LANGuardian Integration Guide

LANGuardian V14

This document describes how to integrate LANGuardian with 3rd party systems.

Author: Morgan Doyle

Revision information: 1.4 Draft

© NetFort Technologies Limited 2018. All rights reserved.

Table of Contents

1 LANGuardian Integration

LANGuardian integrates with 3rd party systems by exporting data. LANGuardian does not import data from 3rd party systems and does not support remote configuration.

LANGuardian can export data in two ways:

- Query of LANGuardian using REST API
- LANGuardian export of (northbound) events via Syslog

This document describes how to configure and use APIs to achieve integrations using both techniques.

2 REST API

The LANGuardian REST API allows any system or application to make http/https requests to query LANGuardian. The LANGuardian REST API provides access to all the data in the LANGuardian database, by way of executing of any of the LANGuardian reports. The REST API can access any of the default reports that LANGuardian is shipped with, as well as any custom reports defined by the administrator. The REST API does not provide direct access to the database (for example, there is no table export function).

If the system or application querying LANGuardian has appropriate privilege, LANGuardian executes the requested report and returns the results in CSV, HTML or JSON format as specified.

The guide describes four different usage models with examples. They are

- CSV
- IFRAME
- SolarWinds Orion Integration
- Excel (data from web)

2.1 Privileges, username and passwords

To bypass the authenticaion page when accessing reports on LANGuardian, it is neccessary to embed a username and password in the REST API request URL. Netfort recommend that the Administrator should create a user profile on LANGuardian (call the account RESTAPI say) and give this profile access to all reports. Use this username and password instead of entering the Administrator username in embedded reports.

DRAFT

2.2 Exporting database tables

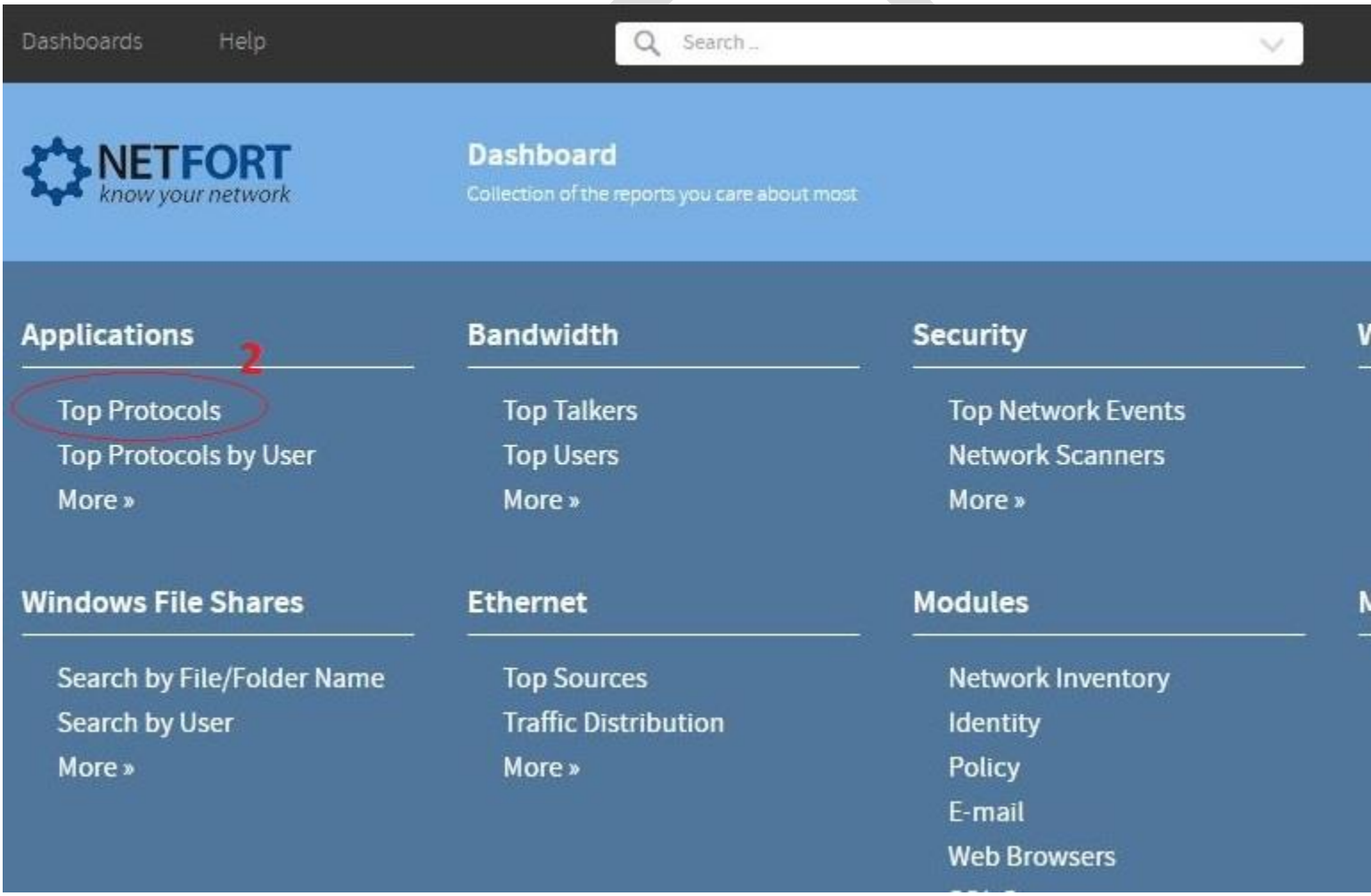
[TBA. Note on the new database tables export in the RID range 1000-1100]

2.3 CSV (Coma Separated Value)

The REST API CSV output format is useful for scripts that need to access information from LANGuardian for further processing. To help with creating scripts the LANGuardian report GUI page has a drop down menu that generates shell script syntax for using wget to run reports.

To use the REST API format, use the following steps as an example.

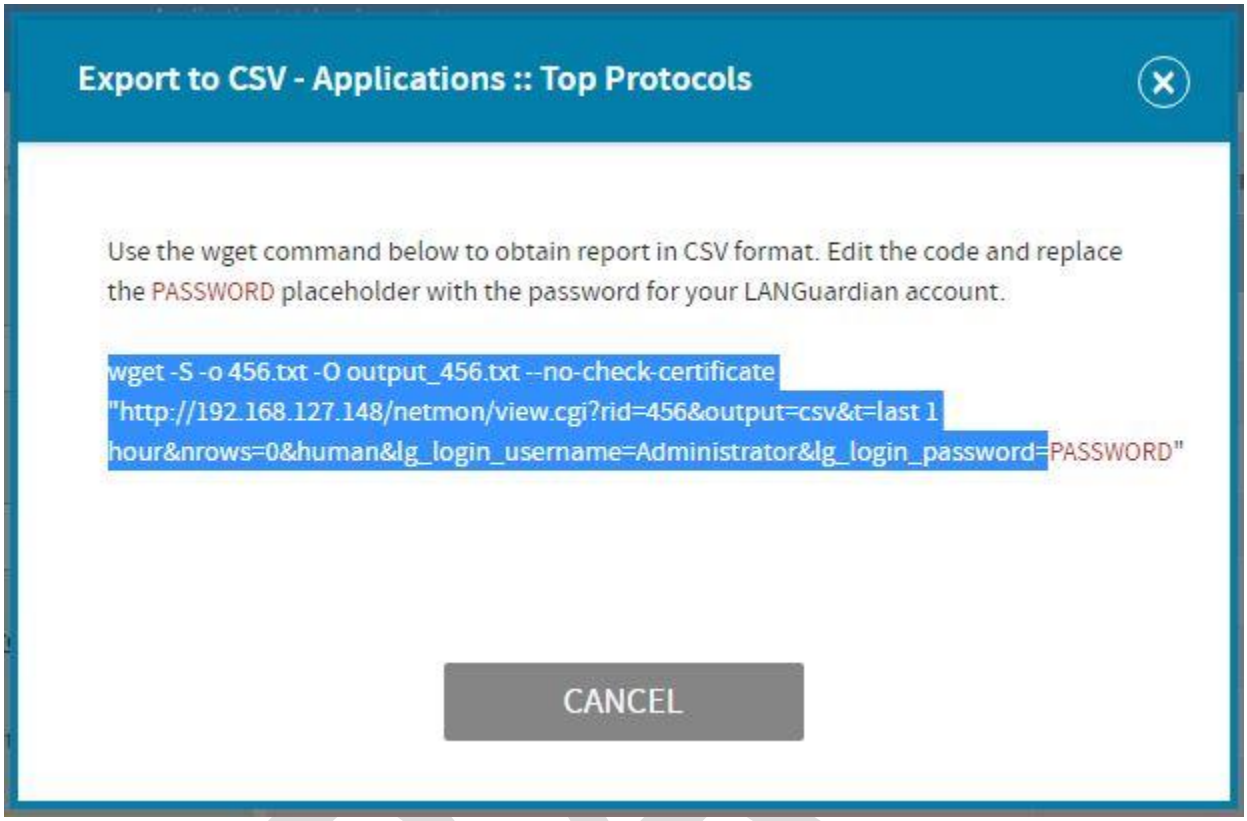
1. Log on the LANGuardian GUI as user RESTAPI
2. Select the report that you want to run via REST API (for example Top Protocols)



3. Run the report, then click on the Integration menu and select CVS

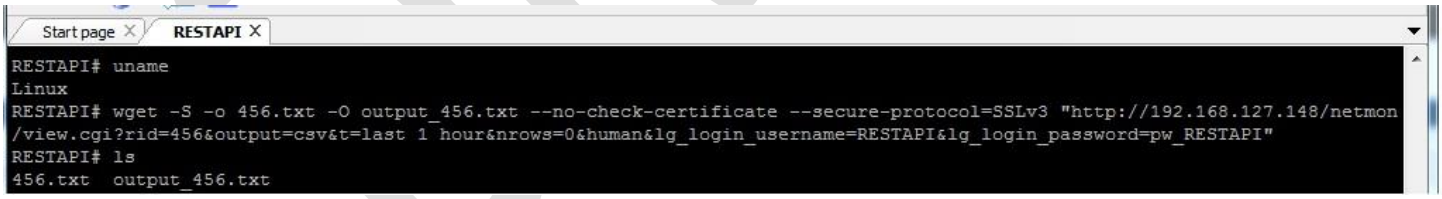
DRAFT

4. From the pop up dialog, select and copy the wget command

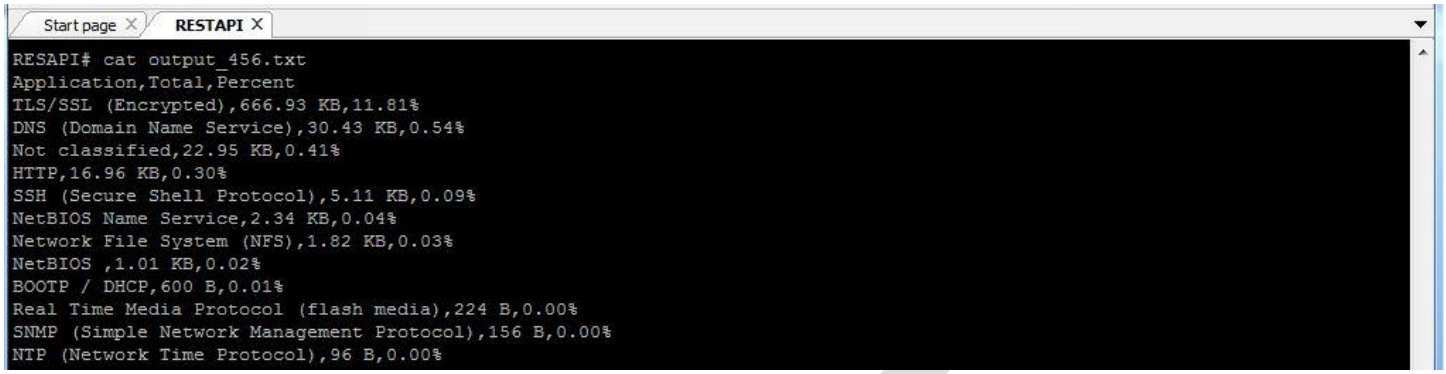


5. Replace the red text PASSWORD, with the correct password for the user account, in this case pw_RESTAPI.

6. Run the command in a shell or embed into a script as appropriate



7. The report results will appear in the local directory, in a file called output_456.csv. In this example 456 is the LANGuardian Report ID (RID) for the Top Protocols report.



8. Modify the output using the following parameters in the URL
    - nrows – specify the number of rows to be returned, or 0 for all rows
    - human – specify human readable output

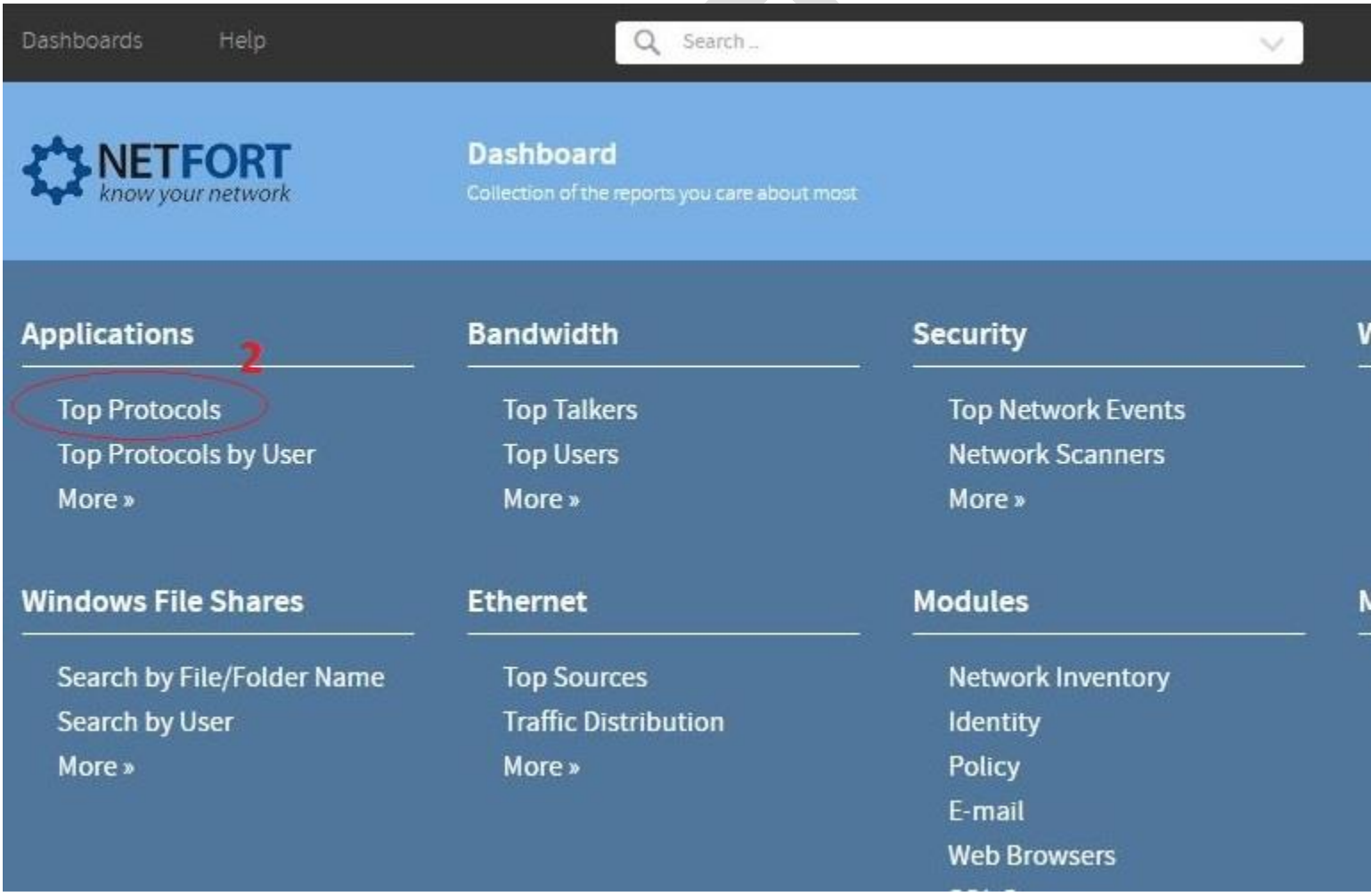
DRAFT

2.4 IFRAME

The RESTAPI IFRAME output is suitable for embedding HTML format information from LANGuardian into any web page. Use this technique to build 'single pane of glass' type dashboards that combine information from various systems together.

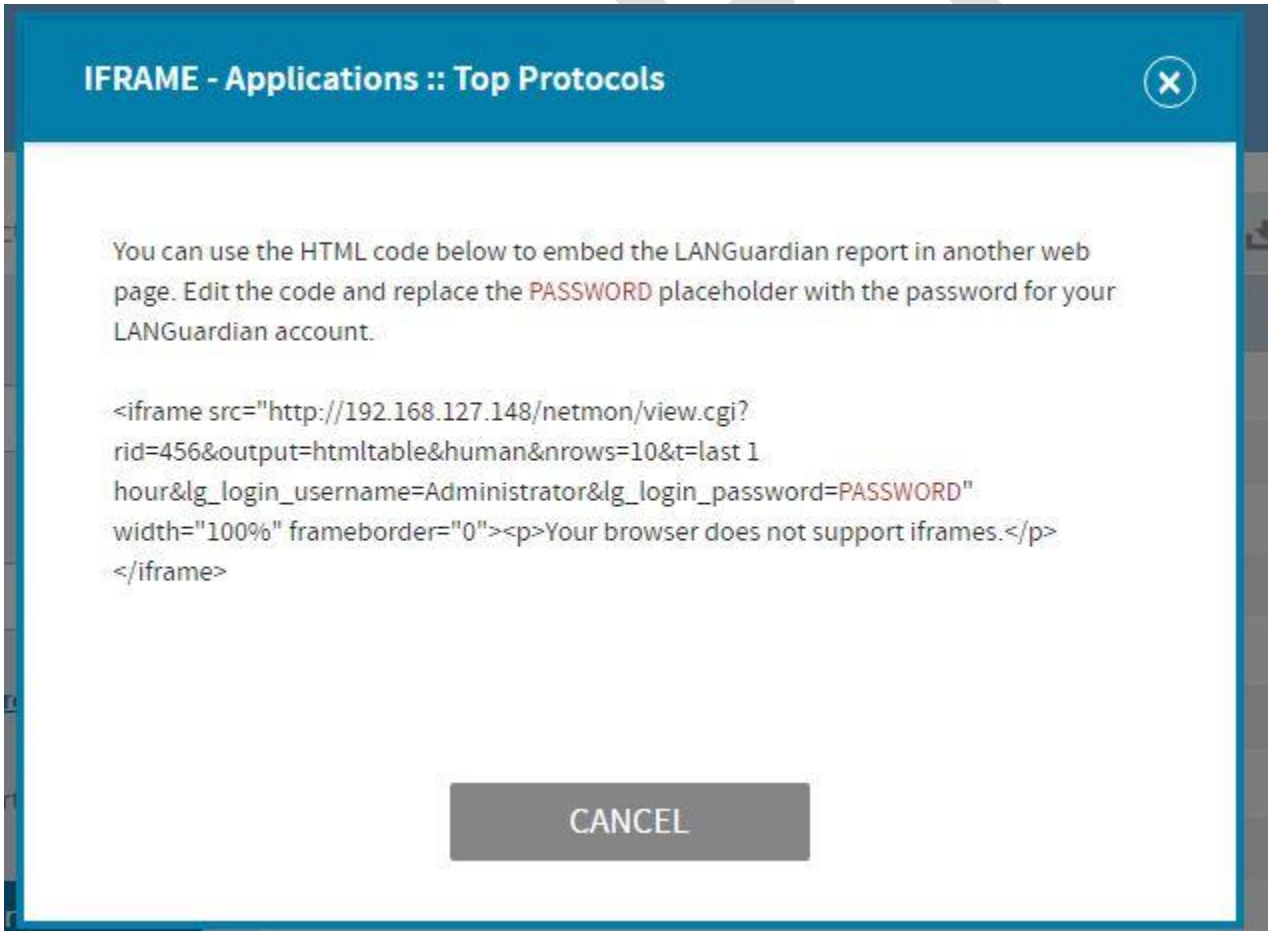
To use the IFRAME API format, use the following steps as an example to embed a LANGuardian report into a Spiceworks dashboard.

1. Log on the LANGuardian GUI as user RESTAPI
2. Select the report that you want to run via REST API (for example Top Protocols)



3. Click on the drop down menu labeled API and select CVS

4. Select the highlighted iframe HTML code from the dialog box.



5. Open the Spiceworks dashlet control and paste in the iframe HTML code. Remember to changes the embedded password to match the RESTAPI user.

2.5 LANGuardian and SolarWinds Orion Integration

Netfort Technologies provide an integration between Netfort LANGuardian and Solarwinds Orion. The integration brings LANGuardian extended network visibilty to the Orion NPM product.

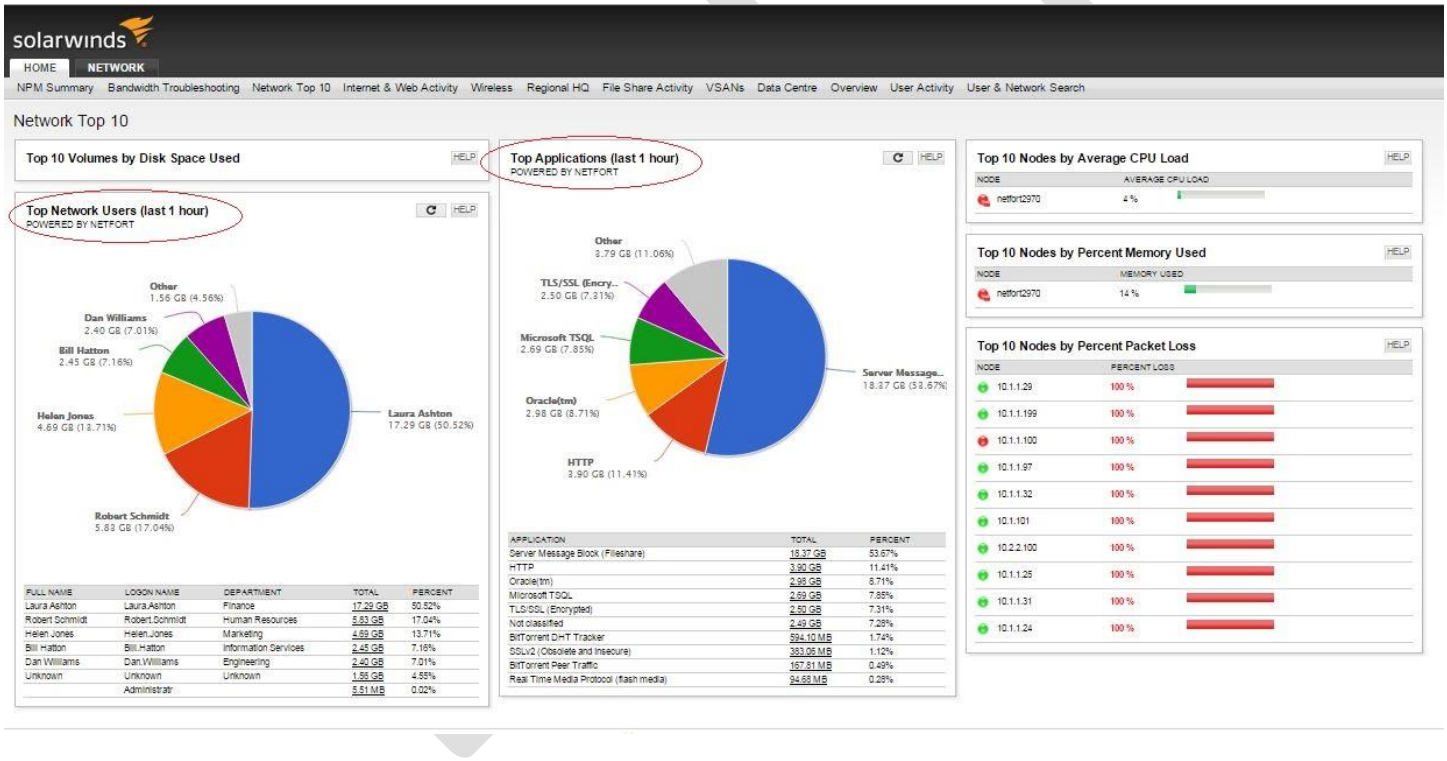
2.5.1 Orion V11 or less

To simplify the configuration, Netfort have created an integration wizard that is exectued on the Orion server.

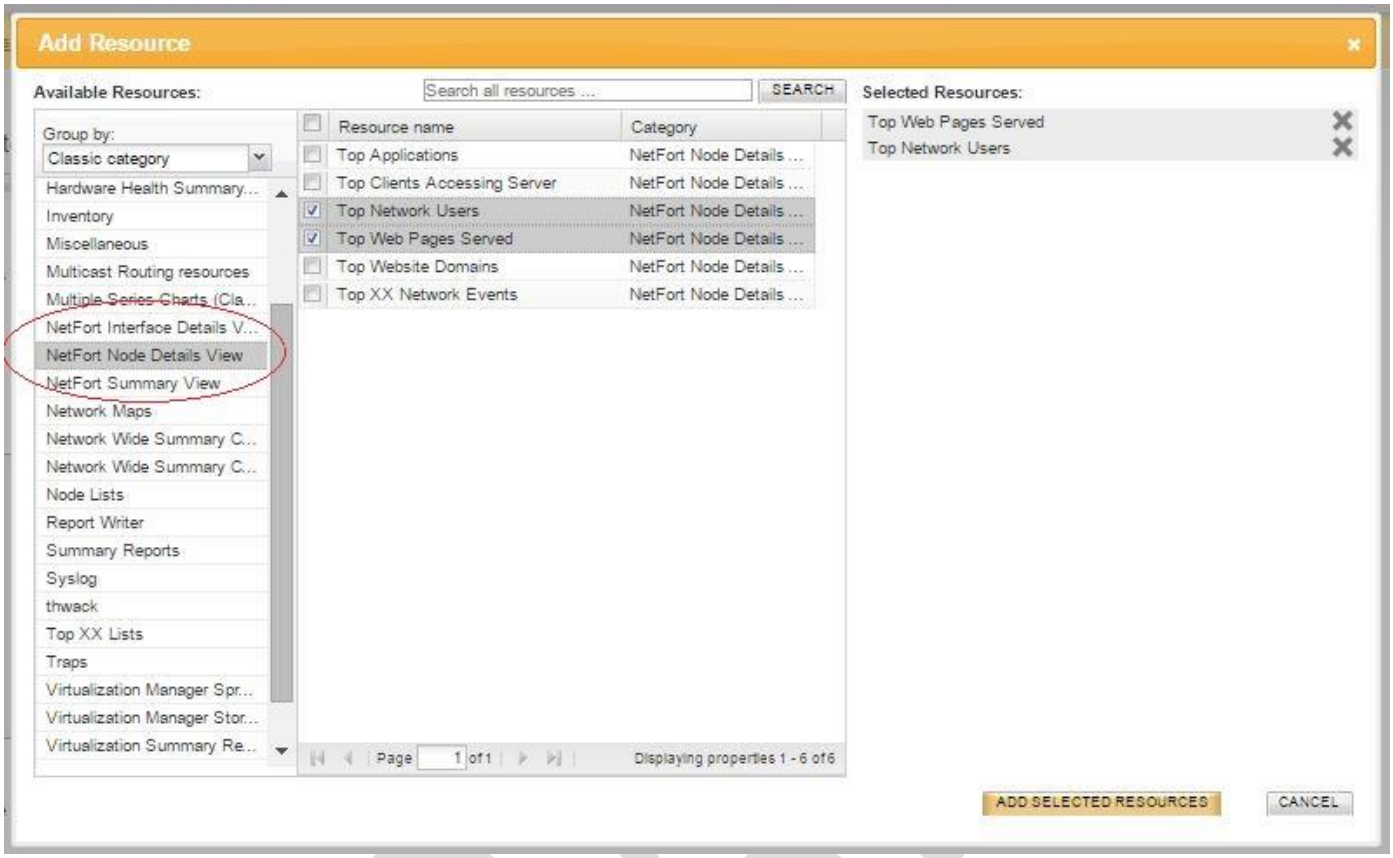
See http://www.netfort.com/downloads/solarwinds-integration/ for access to the integration pack and associated documents.

An example integration is provided at http://demo2.netfort.com

Orion view with embedded LANGuardian reports



Modified Orion menu with LANGuardian recourses for quick configuration


Add Resource
Available Resources:
Search all resources ...
SEARCH
Selected Resources:
Top Web Pages Served
Top Network Users
Group by:
Classic category
Hardware Health Summary...
Inventory
Miscellaneous
Multicast Routing resources
Multiple Series Charts (Cla...
NetFort Interface Details V...
NetFort Node Details View
NetFort Summary View
Network Maps
Network Wide Summary C...
Network Wide Summary C...
Node Lists
Report Writer
Summary Reports
Syslog
thwack
Top XX Lists
Traps
Virtualization Manager Spr...
Virtualization Manager Stor...
Virtualization Summary Re...
Resource name
Category
Top Applications
NetFort Node Details ...
Top Clients Accessing Server
NetFort Node Details ...
Top Network Users
NetFort Node Details ...
Top Web Pages Served
NetFort Node Details ...
Top Website Domains
NetFort Node Details ...
Top XX Network Events
NetFort Node Details ...
Page 1 of 1
Displaying properties 1 - 6 of 6
ADD SELECTED RESOURCES
CANCEL

DRAFT

2.5.2 Orion V12 or more

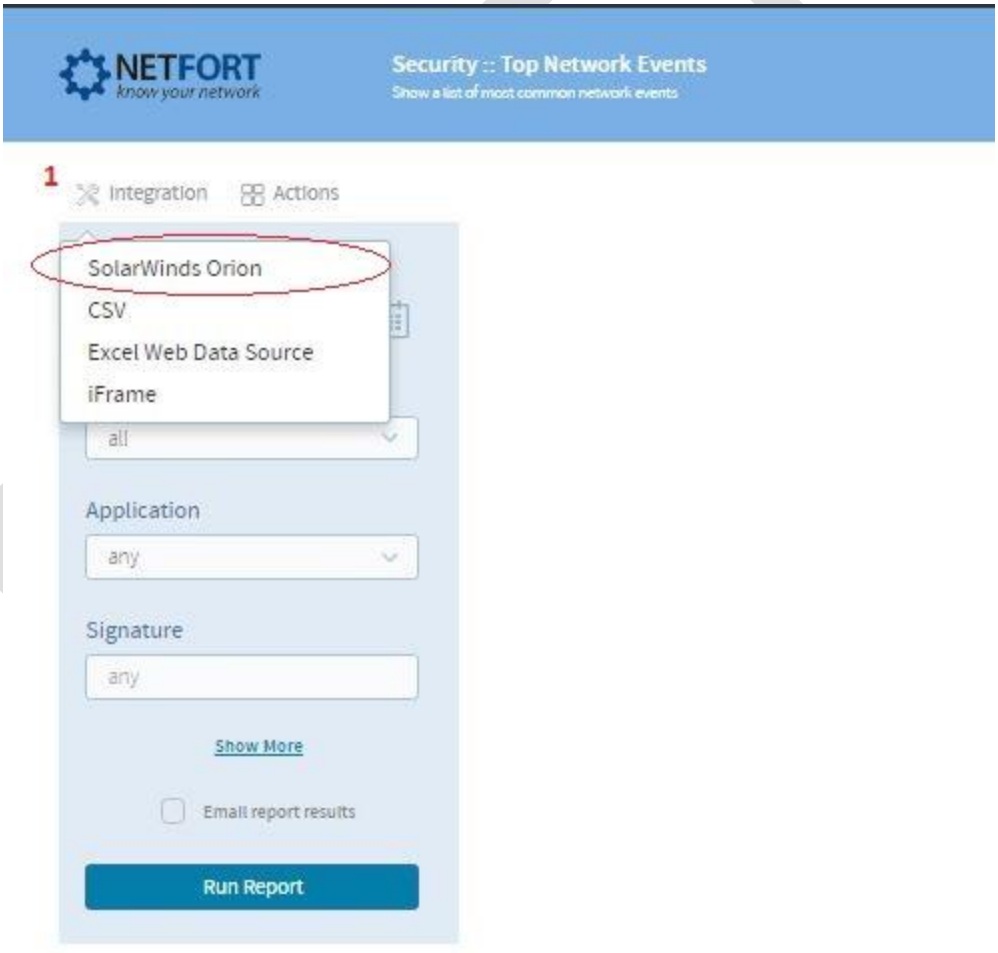
The Netfort integration kit for SolarWinds Orion is not supported by Orion V12 or higher. Instead the integration is achieved using Orion Custom HTML elemements and the LANGuardian reports *Integration menu.*

Add LANGuardian reports to an Orion V12 system, using the following steps.

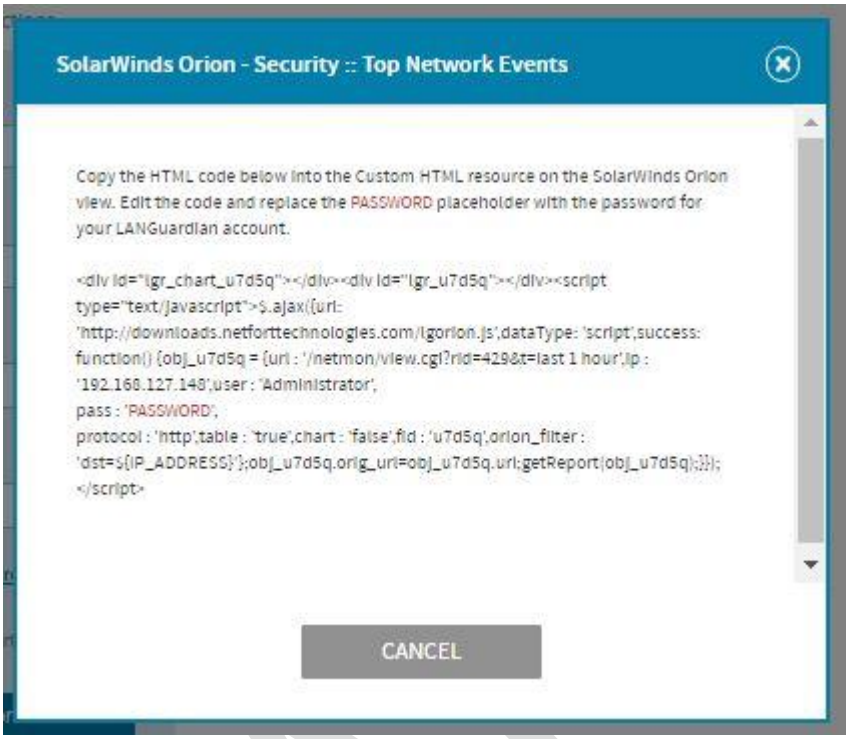
1. Select the dashboard tab on Orion where you want to add the LANGuardian report, and add a custom HTML element. See https://thwack.solarwinds.com/community/solarwinds-community/product-blog/blog/2010/08/05/hidden-gem-the-custom-html-resource for information on how to do this.

2. Open the LANGuardian web GUI and locate the report that you want to add to Orion

3. Click on the Integration menu and select the Solarwinds Orion option.



4. Copy the HTML code that is shown and paste it into the Custom HTML element on the Orion dashboard



2.6 Excel(Data from web)

The Microsoft Excel Data from Web feature can be used to directly import data from LANGuardian into an Excel spreadsheet. See the following article describing the feature

http://office.microsoft.com/en-us/excel-help/query-for-data-from-a-web-page-HP003074190.aspx

Here's an example spreadsheet that runs a report on the Netfort online demo system.

http://downloads.netforttechnologies.com/software/DataImport_TrafficDistribution.xlsx

DRAFT

2.7 Splunk Integration

Netfort have developed and published on Splunkbase the LANGuardian App for Splunk.
Find it here:

https://splunkbase.splunk.com/app/3636/

Important information for configuring the LANGuardian App for Splunk is available on our forum here:

https://forum.netfort.com/netfort/topics/software-configuration-for-languardian-app-for-splunk

Once the LANGuardian App for Splunk is installed on the Splunk server and configured to access LANGuardian, it uses the REST API to periodically retrieve selected information from the LANGuadian database and add it to the Splink indexes. The added data conforms to the Splunk CIM and can be used in all Splunk searches. A prepopulated dashboards is also included.

2.8 Troubleshooting REST API

If the report is not correctly displayed, the following steps may help identify the problem.

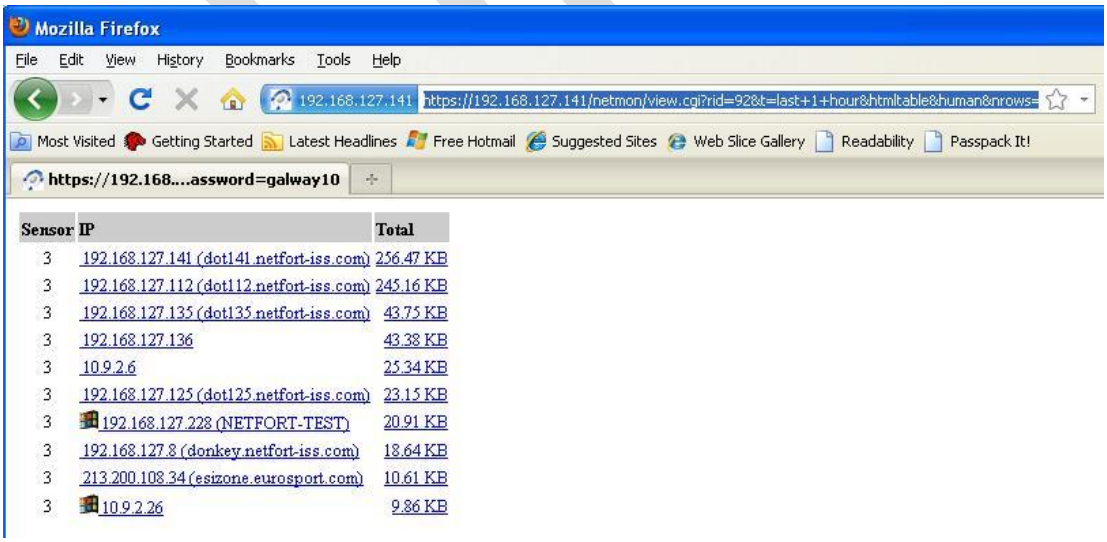
2.8.1 Issues with the LANGuardian REST API

To verify that the LANGuardian REST API is responding correctly to requests, you can copy the report URL and paste it into the address bar of any browser. Instead of the usual LANGuardian report GUI, you will be returned a simple HTML table of results. See the screenshot below.

Extract from the iframe syntax, the portion that looks like

https://192.168.200.179/netmon/view.cgi?rid=49&ip=${IP_ADDRESS}&htmltable&human&nrows=10&t=last 1 hour&lg_login_username=Administrator&lg_login_password=PASSWORD"

and paste into a browser address bar.



Sensor	IP	Total
3	192.168.127.141 (dot141.netfort-iss.com)	256.47 KB
3	192.168.127.112 (dot112.netfort-iss.com)	245.16 KB
3	192.168.127.135 (dot135.netfort-iss.com)	43.75 KB
3	192.168.127.136	43.38 KB
3	10.9.2.6	25.34 KB
3	192.168.127.125 (dot125.netfort-iss.com)	23.15 KB
3	192.168.127.228 (NETFORT-TEST)	20.91 KB
3	192.168.127.8 (donkey.netfort-iss.com)	18.64 KB
3	213.200.108.34 (esizone.eurosport.com)	10.61 KB
3	10.9.2.26	9.86 KB

DRAFT

If the REST API is responding correctly, you'll see a report similar to the one above. If there is no data to display an empty page is dislayed.

Otherwise, an error message will be displayed.

2.8.2 Issues with the custom HTML

To ensure the custom HTML is setup correctly, eliminate LANGuardian from the text and use something like:

<iframe

src ="www.google.com"

width="100%" height="500">

Your browser does not support iframes.
</iframe>
This should display the Google home page in an iframe in the Orion view.

2.9 Support for LANGuardian report filters

The REST API does not export any report filters that may have been set in a report. For example, if you add a Destination IP address filter to a *Traffic Distribution* report and then display a REST API dialog, then the report destination IP address filter will be ignored.

To use report filters with the REST API, create a LANGuardian Custom report, with the correct filters and then generate the REST API dialog from that new custom report.

2.10 Time filters for REST API reports

The default time interval used in all REST API calls is *last 1 hour.* This is specified in the HTTP text as

&t=last 1 hour

The time filter can be selected by modifying the &t variable.

Standard options are

&t=last 1 hour

&t=last 4 hours

&t=last 24 hours

DRAFT

Arbitary time filters can be set as follows

&t=to-from

Where to and from are specified in a pseudo perl time format, as

yyyymmddhhmmss

A caveat with this format however, is that the month is indexed from zero, so Jan is 0, February is 1 etc

To run a report from 11 AM 1st April 2011 to 7:30 PM 2nd April 2011, supply the time filter as

&t = 20110301110000-2011030219300

Alternatively, the time filter can be supplied as a unix timestamp. This may be more suitable scripted calls. To specify the time filter as a unix timestamp, use the &ut variable as,

&ut = from-to.

A time converter resource, such as http://www.onlineconversion.com/unix_time.htm, converts the time range 11 AM 1st April 2011 to 7:30 PM 2nd April 2011 to

&ut = 1301655600 - 1301772600

DRAFT

2.11 Configuring LANGuardian Web server

The LANGuardian web user interface is accessed over http or https. LANGuardian generates a self signed certificate when it boots after installation. This certificate is used by the webserver when running in https mode.

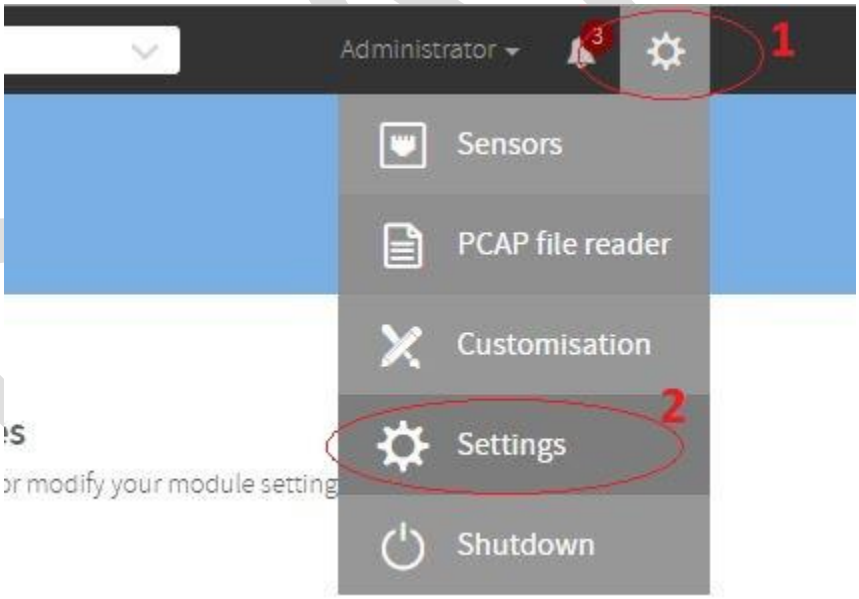
Because the certificate is self signed and may not match the hostname of the LANGuardian, users are frequenly prompted by their browser to accept the untrusted certificate.

This can cause complication when using the REST API, as some user agents do not provide a method to easily accept a certificate or ignore certifcate errors.

The LANGuaridan webserver can be configured to

- Run in HTTP mode
- Create a new self signed (x509) certificate
- Load a new certificate

To reconfigure the LANGuardian webserver, access the **Configuration** page:



Go to the Webserver configuration section:

eports & Blacklist updates or upgrade LANGuardian

ensor rulesets

the LANGuardian

Web Server

Secure your LANGuardian access with SSL

» Secure access configuration

» Change the SSL certificate

tings

Controls

dian user accounts

License

View or update system license

» System license settings

DRAFT

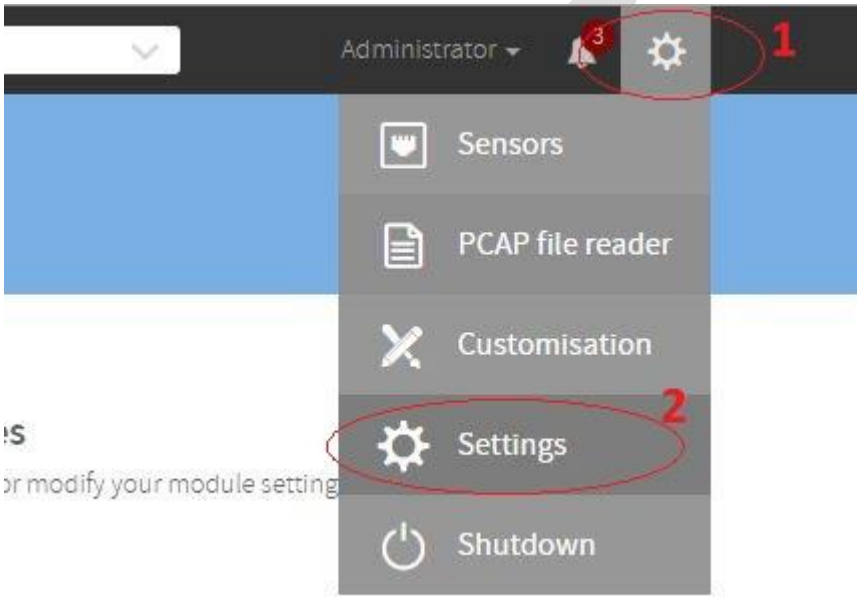
3 Syslog Export

3.1 Configuration

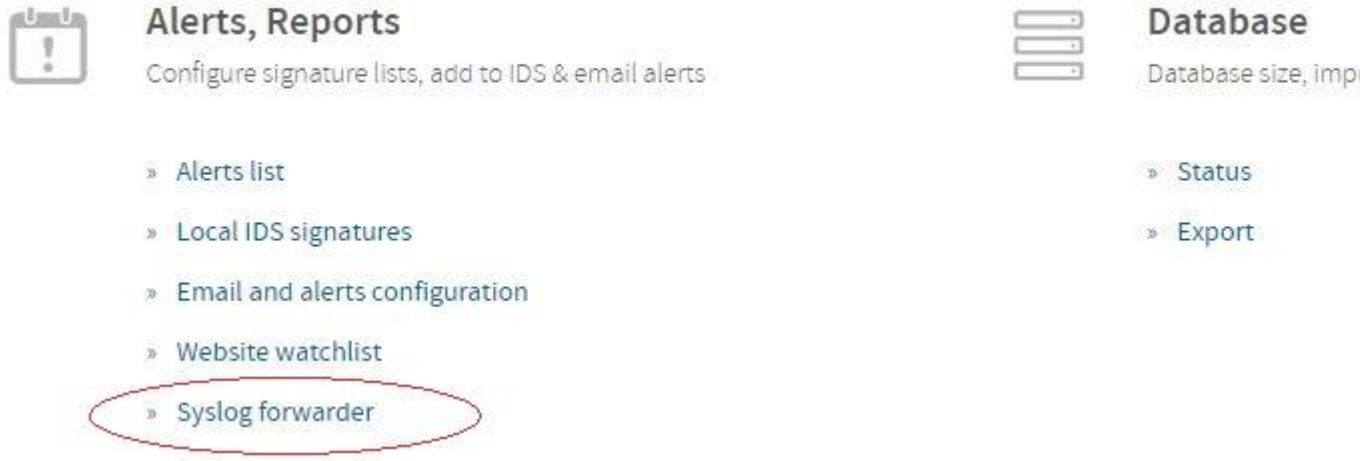
Syslog export from LANGuardian is enabled on all systems (no special license is required).

Follow these steps to configure syslog output:

1. Access the LANGuardian web user interface and go to the **Configuration** page.



2. Scroll down to the **Alerts, Reports** section and click Syslog Forwarder.



3. On the Syslog Forwarder Page, enter the IP address of the syslog collection system and select which types of event should be forwarded. Click on Save.

3.2 Format of exported syslog message

All LANGuardian events are tagged **LANGuardian** and have facility **LOG_USER** and level **LOG_NOTICE**.

The syslog header includes the IP address of the LANGuardian system generating the syslog message.

Jul 26 12:10:14 172.16.60.100 LANGuardian[8895]:

After the syslog header, the syslog message format divides messages into two parts: a common component followed by application-specific components.

3.3 Common component

Field name	Type	Description
sen_id	Integer	The ID of the LANGuardian sensor that detected the event.
sensor_name	String	Test name of the sensor
sensor_ip		IP address of the LANGuardian system where the sensor is hosted.
app_id	Integer	The type of event. For possible values see table Application names and IDs
app	String	The type of event. For possible values see table Application names and IDs
sid	Integer	Signature ID
name	String	Application signature name
src_ip	String	The source IP address, in dotted decimal format, of the system generating the event.
dest_ip	String	The destination IP address, in dotted decimal format, of the system generating the event.
timestamp		Unix timestamp when the event was recorded in the LANGuardian database.
eid		Unique event in the LANGuardian database, can be used to create link to access the event in the LANGauardian database.
prio		Event priority

Table 1: Common syslog message components

3.4 Application names and IDs

Application ID	Application Name	Signature ID	Description
1	web_access	1	Any Attempted Web Access to domain on

			watchlist
1		2	Any Attempted Web Access
2	netscan	1	Attempted connection from single IP to multiple IPs on a single port. Limits configurable via sensor settings menu Portscan variable.
3	packet	multiple	IDS signature triggered. See signature for more details
4	email	1	SMTP email envelope seen
		2	SMTP email with attachment
		3	SMTP email with hyperlink who's description does not match real hyperlink
5	volmeter	1	Excessive traffic exchange for a single IP, limits configurable via sensor settings menu
6	portscan	1	Attempted connection from single IP to multiple IPs on a single port. Limits configurable via sensor settings menu portscan variable.
7	dns_mx	1	Excessive email record lookups from a single IP. Limits configurable via sensor settings menu. Indicates possible malware spammer

DRAFT

			infection.
8	health_monitor	1	Host is down
		2	Service is down
9	smb	1	Windows network share file acess
10	torrent	1	BitTorrent Announce Request
		2	BitTorrent Peer Exchange Request
12	trend	multiple	An alarm level on a trend has been breached.
13	newmacs	1	A new Ethernet MAC address has been detected (a new system is on the network)
14	dns_access	1	A system has attempted to resolve a DNS domain name that is on the watchlist.
15	report_alert	0	A scheduled report has generated an alert (see report alerts, used for arbitrary user defined alerts).
16	ms_sql	1	An access to an ms_sql event was detected.
17	policy	1	User Daily Bandwidth Quota Warning
		2	User Daily Bandwidth Quota Violation
		3	User Weekly Bandwidth Quota Warning

DRAFT

		4	User Weekly Bandwidth Quota Violation
18	nfs	1	Network File System access detected
20	exploit	1	OpenSSL HeartBleed Exploit Attempt
		2	SSL/TLS Server with Heartbeat Extension

DRAFT

3.5 Application-specific components

Event type	Field name	Type	Description
Web access	host	String	The name of the website being accessed
Web access	Uri	String	The URI (page or resource) on the website that is being accessed.
Email (SMTP)	from_addr	String	The **From** address of the mail message.
Email (SMTP)	to_addr	String	The **To** address of the mail message.
Email (SMTP)	subject	String	The subject line of the mail message.
Microsoft Windows file share	smb_action	String	The action performed on the resource. Possible values: create: Create a resource read: Read a resource write: Write a resource delete_file: Delete a file delete_dir: Delete a folder
Microsoft Windows file share	smb_path	String	The pathname of the resource (file or folder) being accessed.
Microsoft SQL Server statement	username	String	MS SQL username making the select (if available)
Microsoft SQL Server statement	appname	String	Application name making the select
Microsoft SQL Server statement	database	String	MSSQL database being queried

Microsoft SQL Server statement	statement	String	MSSQL statement
Microsoft SQL Server Statement	type	String	
nfs	action	String	The action performed on the resource.
nfs	path	String	The pathname of the resource (file or folder) being accessed.
nfs	proto	Integer	Transport Protocol used
nfs	version	Integer	NFS version used

Table 2: Application-specific syslog components

3.6 Some Example Syslog Messages

The following are some examples of syslog messages generated by LANGuardian.

Note: in these examples, dot141.netfort.com is the IP address of the LANGuardian system generating the syslog events.

1. Web Access

   Sep 26 11:57:43 LANGuardian event[5425]: sen_id=3 app_id=1 sid=2 app=web_access name='Web Access' src_ip=200.236.172.245 dest_ip=88.77.168.245 host=download.testband.com uri=/5MB.zip

2. Netscan

   Sep 26 11:58:01 LANGuardian event[5425]: sen_id=3 app_id=2 sid=1 app=netscan name='Netscan' src_ip=172.16.60.128 dest_ip=0.0.0.0

3. Packet/IDS

   Sep 26 11:55:00 LANGuardian event[5425]: sen_id=3 app_id=3 sid=2019088 app=packet name='ET EXPLOIT F5 BIG-IP rsync cmi authorized_keys access attempt' src_ip=1.1.1.1 dest_ip=192.168.1.111

4. Email

   Sep 26 11:55:23 dot141.netfort.com LANGuardian event[5425]: sen_id=3 app_id=4 sid=3 app=email name='Email Traffic with Hyper Link' src_ip=192.168.127.40 dest_ip=74.125.24.27

DRAFT

from_addr=local12@localhost.localdomain to_addr=test.lab@netfort.com subject=SMTP HTML Test Email

5. Voltmeter

   Sep 26 11:55:38 dot141.netfort.com LANGuardian event[5425]: sen_id=3 app_id=5 sid=1 app=volmeter name='Traffic Volume Overflow' src_ip=10.16.0.17 dest_ip=0.0.0.0

6. Portscan

   Sep 26 11:55:56 dot141.netfort.com LANGuardian event[5425]: sen_id=3 app_id=6 sid=1 app=portscan name='Portscan' src_ip=192.168.127.222 dest_ip=192.168.127.148

7. DNS_MX (mail record lookups)

   Sep 26 11:56:16 dot141.netfort.com LANGuardian event[5425]: sen_id=3 app_id=7 sid=1 app=dns_mx name='DNS MX flood (possible SPAM)' src_ip=192.168.127.40 dest_ip=0.0.0.0

8. Obsolete

9. Microsoft Windows file share access (SMB Events)

   Read

   Mar 30 11:50:45 <user.notice> dot141.netfort.com LANGuardian event[9902]: sen_id=7 app_id=9 sid=1 app=smb name='Windows Network File Access' prio=3 src_ip=172.16.0.17 dest_ip=192.168.127.180 smb_action=read smb_path=\\192.168.127.180\SHARE\test2\Thumbs.db

   Map

   Apr 3 11:15:20 <user.notice> dot141.netfort.com LANGuardian event[7455]: sen_id=1 app_id=9 sid=1 app=smb name='Windows Network File Access' prio=3 src_ip=192.168.114.1 dest_ip=192.168.114.129 smb_action=map smb_path="\\192.168.114.129\TEST"

   Create

   Apr 3 11:17:38 <user.notice> dot141.netfort.com LANGuardian event[7455]: sen_id=1 app_id=9 sid=1 app=smb name='Windows Network File Access' prio=3 src_ip=192.168.114.1 dest_ip=192.168.114.129 smb_action=create smb_path="?\testeas\ea.txt"

   Rename

   Apr3 11:22:21 <user.notice> dot141.netfort.com LANGuardian event[7455]: sen_id=1 app_id=9 sid=1 app=smb name='Windows Network File Access' prio=3 src_ip=192.168.127.247 dest_ip=192.168.127.180 smb_action=rename smb_path="?\mp3_uploads\test1.mp3 -> \mp3_uploads\test1_renamed.mp3"

   Write

DRAFT

Apr3 11:23:45 <user.notice> dot141.netfort.com LANGuardian event[7455]: sen_id=1 app_id=9 sid=1 app=smb name='Windows Network File Access' prio=3 src_ip=192.168.114.1 dest_ip=192.168.114.129 smb_action=write smb_path="?\rawopen\torture_chained.txt"

Delete

Apr3 11:24:41 <user.notice> dot141.netfort.com LANGuardian event[7455]: sen_id=1 app_id=9 sid=1 app=smb name='Windows Network File Access' prio=3 src_ip=192.168.127.247 dest_ip=192.168.127.180 smb_action=delete smb_path="?\mp3_uploads\test1_renamed.mp3"

Delete Directory

Apr3 11:26:04 <user.notice> dot141.netfort.com LANGuardian event[7455]: sen_id=1 app_id=9 sid=1 app=smb name='Windows Network File Access' prio=3 src_ip=192.168.114.1 dest_ip=192.168.114.129 smb_action=delete_dir smb_path="?\testsd\inheritance\testdir"

Create Directory

Apr3 11:28:06 <user.notice> dot141.netfort.com LANGuardian event[7455]: sen_id=1 app_id=9 sid=1 app=smb name='Windows Network File Access' prio=3 src_ip=192.168.127.238 dest_ip=192.168.127.223 smb_action=create smb_path="\New folder"

10. Bittorrent

Sep 26 11:56:53 LANGuardian event[5425]: sen_id=3 app_id=10 sid=1 app=torrent name='BitTorrent Announce Request' src_ip=10.0.0.100 dest_ip=91.189.90.143

11. Obsolete

12. MS SQL statements

MSSQL select

Apr 1 10:37:45 <user.notice> dot141.netfort.com LANGuardian event[18238]: sen_id=1 app_id=16 sid=1 app=ms_sql name='MS SQL Access'src_ip=192.168.127.180 dest_ip=192.168.127.152 username= appname= database=vpms statement=SELECT buyer, vndno, vndnam, qtyrec, transqty, vperf FROM rtvperfv01 WHERE recyear = 2008 AND recmonth = 6 AND buyer = 'T1' ORDER BY vperf type=1

MSSQL Login

Apr 1 10:37:35 <user.notice> dot141.netfort.com LANGuardian event[18238]: sen_id=1 app_id=16 sid=1 app=ms_sql name='MS SQL Access' src_ip=11.153.79.20 dest_ip=11.153.79.100 username=sa appname=Stores database= statement=(unknown) type=11

MSSQL Create

DRAFT

Apr3 17:55:46 <user.notice> dot141.netfort.com LANGuardian event[26241]: sen_id=2 app_id=16 sid=1 app=ms_sql name='MS SQL Access' src_ip=192.168.127.245 dest_ip=192.168.127.181 username= appname= database= statement=CREATE DATABASE my_db type=4

MSSQL Drop

Apr3 17:58:02 <user.notice> dot141.netfort.com LANGuardian event[26241]: sen_id=2 app_id=16 sid=1 app=ms_sql name='MS SQL Access' src_ip=192.168.127.245 dest_ip=192.168.127.181 username= appname= database= statement=DROP DATABASE my_db type=8

MSSQL Insert

Apr3 17:59:18 <user.notice> dot141.netfort.com LANGuardian event[26241]: sen_id=2 app_id=16 sid=1 app=ms_sql name='MS SQL Access' src_ip=192.168.127.245 dest_ip=192.168.127.181 username= appname= database= statement=INSERT INTO Persons (P_Id, LastName, FirstName)VALUES (5, 'Tjessem', 'Jakob') type=2

MSSQL Update

Apr3 18:00:04 <user.notice> dot141.netfort.com LANGuardian event[26241]: sen_id=2 app_id=16 sid=1 app=ms_sql name='MS SQL Access' src_ip=192.168.127.245 dest_ip=192.168.127.181 username= appname= database= statement=UPDATE PersonsSET Address='Nissestien 67', City='Sandnes' type=3

MSSQL Delete

Apr3 18:01:10 <user.notice> dot141.netfort.com LANGuardian event[26241]: sen_id=2 app_id=16 sid=1 app=ms_sql name='MS SQL Access' src_ip=192.168.127.245 dest_ip=192.168.127.181 username= appname= database= statement=DELETE * FROM Customers type=5

MSSQL Use

Apr3 18:05:06 <user.notice> dot141.netfort.com LANGuardian event[26241]: sen_id=2 app_id=16 sid=1 app=ms_sql name='MS SQL Access' src_ip=192.168.127.245 dest_ip=192.168.127.181 username= appname= database= statement=SQL> USE northwind; type=0

MSSQL Set

Apr3 18:05:52 <user.notice> dot141.netfort.com LANGuardian event[26241]: sen_id=2 app_id=16 sid=1 app=ms_sql name='MS SQL Access' src_ip=192.168.127.245 dest_ip=192.168.127.181 username= appname= database=northwind statement=UPDATE PersonsSET Address='Nissestien 67', City='Sandnes'WHERE LastName='Tjessem' AND FirstName='Jakob' type=3

MSSQL RPC

Apr3 18:10:02 <user.notice> dot141.netfort.com LANGuardian event[26241]: sen_id=1 app_id=16 sid=1 app=ms_sql name='MS SQL Access' src_ip=11.153.79.23 dest_ip=11.153.79.99 username= appname= database= statement=Proc_GET_SubGroup&& type=0

DRAFT