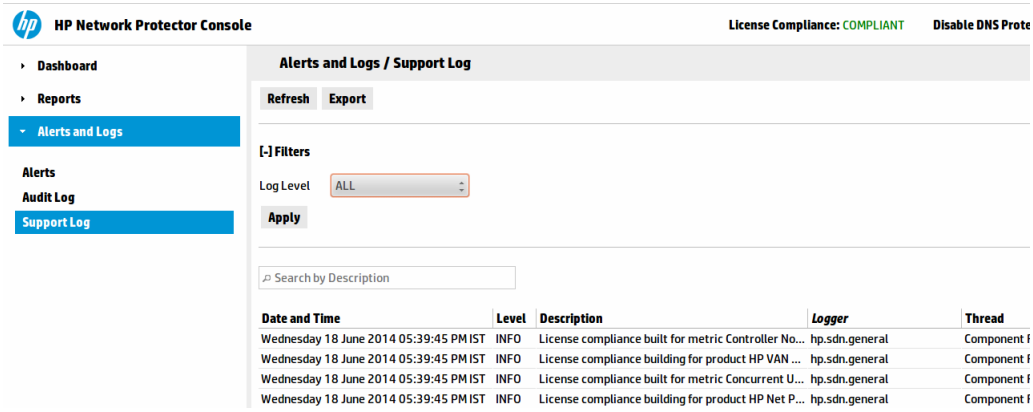
9.4.3 Archiving Audit Log Data outside of the HP Network Protector

To archive the Audit Log data beyond the age-out policy, use the REST API to export the Audit Log data out of the application prior to its age-out date. Exporting Audit Log data does not remove it from persistent storage.

For more information about using REST API to export the Audit Log data, see the *HP VAN SDN Controller Administrator Guide* in the SDN information library.

9.5 Support Logs

The Support Logs function automatically maintains an internal record of events of interest from the operations of the application. This information is the type of data a support engineer would request when troubleshooting application installation.



The application maintains its own support logs. The support logs are disabled by default. You must enable the support log to capture any application errors or issues.

Clicking on the **Refresh** button displays a listing of the most recent log messages, as determined by the currently configured queue size. For example, with a queue size of 100, **Refresh** lists the 100 most recent log messages.

9.5.1 Log Message Levels

Log message levels include the following:

- ERROR
- WARN
- INFO
- DEBUG

In the default configuration, the ERROR, WARN, and INFO levels are recorded in the Support Logs. DEBUG is a verbose logging that is used in troubleshooting situations that may involve support engineering. The logging level for a given component that is writing to the support log can be dynamically changed using the Virgo Administrator console.

9.5.2 Logs and log locations

The logs are saved at the following locations on the Ubuntu server. View the logs for troubleshooting information about the application and the controller. You can download and send the log files to the HP support representative to diagnose and troubleshoot errors.

Log location	Description
/opt/sdn/virgo/serviceability/logs/network-protector.log	View the info log for information regarding the general working of application.
opt/sdn/virgo/serviceability/logs/network-protector-debug.log	View the Debug log for detailed information about issues related to any application malfunction like RepDV download issues, notification sending issues, switch not connecting issues, and generally checking any exception states.
/opt/sdn/virgo/serviceability/logs/packetdaemon.log	View the packetdaemon log for details of the packet demon errors.
/opt/sdn/virgo/serviceability/logs/log.log	View the controller logs for details related to the controller and the switch connection issues. This log also contains information about packet in and packet out issues and the general controller functioning.

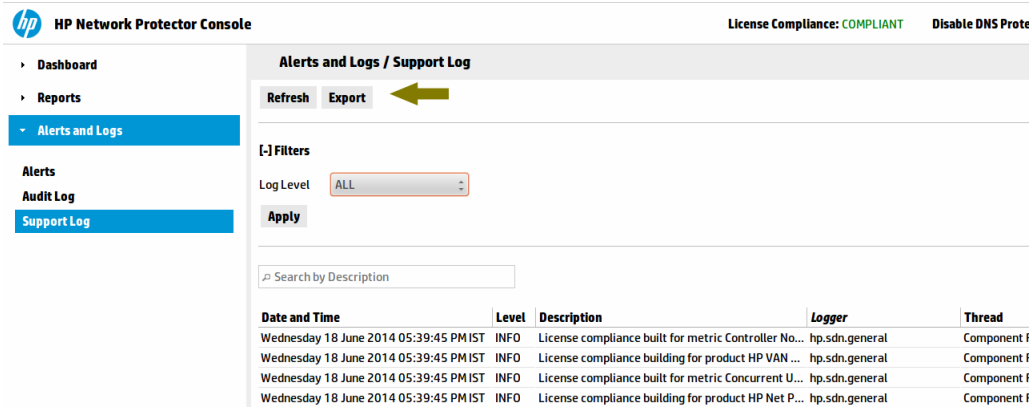
Log location	Description
/opt/sdn/cassandra/log/system.log	View the Cassandra system log for the database logs of application.
/opt/networkprotector/webserver/logs/redirectserver.log	View the redirectserver log for information about the npwebserver process. View this log to debug issues regarding the webserver not installing during the application installation process.

9.5.3 Exporting the Support Logs

The export operation moves the set of application and controller logs from the application (as a compressed file) to the local system running the browser (that is, to the sdn-all-logs.zip file in the directory in which the controller is configured to store downloads). In Ubuntu installations, this is usually the Downloads directory.

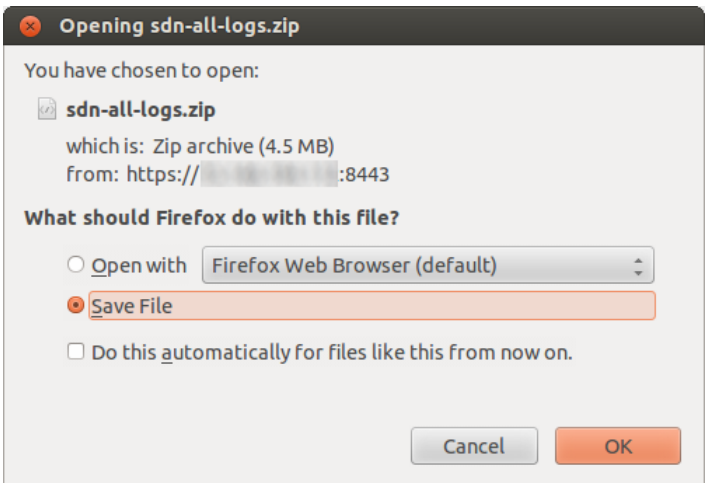
1. To download the support logs, click on the **Export** button.

Figure 28 Exporting Support Logs



The following dialog box appears:

Figure 29 Completion of the Export Operation



2. Select one of the options:
   - Open and view the new log zip file in a browser.
   - Save the log zip file in a default location on your computer.
   - Set the default operation to always open the directory containing the log zip file.
   - Show the log zip file in the default directory for receiving downloads.

NOTE: The actions resulting from these choices are not managed by the application but are a function of the operating system in use.

9.6 Viewing throttler statistics

- Select **Administration** →**Throttler Statistics**.

  The **Administration/Throttler Statistics** page appears. This page displays the number of Top throttled devices

9.7 About policy enforcement settings

When a user tries to access a potentially harmful domain or a webpage, you can configure the policy enforcement settings to one of the following options:

NXDOMAIN	Set this option to send a Non-existent Domain (NXDOMAIN) DNS response to user. By default DNS Response type is set to Non-existent Domain.
Redirection Server	Select the **Redirection Server** option to redirect the host to a known safe site. When you set this option, the application resolves the harmful or malicious domain names to the redirect server IP address. A DNS message with the redirection server IP as a resolved IP for the DNS request is sent back to the user. When the user tries to access the resolved IP address from the browser, the redirect server displays the default webpage. For more information about the default webpage see "Configuring the web server" (page 63).

9.7.1 Configuring the web server

When you install the application, a default redirect web server is installed at the following location

`/opt/networkprotector/webserver`

The default redirect web server service *npwebserver* starts automatically after installation. The web server serves a default page for the browsers accessing malicious websites using either secure (HTTPS) or standard (HTTP) or both (HTTPS & HTTP) the protocol based on the configuration. This server serves requests for both blacklist and greylist. All http requests are serviced at port 80 and the secure https requests are serviced at port 443 which are default ports for http protocol.

Use the following commands to control the *npwebserver* service:

- `service npwebserver start`
- `service npwebserver stop`
- `service npwebserver status`

To configure the redirection server properties, navigate to the following file on the local host on which the application is installed:

/opt/networkprotector/webserver/config/redirectconf.properties

Property	Description	Default value
redirect.listen.http.reqs	Indicates whether the default redirect web server should listen to http requests from client. The web server by default listens to http requests.	True
redirect.http.ip	IP address to which the default redirect web server binds and starts listening to http requests on port 80.	Local host IP address
redirect.listen.https.reqs	Indicates whether the default redirect web server should listen to https requests from client.	False
redirect.https.ip	IP address to which the default redirect web server binds and starts listening to https requests on port 443.	Local host IP address
redirect.webserver.loglevel	Log level which you can set based on the type of information you require in the `redirectserver.log` file. You can set the following values: • ALL • FINE • FINER • FINEST • INFO • SEVERE • WARNING	INFO

NOTE: If you have configured the browser to access a proxy server, then add the controller IP address and the localhost IP address to the **Exceptions** list in the browser proxy setting. When the browser is redirected to the default page on the npwebserver running on the controller, the browser does not access the proxy server to reach the default webpage.

NOTE: Also ensure that the you map the localhost name to its IP address in the `hostname` or `hosts` files in the Ubuntu server where you have installed the application.

The `hostname` or `hosts` files are available at the `/etc` location on the Ubuntu server.

9.7.2 Configuring policy enforcement settings

1. Select **Administration** →**Policy Enforcement Settings**.

   The **Policies/Policy Enforcement Settings** page appears.
2. Click the **Edit** button to edit the policy enforcement settings.
3. Enter the time in seconds in the **TTL (sec)** text box.
4. Select **Non-existent Domain** option to display a message that the domain does not exist.

   Or
5. Select **Redirection Server** option to redirect the host to a known safe site.

   NOTE: By default, the IP address of the local host on which the application is installed is populated for both blacklist and greylist redirection server address text boxes.
6. To change the blacklist redirection address, enter the IP address of the server in the **DNS Blacklist Redirection Server Address** text box.

7. To change the greylist redirection address, enter the IP address of the server in the **DNS Greylist Redirection Server Address** text box.
8. Edit the default message that the web server displays when the user is redirected to the web server in the **Local Redirection Server Message** text box .
9. Click **Save** to save the setting.

9.7.3 Time To Live (TTL) value

The TTL (Time To Live) value is the time the local name resolving servers store records locally before a new copy of the record is retrieved from the DNS server. The record storage is called DNS cache and the act of storing records is called caching. The TTL value limits the lifespan of the DNS response on the client machine. The TTL value is applicable to both NXDOMAIN and REDIRECT responses that are sent by HP Network Protector.

9.7.4 Adding hosts to the ACL

You can add IP addresses on the network to create the ACL (Access Control List). All the hosts on the network can access the IP addresses listed in the ACL even when the they are quarantined. For example, you can add the IP address of the IP phone server to the ACL, so when a host is blocked, the user can still access the IP phone to call the administrator to resolve the issue regarding the blocked host. To add hosts to the ACL, complete the following steps.

1. Select **Administration** →**Policy Enforcement Settings**.

   The **Policies/Policy Enforcement Settings** page appears.

2. Click + icon under **Access Control Configuration** to add the domain name or IP address of the resources that the host can access when it is quarantined.
3. Click ✔ icon to save the list.

9.7.5 Adding hosts to the exception list

You can create an exception list of host IP addresses on your network that must never be blocked or quarantined by the application even if the host IP address appears to have violated threshold limits. Some of the IP addresses you might never want to block or quarantine can be of the middleboxes or network appliance such as firewalls, network address translators, and dedicated middlebox hardware in the network to improve network security and performance. Adding IP addresses to the exception list ensures that the application does not inadvertently block middle boxes in the network.

1. Select **Administration** →**Quarantine & Exception List**.

   The **Administration/Quarantine & Exception List** page appears.

2. Click + icon under the **Exception Users** section to add an IP address.
3. Enter the IP address in the **IP Address** text box and click **OK**.

9.7.6 Deleting hosts from the exception list

1. Select **Administration** →**Quarantine & Exception List**.

   The **Administration/Quarantine & Exception List** page appears.

2. Click **Reset to Defaults** button to release all the hosts in the exception list.
3. To release specific hosts, select the host from the **IP Address** list and click − icon.

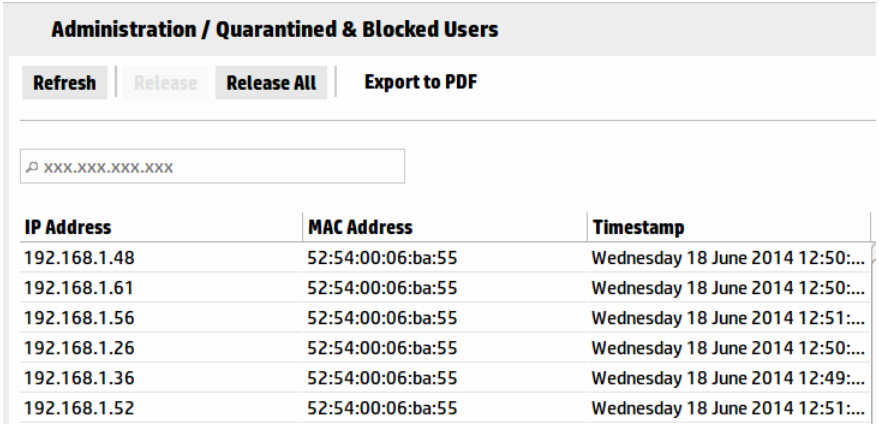
9.8 Releasing quarantined clients

When a client is quarantined, it will be in the quarantine state for the time set in the threshold policies. The top ten quarantined clients are listed in the dashboard and the list is refreshed every

minute. You can release all the clients or few select clients before the set interval. To release the quarantined clients, complete the following steps.

1. Select **Administration** →**Quarantined & Exception List**.

   The **Quarantined & Exception List** page appears:



2. To release select hosts, select the clients and click **Release**.

   Only the selected hosts are released.

3. To release all clients click **Release All**.

   All the quarantined hosts are released.

9.9 Exporting quarantined clients report

Use this report to view all the clients quarantined by the application at any given time. If any client is periodically quarantined by the application, you can examine the client to see if it is affected by malware and isolate the client from the network. You can also use this report to see if any of the middleboxes or network appliance are quarantined. You can add IP addresses of such appliances to the ACL so they are not invariably blocked by the application.

1. Select **Administration** +**Quarantine** →**Quarantined & Blocked Users**.

   In the main application page, the **Quarantined & Blocked Users** appears:

2. Click the **Export to pdf** button to view or save report on any desired location on your machine..

9.10 Notifications

You can configure application to send email notifications of events and alerts to the administrator and other users in the system. The application can also send event notifications to applications such as ArcSight server for viewing and analysis.

9.10.1 Configuring email notifications

Configure the email settings to receive notifications about events related to activities, operations, and configuration changes initiated by an authorized user. You will receive notifications of internal events that affect application operation, and in some cases indicate that some action is needed to correct a condition. You can add multiple email addresses to the list and the notifications are sent to everyone on the list. Along with email notifications, events are logged in the form of Alert log or a Support log or ArcSight log.

Configuring email notification requires two main steps, to configure the email server information and then the email destination address.

1. Select **Administration** →**Notifications**.

   The **Notifications** page appears.

2. Click the **Edit** button to configure the email server options.
3. Enter the email server IP address or the fully qualified domain name (FQDN) in the **Email Server (SMTP)** text box.
4. Enter the email server network port number in the **Email Port** text box.
5. Enable the **Secure Connection for SMTP Server** option if the email server is configured to use secured connection.
6. Enter the email address of the authorized user on the email server in the **HP Network Protector Email Address** text box.
7. Enter the password used on the email server in the **HP Network Protector Email Address** text box.
8. Click the + icon below the **Email Address** to enter the destination email address.
9. Enter the email address you want the email notifications to be sent in the **Email Address** text box and click the ✔ icon to save the email address.

9.10.2 Configuring the HP ArcSight server

The HP ArcSight Security Intelligence platform enables you to collect, analyze, and assess IT security, enterprise security and non-security events for rapid identification, prioritization, and response. You can configure application to log events into the HP ArcSight server.

1. Select **Administration** →**Notifications**.

   The **Notifications** page appears.

2. Click the ✎ icon to the right of **ArcSight** to configure the ArcSight server options.
3. In the **ArcSight domain NameIP Address** text box enter the ArcSight domain nameIP Address.
4. Enter the ArcSight port number in the **ArcSight Port** text box.
5. Select a connection type from the **Connection Type** menu to set the transportation protocol with the ArcSight server.

9.10.3 Configuring HP Intelligent Management Center

You can configure the application to access the IMC UAM module's REST API. The application maps the IP and MAC address of the current users on the network with the information stored on the IMC. When the application sends notification mails and alerts to the administrator, the user details of the corresponding IP and MAC address is sent in the mail. This helps the administrator to identify the user quickly and take necessary action if required. For more information about HP IMC see the *HP Intelligent Management Center v7.0 Basic Platform Software Administrator Guide*.

1. Select **Administration** →**IMC**.

   The **General/IMC** page appears.

2. Click the ✎ icon to configure the IMC server options.
3. Enable **IMC Status**.
4. In the **IMC Server address** text box enter the IMC server domain nameIP Address.
5. Enter the IMC service port number in the **IMC Service Port** text box.
6. Enter the IMC service user name credentials in the **IMC Service Username** text box.
7. Enter the IMC service password credentials in the **IMC Service password** text box.
8. Select the **Require Proxy** option to access IMC server.
9. Click the ✔ icon to save the IMC settings.

9.10.4 Generating license compliance report

Run the license compliance report to determine if the application is optimally licensed. The application saves the license compliance history for last seven days. You can generate and view

compliance reports for the last seven days or choose a date and time interval for which you want to view the report. To generate the report, complete the following steps:

1. Click 

on the application console.

   Or

   Select **Administration** →**License Compliance**.

   The **License Compliance** page displays the current license compliance summary.
2. From the **Compliance History** section, select the date and time interval for which you want to generate the report and click **Render report**.

   The report is generated in the pdf file format.
3. [Click the download button to download and save the report.]

9.10.5 Enable or disable Service Insertion globally

You can choose to enable or disable Service Insertion for the entire application. When you enable or disable Service Insertion globally, the information is persisted and the application retains the same state until you change the state manually.

The following table describes the difference between enabling or disabling Service Insertion globally.

Enable Service Insertion globally	Disable Service Insertion globally
• It enables Service Insertion for all the devices on the network. • The Service Insertion tunnel is created between the switch and the controller NIC you specified. • DNS divert rule is pushed for all the associated datapaths of the switch which is negotiated to Openflow 1.3 to use the newly created tunnel. • For the devices which are discovered after global Service Insertion is enabled, the Service Insertion tunnels are created between the switch and the controller NIC you specified. • If none of the controller NIC is specified and the value is set to **Default**, then the data movement from the switch to the controller is through Openflow.	• It disables Service Insertion for all the devices on the network. • All the previously created tunnels between switches and controller will be destroyed. • DNS divert rule is pushed for all the associated datapaths of the switch which is negotiated to openflow 1.3 to use Openflow channel. • For the devices which are discovered after global Service Insertion option is disabled, Service Insertion tunnels are not created, even though the switch is capable of creating Service Insertion tunnels.

9.10.6 Enabling or disabling Service Insertion globally

1. Select **Administration** →**Service Insertion Tunnel**.

   The **Administration/Service Insertion Tunnel** page appears.
2. Select **Enable** or **Disable** to enable or disable Service Insertion on the network.

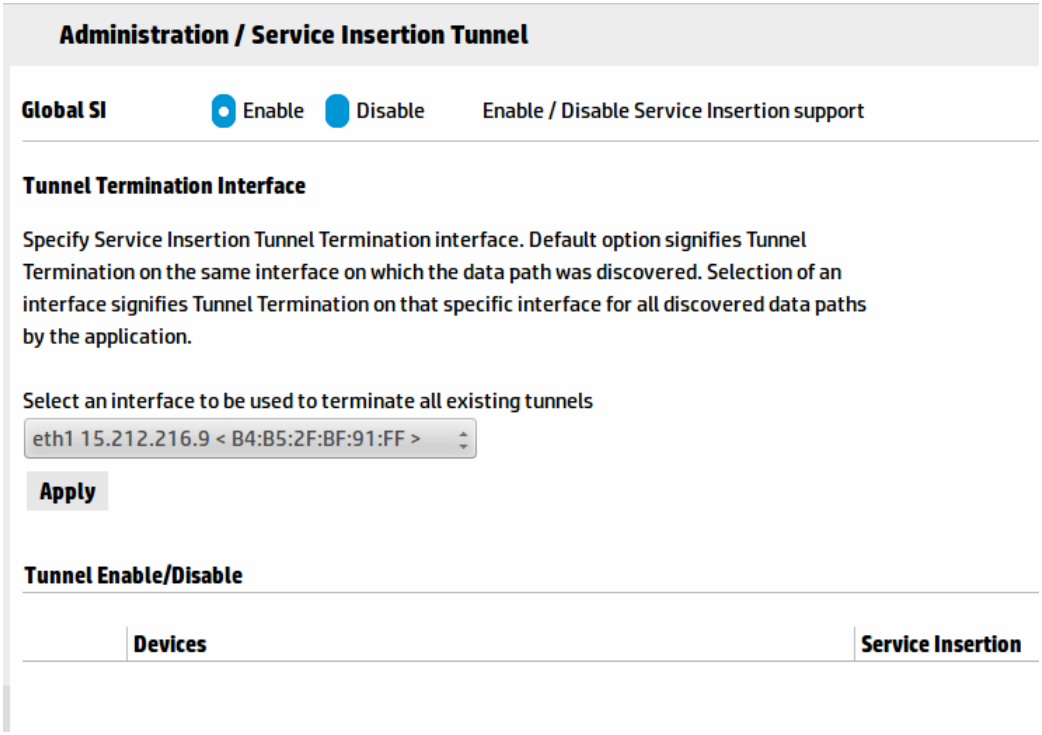
9.10.7 Selecting the controller NIC

Service Insertion is to create and manage a tunnel between the switches and the controller. The tunnel is created with one terminating end as the switch and the other terminating end as the controller's NIC. The tunnel is used for the DNS traffic between the controller and the switch.

When an application is installed for the first time the default NIC will be selected. You can select a specific NIC for Service Insertion tunnel termination in case the controller has more than one NIC. For example, if the controller has multiple bandwidth NICs, such as 1 gigabit and 10 gigabit, then you can select 10 gigabit NIC for tunnel termination for greater efficiency and throughput. The tunnel termination NIC selection is persisted even after you restart the controller and the selected NIC remains as the tunnel termination endpoint.

IMPORTANT: After you select the NIC, you must ensure the switch is reachable from the selected controller NIC. If the switch is not reachable, then Service Insertion tunnels are not created and the datapaths are moved to Openflow channel.

Figure 30 Selecting controller NIC



9.10.8 Enable or disable Service Insertion on a device

You can choose to enable or disable Service Insertion on a switch or multiple switches. When you disable Service Insertion on a switch then the DNS traffic between the controller and switch is through Openflow. When you enable or disable Service Insertion on a switch, the information is persisted even after you start the controller again.

IMPORTANT: After you enable Service Insertion on a switch, you must ensure the switch is reachable from the controller termination NIC. If the switch is not reachable, then Service Insertion tunnels are not created and the datapaths are moved to Openflow channel.

The following table describes the actions that occur in the network when you enable or disable the Service Insertion on a switch.

Enable Service Insertion	Disable Service Insertion
Before you enable Service Insertion on a switch, the Service Insertion must be disabled. • This will enable Service Insertion on the selected devices. • This will create Service Insertion tunnel from the switch and the Controller with the termination NIC provided by Tunnel Termination NIC, if there is no NIC selected, then it would take the NIC to be default. • If the tunnel creation is successful, then DNS divert rules will be pushed for the associated datapath's for the	Before you disable Service Insertion on a switch, the Service Insertion must be already enabled. • This will disable Service Insertion tunnels on the device. • For all the datapaths associated to the switch, which are negotiated to openflow 1.3, DNS divert rule will be pushed to use openflow channel. • The Service Insertion tunnel existing between the controller and the switch will be destroyed.

Enable Service Insertion	Disable Service Insertion
switch which are negotiated to openflow 1.3 to use the newly created tunnel. • If tunnel creation fails for any reason, the switch will remain in the openflow channel itself.	

10 Backing up and restoring the application

10.1 Backup process

You cannot back up and restore the application separately. When you back up the controller, the application is backed up along with the controller. To back up the application, follow the same process as backing up the HP VAN SDN Controller. For more information about backing up HP VAN SDN Controller, see the *HP VAN SDN Controller Administrator Guide* in the SDN information library.

10.2 Restoring the application

The restore process of application is not exactly the same as restoring controller. After you start the restore process, complete the following steps.

1. Uninstall the application.
2. Complete the following initial HP VAN SDN Controller restore steps.
   a. Uninstall the controller.
   b. Set CTL_RESTORE_INSTALL_MODE=True
   c. Reinstall the failed controller.
3. Install the application. For more information about installing application, see the *HP Network Protector SDN Application Installation Guide* in the SDN information library.
4. Continue and complete the remaining HP VAN SDN Controller restore steps.

IMPORTANT: If you restore HP VAN SDN Controller without installing application, then HP Network Protector SDN Application packet daemon and other files outside the /opt/sdn directory structure will not be restored.

10.3 Saving the application configuration settings

There might be instances where you want to save the various configuration settings of the application, such as:

- When migrating the application to a new machine.
- When installing the application again on the same machine.

Use the `npConfig` shell script to capture the configuration setting. The `npConfig` script backs up only those configurations which do not involve any authentication, such as:

- Profiles – Holidays, Schedules, RepDV Filters, VLAN Groups, Custom Lists Policies
- Administration – Exception List, Policy Enforcement Settings, ACL Manager settings
- Notifications – Email Addresses (and not Email configurations), ArcSight Configuration, Log Configuration
- Global Service Insertion and Disable or Enable DNS Protector status

The `npConfig` script does not back up the following configurations which involve authentication process:

- SNMP, Users, IMC Configuration, Account Settings

10.3.1 Prerequisites

Before you run the `npConfig` script, use the system command `apt-get` to install the curl, zip, unzip, and python Linux packages on the terminal.

Example 6 Command to install curl package

```
sudo apt-get install curl
```

10.3.2 Running the npConfig script

Ensure that you have root access on the Ubuntu system (sudo).

1. From the Ubuntu terminal, navigate to the location where you saved the `npConfig` script and enter the following command to capture the configuration details:
   `sudo ./npConfig --snapshot --dir <absolute path of dir to store the snapshot file> --name <name of the snapshot file>`
2. Enter your Network Protector credentials when prompted.

   The `npConfig` script starts the capture process. Depending on the size of the data, the time to capture the configuration settings may vary. For large data, the time taken might be longer.
3. After the `npConfig` script captures the configuration details, ensure that the backup file is available in the specified directory.

Example 7 To save the backup file at specified location

```
sudo ./npConfig --snapshot --dir /home/sdn/npsnapshots --name npSnapshot04142015
```

In this example the backup file will be stored at /home/sdn/npsnapshots/npSnapshot04142015.zip

Example 8 To save the backup file at default location

```
sudo ./npConfig --snapshot
```

In this example the configuration settings file will be stored at default location, where /opt/ is default location and `np-snapshot.zip` is the default filename.

10.4 Restoring the application configuration settings

Use the same `npConfig` shell script to restore the application configuration settings. Before you run the `npConfig` script, ensure that you have root access on the Ubuntu system (sudo). All other prerequisites to use the `npConfig` script to restore the settings is the same.

1. From the Ubuntu terminal, navigate to the location where you saved the `npConfig` script and enter the following command to restore the snapshot:
   `sudo ./npConfig --restore --file-path  <absolute path of the snapshot file>`
2. Enter your Network Protector credentials when prompted.

   The `npConfig` script starts the restore process. Depending on the size of the data, the time it takes to restore the configuration settings may vary. For large data, the time taken might be longer.

Example 9 To restore the configuration settings

```
sudo ./npConfig --restore --file-path /home/sdn/npsnapshots/npSnapshot04142015.zip
```

11 Troubleshooting the application

11.1 Basic troubleshooting techniques

The application has various troubleshooting tools you can use to resolve issues. By following a combined approach of examining screens and logs, you can obtain a history of activity and the errors encountered.

- The audit log displays a log of all changes made on the application, whether user-initiated or application-initiated.
- The support log displays a log of all events of interest generated from the working of the application.
- You can gather logs and other information required for debugging and analysis.

For more information

"Logs and log locations" (page 61)
"Exporting the Support Logs " (page 62)

11.2 Service Insertion tunnels are down

Symptom

When you disable and again enable the application from the HP VAN SDN Controller UI, the *Service Insertion* tunnels between the switch and the application is down and the packet inspection is through the OpenFlow mode.

For more information about device status, see "Checking VLAN status" (page 54)

Action

Enter the following command `# service sentunneld restart` to restart sentunneld service from the Ubuntu terminal.

11.3 npwebserver process fails to start during installation

Symptom

When installing the application, the following error appears:

```
Service 'npwebserver' failed to start...

Check redirect webserver log
'/opt/networkprotector/webserver/logs/redirectserver.log' for more
information.
```

Cause

This error occurs because the npwebserver process is already running on ports 80 or 443. You must first stop and start the npwebserver process before you restart the installation process.

Action

Navigate to the `/opt/networkprotector/webserver/logs/` location and view the `redirectserver.log` file to verify that the npwebserver process is running on port 80 or 443.

The following messages is logged by the application in the `redirectserver.log` file.

```
SERVER: Address already in use, try stopping the process holding port
80 or 443 and restart service - Address already in use
```

To stop and start npwebserver, navigate to the location where webserver is installed on the Ubuntu server and enter the following command:

```
/opt/networkprotector/webserver
```

```
service npwebserver stop
service npwebserver start
```

11.4 Application is not monitoring the DNS traffic

Symptom

- Switch is not registered in the Device Panel.
- No activity observed on the Application user interface after the installation.

Cause

After you install the application, the controller service has not started on port 6633 because a different process is already running

Action

1. Shutdown the process running on port 6633.
2. Restart the Controller and the application.

11.5 I can access a website even when it is on the blacklist

Symptom

I can access a website even when it is on the blacklist.

Cause

When you access a website from a browser, the HTTP request is directed towards the proxy server depending on the browser settings. The DNS requests are not processed by the DNS server.

Action

Configure the Proxy Access Control (PAC) file to direct the HTTP requests from the web browsers to the DNS server. To set up the PAC file, locate the PAC file on your system and complete the following steps.

1. Find the function `FindProxyForURL function` in the file.
2. Update the file to direct the HTTP requests to the DNS server.

Sample code

```
//Define Sentinel Proxy
var sentinel_proxy = "PROXY 180.44.200.61:8080;DIRECT";
function FindProxyForURL(url, host){
// Define Conditions for Local Networks whose hosts are
queried direct
if (
isInNet(host, "10.181.1.0", "255.255.255.0") ||
isInNet(host, "10.181.2.0", "255.255.255.0") ||
isPlainHostName(host) ||
localHostOrDomainIs(host, "127.0.0.1") ||
dnsDomainIs(host, ".sentinel.net")
)
return "DIRECT";
// Define Conditions for Sentinel Protected Networks
```

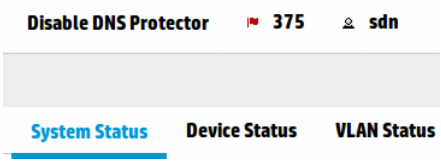
```
if (
isInNet(myIpAddress(), "10.181.3.0", "255.255.255.0") &&
isResolvable(host)
|| isInNet(myIpAddress(), "10.181.4.0", "255.255.255.0") &&
isResolvable(host)
|| isInNet(myIpAddress(), "10.181.5.0", "255.255.255.0") &&
)
return(sentinel_proxy)
} //End FindProxyForURL()
```

For more information about PAC files and supported browser information see http://findproxyforurl.com/browser-support/

11.6 Disabling HP Network Protector SDN Application

Occasionally it might be useful to disable the application to determine the source of a problem in a multi application environment.

To disable the application, click **Disable DNS Protector**



on the application console.

11.7 Disabling the application for a specific VLAN or device

Occasionally it might be useful to disable the application for specific VLANs or devices to help you determine the cause of an issue. To disable the application for a specific VLAN:

1. From the application console, select **VLAN Status**.
2. Select the VLAN you want to exclude from the application and click **Enable or Disable VLAN DNS**.

   The application displays the **Enable or Disable VLAN DNS** dialog box.
3. Select either **Device** or **Entire VLAN** and click **Disable VLAN**.

11.8 Troubleshooting user accounts

11.8.1 Cannot log on to the application

Symptom

I cannot log on to the application.

Solution 1

Cause

Each user is authenticated on login to the application by the authentication service that confirms the user name and password. The username or password you entered is incorrect.

Action

1. Enter the correct username and password.
2. Click **OK**

Solution 2

Cause

The application is not installed on the recommended version of operating system.

Action

1. Check and ensure you are have installed the application on the recommended version of operating system.

11.9 Troubleshooting licensing

11.9.1 Licensing numbers appear to be inaccurate

Symptom

Recently added or assigned licenses are not reported in the controller user interface

Cause

The license screen is not up to date.

Action

Refresh the browser screen for the licensing information to display recent changes.

11.10 Troubleshooting RepDV database issues

Symptom

The **Databases→Overview** screen shows a status of `Unsuccessful` for **Last Check for TippingPoint Database Update**.

Solution 1

Cause

The Tipping Point Database fails to update

Action

The Tipping Point Database update failed either during initial complete update or during subsequent partial updates. When either of the updates fail, start the full update using the following curl command:

NOTE: Starting a full update operation does not disable subsequent partial updates. You can modify the update interval of partial updates from the Database overview page of Network protector GUI.

```
curl --noproxy <IP_address> --header "X-Auth-Token: session token"
--header "Content-Type:application/json" -iksS --request POST --url
"https://ip_addr:8443/sdn/networkprotector/v1.1/database/action"
--data-binary full
```

The following sample response for the curl command is displayed:

```
HTTP/1.1 202 Accepted
Server: Apache-Coyote/1.1
Location: /database/1403154531784
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, PUT, HEAD, PATCH
Access-Control-Allow-Headers: Content-Type, Accept, X-Auth-Token
```

```
Content-Length: 0
Date: Thu, 19 Jun 2014 05:08:51 GMT
```

From the response body, copy the UniqueID generated for the update operation. For example, in the above mentioned response body, UniqueID is *1403154531784*. Use this ID to verify the status of update operation.

Enter the following command to verify the update status of the TippingPoint database:

```
curl --noproxy <IP_address> --header "X-Auth-Token: session token"
--header "Content-Type:application/json" -iksS --request GET --url
"https://ip_addr:8443/sdn/networkprotector/v1.1/database/1403154531784"
```

Example response for the curl command as shown is displayed:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, PUT, HEAD, PATCH
Access-Control-Allow-Headers: Content-Type, Accept, X-Auth-Token
Content-Type: text/plain
Transfer-Encoding: chunked
Date: Thu, 19 Jun 2014 05:10:04 GMT
{"status":"Update under progress"}
```

The Status of the update operation can be any one of the following:

- Update under progress
- Failed
- Completed successfully

In the sample code, the status of the update process is *under progress*.

The following table lists the status and the corresponding response codes of the update operation.

Table 8 Update status code

Status	Response Code
Accepted (Normal)	202
OK (Normal)	200
Bad Request (Error)	400
Unauthorized (Error)	401
Forbidden (Error)	403
Server Error (Error)	500
Service Unavailable (Error)	503

Solution 2

Cause

The proxy settings for the application are incorrect.

Action

1. Check and update the proxy settings for the application.
2. View network-protector.log and network-protector-debug.log to gather issue details.

11.11 Troubleshooting switch connection issues

11.11.1 Switch connection is not showing as registered in the HP VAN SDN Controller

Symptom 1

Health status of the switch connection is grey.

Solution

Cause

The VLAN instance is not active

Action

1. Check the HP VAN SDN Controller OpenFlow Monitor and check whether the switch is listed.
2. If the switch is listed in HP VAN SDN Controller, but not in the application **Device status** tab, check the SNMPV3 credentials.
3. Delete and add the SNMPV3 credentials in the application.

Symptom 2

You see the device listed in the HP VAN SDN Controller (OpenFlow monitor tab) but you do not see the same device listed in the application's device status tab.

Solution

Cause

SNMPv3 credentials setup issue on the switch or SNMPv3 credentials for the switch does not match the credentials configured in the application.

Action

Check the SNMPv3 credentials on the switch.

An example of the running configuration snippet is shown below:

```
snmpv3 enable
snmpv3 group managerpriv user <user> sec-model ver3
snmpv3 user "initial"
snmpv3 user <user>
```

Symptom 3

Health status of the switch connection is yellow.

Solution 1

Cause

The SNMPv3 credentials for the switch do not match the credentials configured in the application.

Action

1. Check the switch SNMPv3 credentials on the switch
2. Verify that the same credentials are set on the SNMP tab

Solution 2

Cause

Switch connection configured to use a tunnel but the senttunneld service is not running.

Action

1. From the Ubuntu terminal, enter the following command to check the status: `# service sentunneld status`

   The sentunneld service status must be either started or running
2. Start the sentunneld service, if the service is not running
3. From the Ubuntu terminal, enter the following command to start the service: `# service sentunneld start`

Solution 3

Cause

The firmware version on the switch is not KA.15.15 or WA.15.15 and the OpenFlow version is not 1.3.

Action

1. From the switch terminal, enter the following command: `show version`
2. From the switch terminal, enter the following command: `show openflow instance Datapath`

   Update the firmware or the OpenFlow version on the switch

Solution 4

Cause

Switch connection is configured to use a tunnel but the Service Insertion tunnel is down.

Action

1. Check whether the heartbeat packet is transmitted between the switch and the application
2. From the switch terminal, enter the following command more than once: `show interfaces tunnel type intercept statistics`
3. The heartbeat packet must increment if the tunnel is up, indicating that the switch and the application are communicating with each other
4. View network-protector.log for more information on the working of the tunnel
5. Use a packet analyzer such as WireShark Capture to analyze the heartbeat packets

Solution 5

Cause

Switch is a modular switch and has both V1 and V2 modules. Only V2 modules support Service Insertion tunnels

Action

1. From the CLI, enter the command `no allow-v1-modules`.
2. From SNMPv3, set hpSwitchAllowV1Modules to false.
3. From the switch terminal, enter the following command: `getMib hpSwitchAllowV1Modules.0` and the result should be 2.

For more information

"Device status panel" (page 53)

Symptom

The application does not recognize any switch.

Solution

Cause

Provision switches are running on software version K/KA/WB.15.14.yyyy

Action

Configure SNMP settings for Provision switches (software version K/KA/WB.15.14.yyyy):

- Read-only access to the device
- Enabled SNMP v1/v2 support

To enable these settings, enter the following on the switch:

```
(config)#  snmp-server community "public" operator
(config)#  no snmpv3 only
```

11.11.2 Switching off V1 module in a mix of V1 and V2 modules on Provision OS

When the application detects a device that is capable of starting Service Insertion but has V1 modules, a Service Insertion tunnel fails to establish and the application will fallback to using OpenFlow.

To enable Service Insertion, turn off V1 module. You can turn off V1 module from the CLI or through SNMPv3.

- From the CLI, enter the command `no allow-v1-modules`.

  The V1 modules are disabled and are not operational.

OR

1. From SNMPv3, set hpSwitchAllowV1Modules to false.
2. To confirm the status, enter the following command from the switch terminal: `getMib hpSwitchAllowV1Modules.0`

   The output must be 2.

11.11.3 Gathering information from switches

Use the following switch commands to gather switch information.

Command	Description
`show openflow`	To view the various OpenFlow instance, OpenFlow instance version, their state, their flow rules, and location
`show openflow instance_name`	To view the details of the OpenFlow instance
`show openflow instance_name flows`	To view the flows present for the given OpenFlow instance in the switch
`show running-config`	To view the running configuration, the OpenFlow instance, VLAN, and controller configuration on the switch
`debug openflow errors|events|instance|packets`	To view OpenFlow protocol packets or event description
`openflow instance instance_name disable|enable`	To enable or disable a specific OpenFlow instance

The OpenFlow instance flows can also be seen in the VAN SDN Controller GUI under **Openflow Monitor →DPID→ Flows**.

12 Support and other resources

To learn how to contact HP, obtain software updates, submit feedback on documentation, and locate links to HP SDN websites and other related HP products, see the following topics.

12.1 Gather information before contacting an authorized support representative

If you need to contact an authorized HP support representative, be sure to have the following information available:

- If you have a Care Pack or other support contract, either your Service Agreement Identifier (SAID) or other proof of purchase of support for the controller and any HP SDN applications
- The HP VAN SDN Controller version and installed licenses
- The HP SDN application product names, versions, and installed licenses
- If you use a virtual machine for the operating system, the hypervisor virtualization platform and version
- Messages generated by the controller and applications
- Other HP or third-party software in use

12.2 How to contact HP

- See the Contact HP Worldwide website to obtain contact information for any country:
  http://www.hp.com/go/assistance
- See the contact information provided on the HP Support Center website:
  http://www.hp.com/go/hpsc
- In the United States, call +1 800 334 5144 to contact HP by telephone. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, conversations might be recorded or monitored.

12.3 Get connected to the HP SDN online user forum

The HP SDN community forum interactive online forum enables you to share your experiences and pose and answer questions related to using the HP VAN SDN Controller and SDN applications.

To join the discussion, see:

http://www.hp.com/networking/sdnforum

12.4 Software technical support and software updates

HP provides 90 days of limited technical support with the purchase of a base license for the HP VAN SDN Controller.

Some HP SDN applications have a trial period, during which limited technical support is provided for 90 days. Other HP SDN applications do not have a trial period and you must purchase a base license for the application to receive 90 days of limited support. Support for the controller and each HP SDN application is purchased separately, but you must have a base license for the controller to receive support for your licensed HP SDN application.

- For information about licenses for the controller, see the *HP VAN SDN Controller Administrator Guide* in the SDN information library at http://www.hp.com/go/sdn/infolib.
- For information about licenses for HP SDN applications, see the information about licensing in the administrator guide for the application.

12.4.1 Care Packs

To supplement the technical support provided with the purchase of a license, HP offers a wide variety of Care Packs that provide full technical support at 9x5 or 24x7 availability with annual or multi-year options. To purchase a Care Pack for an HP SDN application, you must have a license for that application and a license for the controller.

For a list of Care Packs available for the controller and HP SDN applications, see:

http://www.hp.com/go/cpc

Enter the SDN license product number to see a list of Care Packs offered.

Once registered, you receive a service contract in the mail containing the customer service phone number and your Service Agreement Identifier (SAID). You need the SAID when you phone for technical support.

To obtain full technical support prior to receiving the service contract in the mail, please call Technical Support with the proof of purchase of the Care Pack.

12.4.2 Obtaining software updates

The software for the HP VAN SDN Controller and HP SDN applications can be downloaded for free from the HP Networking support lookup tool:

http://www.hp.com/networking/support

This website also provides links for manuals, electronic case submission, and other support functions.

12.4.3 Warranty

For the software end user license agreement and warranty information for HP Networking products, see http://www.hp.com/networking/support.

12.5 Related information

Documentation

- HP SDN information library
  http://www.hp.com/go/sdn/infolib

Product websites

- HP Software-Defined Networking website:
  - Primary website:
    http://www.hp.com/go/sdn
  - Development center:
    http://sdndevcenter.hp.com
  - User community forum:
    http://www.hp.com/networking/sdnforum
- HP Open Source Download Site:
  http://www.hp.com/software/opensource
- HP Networking services website:
  http://www.hp.com/networking/services

13 Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hp.com). Include the document title and part number, version number, or the URL when submitting your feedback.

Glossary

API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
BYOD	Bring Your Own Device
CEF	Common Event Format
CLI	Command Line Interface
DNS	Domain Name System
HTTP	Hyper Text Transfer Protocol
IMC	Intelligent Management Center
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
MAC	Media Access Control Address
MSM	Multiservice Mobility Controller
MTM	Mobility Traffic Manager
NAT	Network Address Translation
PAC	Proxy Auto Config
PVOS	ProVision Operating System
Rep DV	Reputation Digital Vaccine
REST	Representational State Transfer
SDN	Software Defined Networking
SNMPv3	Simple Network Management Protocol Version 3
TCP	Transmission Control Protocol
TMC	Threat Management Center
UAM	User Access Management
UDP	User Datagram Protocol
VAN	Virtual Application Network
VLAN	Virtual Local Area Network
VSC	Virtual Service Communities

Index

A

adding
  administrator, 33
  user, 33
alerts, 33
application console, 31
ArcSight CEF Logger
  overview, 10

C

commands
  switch information, 80
configuring
  controller NIC, 38
  general policy, 47
  link aggregation, 38
  policy enforcement settings, 64
  redirect web server, 63
  switch NIC, 38
contact HP, 81
controller
  application components, 35
  overview, 8
creating
  VLAN group, 41

D

debug log, 36
deployment
  aggregate approach , 12
  DNS inspection approach, 16
  edge routing approach, 15
  examples, 11
  fuzzy edge approach, 14
  instance approach, 11
  MSM wireless approach, 17
  stacked switch, 18
documentation
  providing feedback on, 83

F

forum
  user community, 81

G

general policies
  overview, 46
group policies
  overview, 43
grouping VLANs, 41

H

heartbeat manager, 35
HP
  contacting, 81
HP Intelligent Management Center
  overview, 10
HP Network Protector
  overview, 7
HP SDN information library, 82
HP TippingPoint RepDV Cloud Service
  overview, 9
HP VAN SDN Controller
  overview, 8

I

Inspection Service, 9
instance approach
  deployment, 11

L

license
  activation, 21
  compliance, 33
  grace allowance, 21
  overview, 20
  product key, 21
  registration, 21
  transfer , 25
link aggregation, 9, 38

O

online user forum, 81
OpenFlow enabled switches
  overview, 8

R

releasing
  quarantined clients, 65
report
  quarantined clients, 66
rule refresher, 35

S

Service Insertion
  overview, 9
service manager, 36
stacked deployment
  data port, 19
  OOBM port, 19
stacked switch deployment, 18

T

throttle manager, 36
transfer
  license, 25
transport manager, 37
troubleshoot
  licensing, 76
  switch connections, 78
  user settings, 75

TTL, 65

U

user community
  online forum, 81

V

verifying
  link aggregation, 39

W

website
  documentation, 82
  HP SDN community forum, 81
  HP VAN SDN Controller, 82