NETFORT
know your network

LANGuardian

Administration and User Guide

This guide describes how to install, configure, and use NetFort LANGuardian to monitor activity on your network.

Product Release: LANGuardian version 11.0
Date: 29 May 2013

Corporate Headquarters

Unit 7
IDA Innovation Centre
Upper Newcastle
Galway
Ireland

Tel: +353 (91) 520501
Email: sales@netfort.com

www.netfort.com

Table of Contents

Preface

About this guide

This guide tells you how NetFort LANGuardian works, and explains how to install, configure, and use the software.

Intended audience

This guide is intended for anyone who wants to install or use NetFort LANGuardian – typically, network engineers, system administrators, IT managers, human resource managers, and compliance officers.

What's in this guide?

This guide contains the following information:

- Chapter 1 explains how LANGuardian works and describes the deployment options.
- Chapter 2 describes how to install and configure LANGuardian.
- Chapter 3 describes how to use LANGuardian to monitor and troubleshoot your network.
- Chapter 4 describes how to integrate LANGuardian with Solarwinds Orion.
- Appendix A is a reference guide to the report categories.
- Appendix B is a reference guide to the ports and protocols.
- Appendix C is a glossary of terms.
- An index.

Document conventions

This guide uses the following conventions:

- LANGuardian menu items and user interface commands are shown in **bold** font.

- Commands you enter on screen are shown in `monospace` font.

Additional information and resources

The following additional information and resources are available:

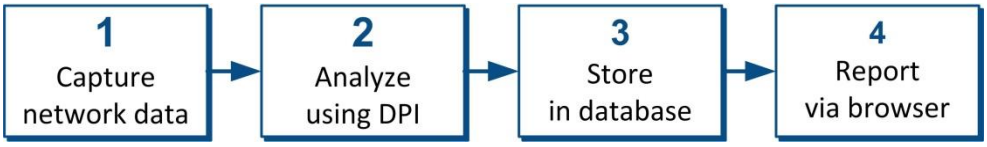
- NetFort Technologies website: www.netfort.com
- NetFort Technologies forum: forum.netfort.com
- NetFort Technologies support: support@netfort.com

Chapter 1

Chapter 1 - Welcome to LANGuardian

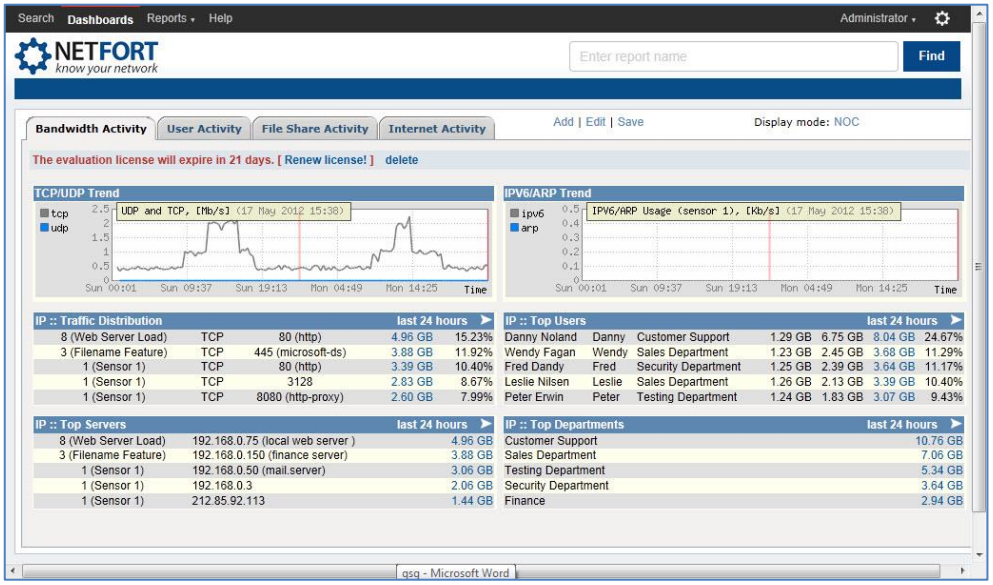
NetFort LANGuardian is software that monitors and reports on network activity. The browser-based user interface gives you a unique level of visibility into everything that's happening on your network, including user logons, bandwidth usage, Internet access, file share and database operations, and security threats.

1.1 LANGuardian overview



NetFort LANGuardian gives you a detailed view of the activity on your network. It captures a copy of data packets flowing through those ports and stores the details in a secure standalone database. It uses advanced deep packet inspection (DPI) techniques to analyze the data packets and generate detailed information about the source, destination, protocol, and contents of each packet. Because LANGuardian stores its information in a database, you can view details of historical, as well as real-time, LAN activity.

LANGuardian has a browser-based user interface made up of a search page, dashboards, and reports. You can customize the user interface to organize, present, and prioritize the network activity data that is of interest to you. From the dashboards, you can drill down to more detailed information about individual servers, clients, files, databases, users, websites, and so on.



LANGuardian is easy to deploy on your network. It is available as a standalone system and as a VMware® virtual appliance. Installing the software usually takes less than 15 minutes. To complete the installation and begin capturing traffic data, you connect LANGuardian to your network switch and configure port mirroring on the ports whose traffic you want to monitor.

Port monitoring

Most network core switches have the ability to copy network traffic from one port on the switch to another. This feature, which is called **port monitoring** or **port mirroring,** enables LANGuardian to capture traffic data for analysis.

Configuring a monitoring port on your switch involves the following steps:

- Identify an unused switch port to designate as a monitoring port for LANGuardian.
- Identify the switch ports you want to monitor (these are often called source ports).
- Configure the switch to associate the source ports with the monitoring port.

The switch will send a copy to the monitoring port of all data flowing through the source ports. LANGuardian captures the data from the monitoring port for analysis. The actual data itself is not affected and there is no performance impact.

Port monitoring is given different names by different switch vendors:

- On a Cisco® Systems switch, port monitoring is called Switched Port Analyzer (SPAN). You will often see references in the documentation to a SPAN port.
- On a 3Com® switch, it is called a Roving Analysis Port (RAP).
- The documentation for HP switches uses the term trunk monitoring.

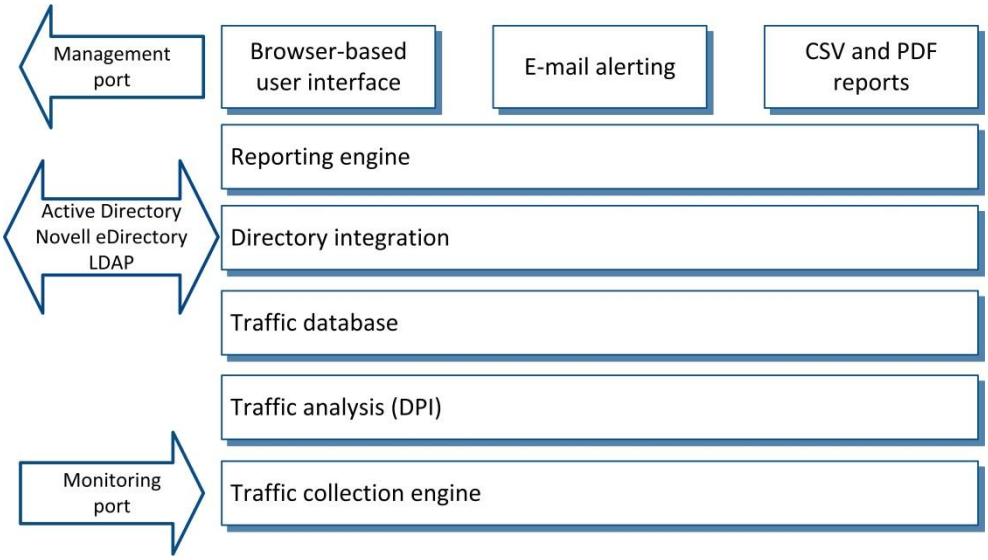
1.2 Architecture

LANGuardian uses advanced deep packet inspection (DPI) techniques to analyze the data packets flowing through the core switch on your network.

LANGuardian creates and maintains a database of traffic information, which gives you access to historical, as well as real-time, network activity

data. Historical data is indispensable for network forensics, and for identifying network issues and trends that cannot be identified using real-time data alone.

The diagram below shows the LANGuardian system architecture.



1.2.1 Management port

The management port on the LANGuardian system enables network administrators to establish a browser connection so that they can view the traffic data captured and stored by system.

1.2.2 Browser-based user interface

LANGuardian has a browser-based user interface with a customizable dashboard and drill-down capability to whatever level of detail you need. All modern browsers are supported.

1.2.3 E-mail alerting

You can configure any LANGuardian report to send you an e-mail alert immediately when certain conditions are met (for example, when a user accesses a specified website or file share).

1.2.4 CSV and PDF reports

You can generate CSV (for importing into Microsoft® Excel® and other spreadsheet applications) and PDF versions of all LANGuardian reports.

1.2.5 Reporting engine

The LANGuardian reporting engine uses the information in the traffic database to generate interactive web pages, e-mail alerts, CSV files, and PDF reports.

1.2.6 Directory services integration

With the directory services integration module, you can generate reports that include user names and other details derived from your corporate

directory. You can also configure the system to ignore specific accounts such as those that are used to download anti-virus updates and operating system patches.

LANGuardian supports Microsoft Active Directory®, Novell® eDirectory™, and the industry standard LDAP format.

1.2.7 Traffic database

LANGuardian stores a historical record of traffic data in a secure, hardened, and highly-optimized database. The database is a proprietary system specifically designed for very fast storage and retrieval of large amounts of flow and alert data that is organized in a time-ordered fashion.

The database capacity is limited only by the amount of storage space available, while the storage used per day is determined by the amount of traffic on your network. Because the database is independent of system log files, you can use it to demonstrate compliance with the segregation of duties requirements of internal and external auditors.

1.2.8 Traffic analysis – deep packet inspection

LANGuardian uses deep packet inspection (DPI) techniques to inspect the contents (payload) of data packets in addition to the packet header, enabling it to identify threats that cannot be identified using standard networking components alone. LANGuardian implements DPI at full wire speed and does not slow down the network.

The LANGuardian DPI engine has two components, traffic analysis and intrusion detection, which analyze the network traffic in parallel:

- Traffic analysis

  The traffic analysis engine identifies traffic flows in two ways:

  - The 5-tuple that uniquely identifies the TCP/IP connection – source IP address, source port, destination IP address, destination port, and protocol (TCP or UDP).
  - The source and destination hardware addresses, and the IP protocol used (IPv4 or IPv6).

  It also extracts other details from the traffic flows, for example:

  - Local services in use on the network
  - Operating system information

  The traffic analysis engine aggregates all of this information into its own proprietary internal flow representation, which it stores in the LANGuardian database.

- Intrusion detection

  The intrusion detection system (IDS) is based on Snort, an open-source network intrusion prevention system that performs real-time traffic

analysis on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.

The IDS is configured with over 1600 signatures that include DPI for HTTP, RPC, and Telnet protocols. The signatures cover the events that typically occur on a network, for example:

- File accesses
- Database operations
- E-mail activity
- Web access

The IDS signatures are continually updated and you can choose to apply the updates manually or automatically. You can also define your own signatures.

When the IDS detects an event that matches a signature, it stores the details in the LANGuardian database, including the source and destination IP addresses, the rule that triggered the event, and event-specific information.

Combined, the information stored in the database by the traffic analysis engine and the IDS provide a detailed snapshot of network activity, with efficient storage and no performance impact.

1.2.9 Traffic collection engine

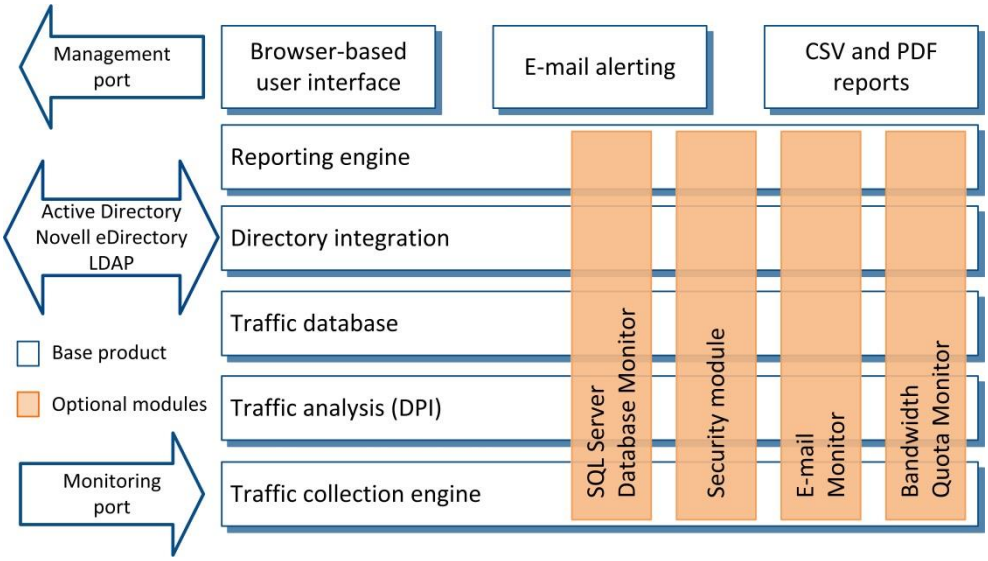
The traffic collection engine collects network activity data from the monitoring port on your core switch and prepares it for deep packet inspection (DPI) and subsequent storage in the LANGuardian traffic database.

1.2.10 Monitoring port

When monitoring a physical network, the monitoring port on the LANGuardian system connects to the monitoring port on the core switch. When monitoring a virtual network, the monitoring port connects to a virtual switch, which must be configured to allow promiscuous mode connections. The network traffic seen by the monitoring port is collected by the LANGuardian traffic collection engine.

1.3 Optional modules

The base LANGuardian product monitors and reports on traffic flowing through your network. A number of optional modules are available that provide more detailed information on specific types of network activity. The diagram below shows the optional modules.



1.3.1 SQL Server Database Monitor

This module monitors and records every access to your SQL Server databases, helping you to protect sensitive business data, secure your database infrastructure, detect fraudulent activity, and more easily meet your audit and compliance obligations.

1.3.2 Security Module

This module provides an intrusion detection system (IDS), which is based on Snort. Snort is an open-source network intrusion prevention system that performs real-time traffic analysis on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.

1.3.3 E-mail Monitor

This module decodes, extracts, and stores the headers of incoming (POP3) and outgoing (SMTP) mail messages, allowing you to search by sender, recipient and subject, along with more detailed information such as timestamps and the IP addresses of sender and recipient.

1.3.4 Bandwidth Quota Monitor

This module defines and monitors bandwidth quotas for users or groups of users on a network. You can configure warning emails and automatic actions to notify users are quota limits0 are approached or exceeded.

1.4 Deployment options

You can deploy LANGuardian in the following ways:

- Install it on a dedicated physical PC or server.

  When installed on a dedicated physical PC or server, LANGuardian runs on industry-standard hardware. The only special requirement is

that the PC or server must have two NICs (network interface cards) – one to collect the traffic data, and one to provide access to the LANGuardian user interface.

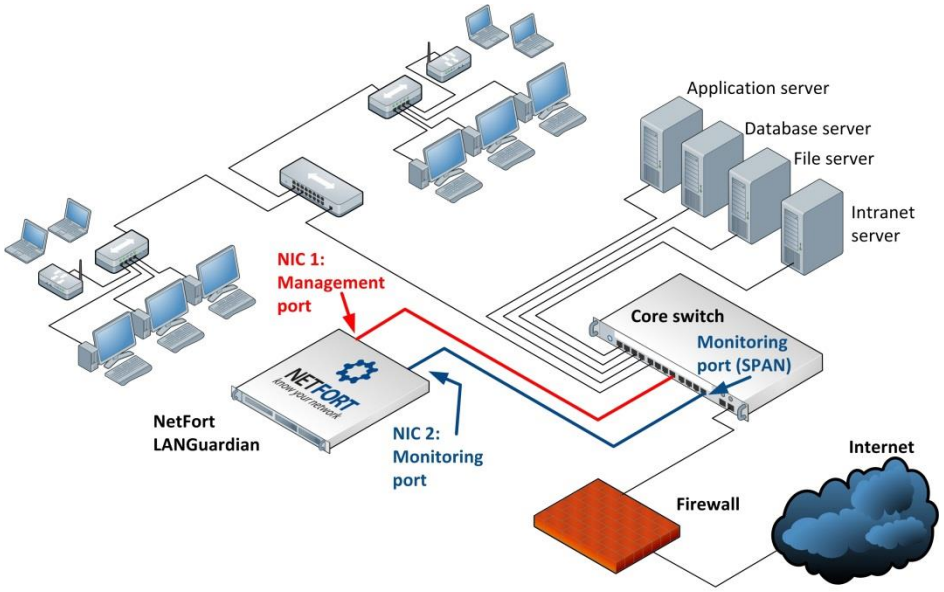
- Install it as a VMware virtual appliance.

  When deployed as a virtual appliance, LANGuardian can monitor internal virtual and physical network traffic. To monitor virtual network traffic, the virtual switch you are monitoring must be configured to allow promiscuous mode connections. To monitor physical network traffic with a LANGuardian virtual appliance, you need a dedicated virtual switch that is associated with its own NIC.

LANGuardian has its own standalone operating system and requires no operating system licenses.

1.4.1 Monitoring a physical network

The diagram below shows LANGuardian in a typical network setup consisting of PCs, laptops, servers, a core switch, and a firewalled Internet connection. LANGuardian is installed on a standalone server that is connected directly to the core switch.



In this network, the core switch port assignments are as follows:

Port number	Description
1	Intranet server
2	File server
3	SQL Server database server
4	Application server

5	User LAN
6	Unused port
7	Unused port
8	Management port
9	Unused port
10	Unused port
11	Unused port
12	Monitoring (SPAN) port

To monitor this network, the following steps are necessary:

1. On your network switch:

   a. Configure **port 12** as a monitoring port.

   b. Configure **ports 1, 2, 3, 4, 5,** and the **uplink port** as the source ports to be monitored.

2. Connect a network cable from the monitoring port on the switch **(port 12)** to one of the network interface cards on the LANGuardian server.

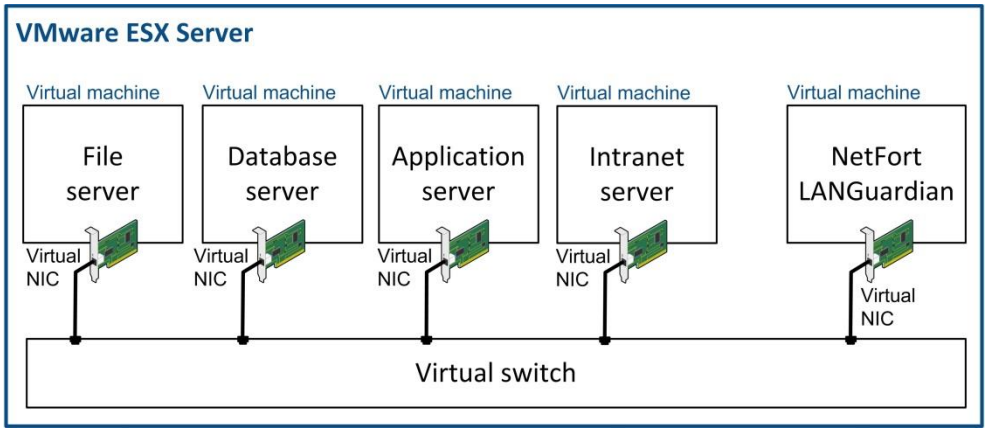
3. Connect a network cable from an unused port on the switch **(port 8)** to the other network interface card on the LANGuardian server.

1.4.2 Monitoring a virtual network

LANGuardian works on the same principle in virtual networks as in physical networks. LANGuardian supports a number of virtual environments, including VMware ESX®. For the purposes of describing LANGuardian in a virtual environment, this manual uses VMware ESX as an example.

A VMware ESX environment incorporates a virtual network switch, which is the virtual equivalent of the core switch in a physical network. The virtual network switch supports **promiscuous mode,** a setting that enables virtual adapters to see all traffic flowing through the switch and essentially providing the same functionality as a SPAN or monitoring port on a physical network. This makes it possible for the LANGuardian virtual appliance to monitor and report on all network traffic flowing through the virtual network.

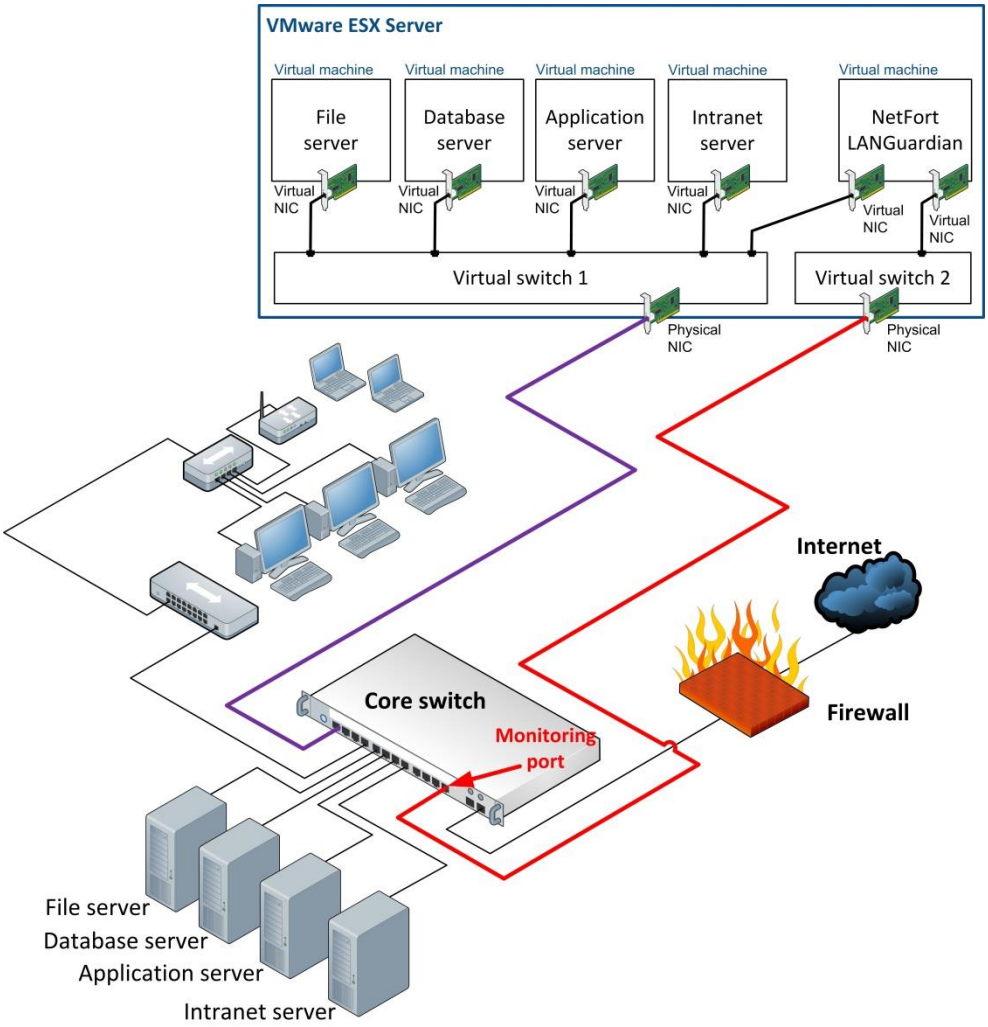
The illustration below shows a typical virtual network setup consisting of file, application, and database servers connected to a virtual switch. When connected to the same virtual switch as the servers, the LANGuardian virtual appliance can monitor all network activity on the servers.



In this network, LANGuardian is installed on a virtual server that is connected to a virtual switch. When the switch is configured in promiscuous mode, LANGuardian can capture all traffic flowing through the switch.

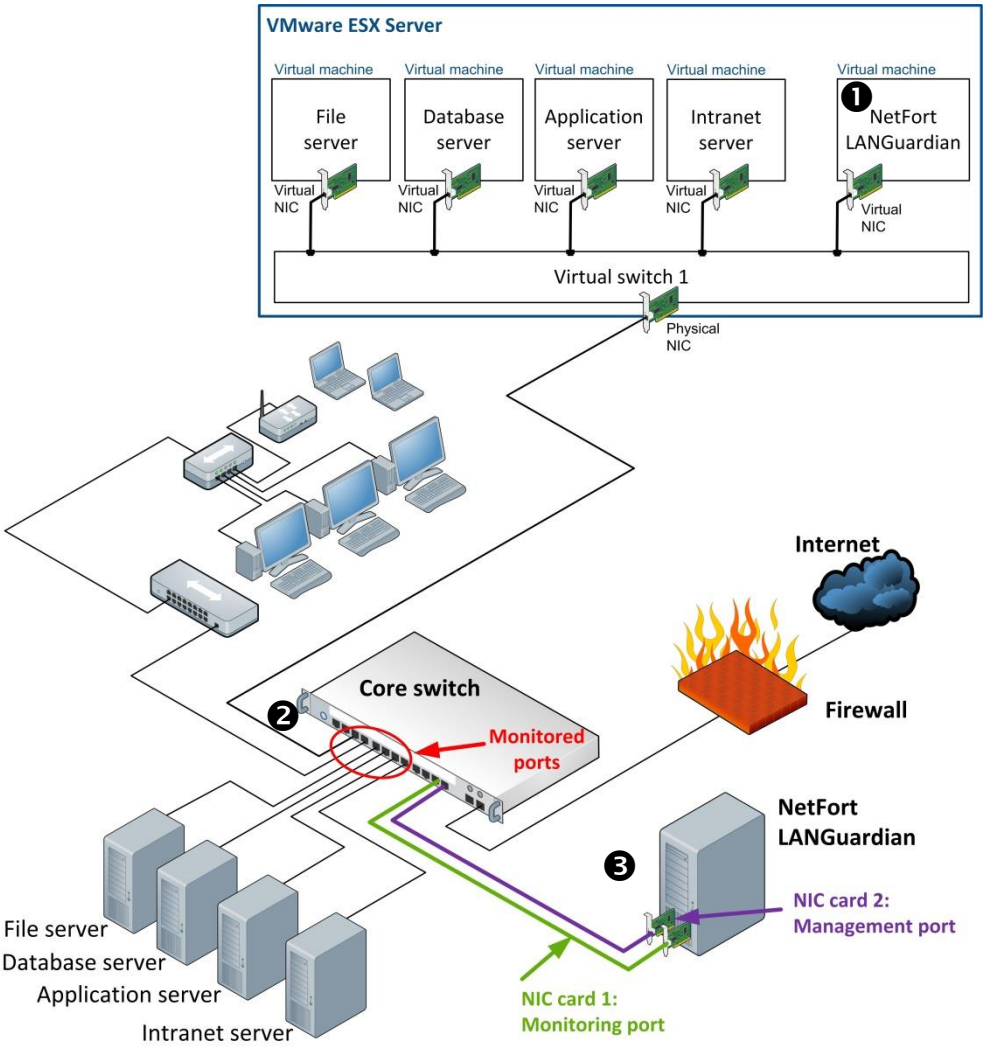
1.4.3 Monitoring physical network traffic with a LANGuardian virtual appliance

As well as monitoring traffic on your virtual network, a LANGuardian virtual appliance can monitor network traffic on your physical network. In this configuration, you must configure an additional sensor in the LANGuardian user interface and connect this sensor to a separate virtual switch, which in turn must be connected to the physical network. The diagram below illustrates this configuration.



1.4.4 Monitoring virtual network traffic with a physical LANGuardian device

LANGuardian can give you a single point of access to traffic information for your combined physical and virtual environment. The diagram below shows this configuration.



❶ A LANGuardian virtual appliance in the VMware ESX environment captures data from the virtual network switch.

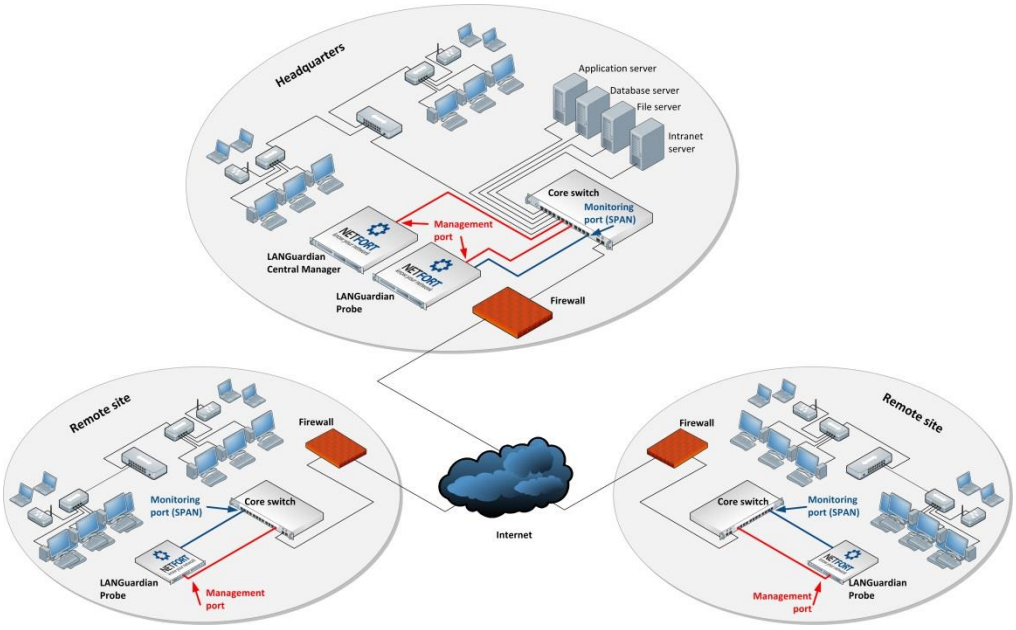
❷ The VMware ESX server is connected to the core switch on the physical network, and the port to which it is connected is a monitored port.

❸ A LANGuardian device on the physical network, which is connected to the monitoring port, can then capture and store the traffic data from the virtual network.

1.4.5 Monitoring large-scale enterprise networks with LANGuardian

You can deploy LANGuardian on any size of network, from a local office to a global enterprise network. In large networks that contain multiple core switches, you must deploy a LANGuardian instance for each core switch. You designate one instance as a **central manager** and each of the other instances as a **probe.** The probe instances do not have a traffic

database or user interface; instead, the traffic collection engine sends the traffic data it captures to the central manager instance, and the data is accessible through the user interface of the central manager instance. The following diagram shows a large enterprise network with one central manager and two probes.



1.4.6 Sensors

During installation, you connect one of the NICs on the LANGuardian system to the monitoring port on your network's core switch. The LANGuardian software automatically creates a sensor to associate that NIC with the software. LANGuardian instantly begins capturing network traffic and you can view the results in your web browser.

There are some situations where you might want to create more than one sensor in LANGuardian. For example, you might want to monitor your internal and external network traffic separately. In these situations, you need a monitoring port on your switch for each sensor and a corresponding NIC on your LANGuardian system. For example, if you have three sensors, you would need three monitoring ports on your switch and four NICs on your LANGuardian system – one for each of the sensors, and one to deliver the browser-based user interface.

Chapter 2

Chapter 2 - Installing and configuring LANGuardian

You can install LANGuardian on a machine that is connected to a physical network, or you can install it as a virtual machine in a virtual environment.

2.1 Before you begin

The method and requirements for installing LANGuardian vary depending on whether you are installing the application on a dedicated PC or in a VMware environment. The following table describes the differences.

	LANGuardian Dedicated PC	VMware Environment
Installation Method	Download the ISO image. See Section 2.2 Installing the LANGuardian ISO image.	Download and deploy the pre-configured virtual appliance. The virtualized version of LANGuardian is provided as a pre-configured VMware .OVA file that you can install with the VMware vSphere™ client. See Section 2.3 Installing the LANGuardian VMware appliance.
System Requirements	• 2 GHz or faster dual core processor • At least 2 GB RAM • At least 40 GB disk space for the traffic database	**Important!** The LANGuardian VMware appliance requires a dedicated network adapter on the VMware server. See Section 2.3.5 Setting up external monitoring. The virtual appliance is preconfigured to use the following resources: • One CPU • 800 MB RAM • 16 GB disk space You can adjust these values

		after installation. If you need to capture large amounts of traffic, please install and configure LANGuardian using the ISO image because then you can specify a suitable disk size.
Network Requirements	• Two network adapters; one for the management interface and one for the monitoring interface. The network adapter for the management interface connects to a standard network port. This adapter requires a fixed IP address. Before starting the installation, please ensure that you have obtained a: • Valid IP address • Subnet mask • Gateway address The network adapter for the monitoring interface connects to a monitoring (SPAN) port on your core switch.	During the installation, you will configure LANGuardian to join your network. You must use a fixed IP address. Before starting the installation, please ensure that you have obtained a: • Valid IP address • Subnet mask • Gateway address
Software Requirements	LANGuardian does not require a host operating system. You deploy it as a bare-metal install onto dedicated hardware. If you install LANGuardian on a machine that already has an operating system installed, please note that the existing operating system and all data on the machine will be irrevocably erased.	The LANGuardian VMWare appliance is suitable for installation on a VMware ESX hypervisor. It may be installed on VMWare ESX servers version 4.0 and ESXi® version 5.0. It may not be suitable for certain ESXi 4.0 platforms, however, you can still install LANGuardian in these environments using the ISO image.

2.2 Installing the LANGuardian ISO image

Warning!

LANGuardian does not require a host operating system. You deploy it as a bare-metal install onto a dedicated PC or server. If you install LANGuardian on a machine that already has an operating system installed, the existing operating system and all data on the machine will be irrevocably erased.

Installing LANGuardian from the ISO image is a three-part process:

1. Complete the bare-metal installation using the LANGuardian Setup Utility. In this part of the installation, you configure the hard disk on which LANGuardian will be installed, and you specify some network settings so that LANGuardian can install itself and join your network. See Section 2.2.1 Installing LANGuardian.

2. Configure a monitoring (SPAN) port on your core switch and connect the LANGuardian machine to this port. See Section 2.3.6 Configuring a monitoring port on the external network.

3. Access the LANGuardian user interface via a web browser and use the Configuration Wizard to complete the installation. You can also integrate LANGuardian with Active Directory. See Section 2.4 Using the LANGuardian Configuration Wizard.

After completing the LANGuardian installation, you can log on using the default username **Administrator**.

2.2.1 Installing LANGuardian

An ISO image is a single file that contains the entire contents of a CD. You can re-create the CD from the file by "burning" the image onto a blank CD using software such as ImgBurn, which is available free from **www.imgburn.com.**

Follow these steps to install LANGuardian from the ISO image:

1. Burn the ISO image onto a CD.

2. Insert the disc in the PC or server.

3. Boot the machine from the CD (you may need to modify the BIOS to enable booting from CD). The LANGuardian Setup utility runs when you boot the LANGuardian CD.

Note

If you are installing LANGuardian in a virtual environment, you will need to create a new virtual machine and boot it from the ISO image or installation media. Most environments (for example, VirtualBox and VMware) will ask you to specify the guest operating system. Choose CentOS 64-bit if it is available, otherwise choose an alternative 64-but Unix version such as Ubuntu or Red Hat.

```
LANGuardian Setup
-----------------

Copyright 2012 NetFort Technologies Limited. All rights reserved.

Welcome to the setup utility for LANGuardian.

This utility will guide you through the LANGuardian installation process. The
installation takes less than five minutes.

+-----------------------------------------------------+
| PLEASE NOTE:                                        |
|                                                     |
| This installation will overwrite any data or operating |
| system that exists on the selected hard disk.       |
|                                                     |
+-----------------------------------------------------+

Type YES to continue with the installation. Type NO to quit the setup program
without installing LANGuardian.

Do you want to continue with the installation [NO]?
```

Enter YES to continue with the installation.

4. Complete the LANGuardian Setup process. There are six steps as follows:

```
LANGuardian Setup
-----------------

Step 1 of 6: Select the installation disk

The following list shows the existing disks on this computer.

Disk ID   Description                                                    Size
-------------------------------------------------------------------------------
1         Western Digital WD5000B                                     100 GB
2         Maxtor                                                      400 GB
3         Hitachi SD160002                                            260 GB
4         Seagate HD Barracuda 7200 RPM                               500 GB

Please select the disk on which you want to install LANGuardian.

Enter the disk ID number:
```

Enter the disk ID number for the disk on which you want to install LANGuardian (note that any data already on the disk will be deleted).

```
LANGuardian Setup
-----------------

Step 2 of 6: Confirm the installation disk

You have chosen to install LANGuardian on this disk:

Description                                                        Size
-------------------------------------------------------------------------------
Maxtor                                                             400 GB


If you proceed with the installation, all data on this disk will be erased.
Type YES to continue with the installation. Type NO to quit the setup utility
without installing LANGuardian.

Do you want to continue [NO]?
```

Confirm the installation disk before continuing.

```
LANGuardian Setup
-----------------

Step 3 of 6: Select a network device for the LANGuardian user interface

LANGuardian requires at least two network interface cards (NICs). One NIC will
be assigned to the browser-based user interface. LANGuardian will use the
other NICs to capture network traffic data.

The following NICs are available on your system:

NIC ID    Description                                                    Status
------------------------------------------------------------------------------
1         Intel PRO/1000 Network Connection                            Connected
2         Intel PRO/1000 Network Connection                            Connected
3         Intel PRO/1000 Network Connection                            Connected
4         Marvell Yukon 88E805 PCI-E Gigabit Ethernet...           Not connected

Please select a NIC to assign to the user interface.

If you want to be sure of the ID of each NIC, disconnect all network cables
and reconnect them one at a time, pressing the R key after you connect each one.

Enter the NIC ID number or press the R key to refresh the list [R]:
```

Enter the NIC ID number for the management interface or press R to refresh the list.

```
LANGuardian Setup
-----------------

Step 4 of 6: Configure the user interface network device

You have chosen to assign this device to the LANGuardian user interface:

Description                                                    Status
------------------------------------------------------------------------------
Intel PRO/1000 Network Connection                              Connected

Please enter the following network settings:

LANGuardian computer IP address:    192.168.127.200
LANGuardian computer network mask:  255.255.255.0
Default gateway IP address:         192.168.127.1
DNS server IP address:              16.1.20.232

Press any key to continue with the installation.
```

Enter the following network settings:

- IP address – the static IP address of the management interface (this will be the address you enter in your web browser to access the LANGuardian home page).
- Subnet mask
- Gateway address
- DNS server address

At this stage in the installation process, no changes have been made to your system and your disk has not been modified. LANGuardian asks you to confirm your settings once again before beginning the installation.

```
LANGuardian Setup
-----------------

Step 5 of 6: Confirm settings

LANGuardian Setup will now complete the installation using these settings:

Disk Description                                                          Size
-------------------------------------------------------------------------------
2    Maxtor                                                               400 GB

NIC  Description                                                        Status
-------------------------------------------------------------------------------
3    Intel PRO/1000 Network Connection                                Connected

          LANGuardian computer IP address:  192.168.127.200
          LANGuardian computer network mask: 255.255.255.0
          Default gateway:
          DNS server

Type YES to continue with the installation. Type NO to quit the setup program
without installing LANGuardian.

Are you sure you want to install LANGuardian using these settings [YES]?
```

Enter YES to complete the installation.

```
LANGuardian Setup
-----------------

Step 6 of 6: Complete the installation

Please wait while LANGuardian Setup completes the installation.


LANGuardian Setup
-----------------

Finished!

LANGuardian has been installed successfully. Please remove the LANGuardian
CD and restart the system to complete the installation. After restart, you
can use the LANGuardian Management Utility on this console to change the
operating mode and network settings.

You can access the main LANGuardian user interface via a web browser at:

https://192.168.127.200

The first time you visit this URL, LANGuardian will display the Configuration
Wizard, which will guide you through the remaining configuration steps.

We hope you enjoy using LANGuardian.

The NetFort team (support@netfort.com)

Press any key to restart...
```

Wait for the installation to complete.

5. Remove the CD and press any key to restart the machine. The LANGuardian machine is now available on your network.

6. To access the LANGuardian user interface, start your preferred web browser and go to the LANGuardian home page at the IP address you specified during the installation. For example, if the IP address you specified during the installation is `192.168.10.200`, go to `https://192.168.10.200`.

7. The first time you log in to LANGuardian, it displays the Configuration Wizard. Follow the steps described in Section 2.4 Using the LANGuardian Configuration Wizard to complete the LANGuardian installation and begin monitoring traffic data.

2.3 Installing the LANGuardian VMware appliance

The steps to install and configure a LANGuardian VMware appliance are:

Step	Description	Refer to…
1.	Deploy the virtual machine on your VMware ESX infrastructure.	Section 2.3.1 Deploying the virtual appliance.
2.	Initialize the virtual appliance.	Section 2.3.2 Initializing the virtual appliance.
3.	Configure LANGuardian for local ESX Server monitoring.	Section 2.3.3 Setting up local ESX Server monitoring.
4.	Access the LANGuardian user interface via a web browser and use the Configuration Wizard to complete the installation.	Section 2.4 Using the LANGuardian Configuration Wizard.
Optional advanced configuration		
5.	Monitor additional virtual switches.	Section 2.3.4 Monitoring additional virtual switches.
6.	Set up external monitoring.	Section 2.3.5 Setting up external monitoring.
7.	Configure a monitoring port on the external network.	Section 2.3.6 Configuring a monitoring port on the external network.

2.3.1 Deploying the virtual appliance

Follow these steps to deploy the LANGuardian virtual appliance:

1. Open the vSphere client and choose **Deploy OVF Template** from the **File** menu.
2. On the **Source** page, click **Deploy From File**.
3. Browse to find the LANGuardian .OVA file that you downloaded from the **Download** page.
4. Review the OVF template details.
5. Select the datastore in which you want to store the virtual machine and its virtual disk files.
6. Map the network in the template (VM Network) to a network in your inventory.
7. Review the settings and click **Finish** to deploy the virtual machine.

The vSphere client will load the LANGuardian appliance and install it in the ESX server.

After the installation completes, LANGuardian will appear in a powered-down state in the vSphere client.

2.3.2 Initializing the virtual appliance

Follow these steps to initialize your newly-installed LANGuardian appliance:

1. Open the vSphere client, select your virtual machine, and power it on.

2. Click the **Console** tab, wait for the virtual machine to boot, and verify that it boots correctly.

3. The command-line interface (CLI) LANGuardian Management Utility has a menu of options for basic administration of the virtual machine.

```
LANGuardian Management Utility
------------------------------

System commands             System configuration

1. View status              5. Select network device
2. Restart LANGuardian      6. Configure network device
3. Shutdown LANGuardian     7. Set operating mode
4. Ping command             8. Reset web user interface password

Enter a command [1-8] (or type EXIT to exit):
```

   The option that is relevant for initial configuration is option `6` (`Configure network device`). Type `6` and press Enter.

```
LANGuardian Management Utility
------------------------------

Configure the network device

You have chosen to assign this device to the LANGuardian management
interface:

Description                                          Status
-------------------------------------------------------------------------------
Intel PRO/1000 Network Connection           Connected

Please enter the following network settings:

LANGuardian computer IP address [192.168.127.200]: 192.168.127.200
LANGuardian computer network mask [255.255.255.0]: 255.255.255.0
Default gateway IP address [192.168.127.1]: 192.168.127.1
DNS server IP address [16.1.20.232]: 16.1.20.232

Press ENTER to return to the main menu:
```

   Specify the IP address, subnet mask, default gateway address, and DNS server IP address.

4. Visit the home page at the IP address you specified during the installation. For example, if the IP address you specified during the installation is `192.168.10.200`, the address of your LANGuardian home page will be `https://192.168.10.200`.

The first time you access the LANGuardian user interface, it displays the LANGuardian Configuration Wizard. Follow the wizard steps to complete

the configuration of your LANGuardian system. A predefined sensor will be in place to enable LANGuardian to monitor traffic once you set up local ESX server monitoring.

2.3.3 Setting up local ESX Server monitoring

You must activate promiscuous mode on the ESX Server virtual switch to enable LANGuardian to monitor the internal traffic in your ESX Server environment. The steps are as follows:

1. Open the host settings for the ESX Server and click the **Configuration** tab.
2. Click **Properties…** to view the properties for the virtual switch.
3. Edit the properties, then click the **Security** tab.
4. Click **Accept** from the **Promiscuous Mode** drop-down list, then click **OK**.

LANGuardian will immediately begin monitoring all traffic flowing through the virtual switch.

2.3.4 Monitoring additional virtual switches

You can monitor additional virtual switches with LANGuardian by adding more network adapters to the LANGuardian virtual appliance and configuring LANGuardian sensors to monitor them. The steps to add a network adapter are as follows:

1. Open the settings for the LANGuardian appliance and click the **Edit Settings** tab.
2. Click the **Add** button, select **Ethernet Adapter**, and click **Next**.
3. Specify **E1000M** in the **Adapter Type** field.
4. In the **Network Label** field, select the virtual switch you want to monitor.
5. Restart the LANGuardian appliance to allow it to detect the new network adapter.

After the appliance has rebooted, log on to the LANGuardian user interface and add a new sensor. The steps are as follows:

1. Click on  in the LANGuardian menu bar and select **Sensors**.
2. On the **Sensors** page, click **Add New Sensor**. LANGuardian will display a list of network adapters, including the one you just added.
3. Select the adapter you just added and click **Next**.

4. Assign a name to the new sensor, alter the parameters as required, and click **Create**.

To enable the LANGuardian appliance to monitor the additional virtual switch, configure the switch to accept promiscuous mode connections as described above.

2.3.5 Setting up external monitoring

After you install LANGuardian, it will be connected to a network adapter in your ESX Server environment. This adapter provides connectivity to the web browser user interface. To enable LANGuardian to monitor traffic flowing through an external network switch, you must create an additional virtual switch and network adapter in the ESX Server, associate them with a physical adapter on the ESX server, and connect the physical adapter to the external switch. The additional virtual network switch and adapter are necessary because:

- Accessing traffic on a SPAN port requires a dedicated network adapter.
- Due to the volume of traffic generated by a monitoring session, using a dedicated virtual switch and adapter helps to avoid performance problems with other virtual machines.

Follow these steps to create the new virtual switch:

1. Open the host settings for the ESX Server and click the **Configuration** tab.
2. Click on **Networking** in the **Hardware** menu, then click **Add Networking...**
3. In the Add Network Wizard:
    a. Click on **Virtual Machine** in the list of connection types, then click **Next**.
    b. Select **Create a New Virtual Switch** and click **Next**.
    c. Select a network adapter from the list of available adapters and click **Next**.
    d. Enter the switch name in the **Network Label** field and click **Next**.
    e. Click **Finish**.

Follow these steps to create a new virtual adapter:

1. Open the settings for the LANGuardian appliance and click the **Edit Settings** tab.

2. Click on the **Add** button, select **Ethernet Adapter,** and click **Next.**
3. Specify **E1000** in the **Adapter Type** field.
4. In the **Network Label** field, select the virtual switch you have just created.
5. Restart the LANGuardian appliance to allow it to detect the new network adapter.

After the appliance has rebooted, log on to the LANGuardian user interface and add a new sensor. The steps are as follows:

1. Click on  in the LANGuardian menu bar and select **Sensors**.
2. On the **Sensors** page, click **Add New Sensor**. LANGuardian displays a list of network adapters, including the one you just added.
3. Select the adapter you just added and click **Next**.
4. Assign a name to the new sensor, alter the parameters as required, and click **Create**.

Note

The LANGuardian base product allows you to create two local sensors. To add more than two sensors requires additional licensing. For more information about LANGuardian licensing, please contact the NetFort support team.

Follow these steps to configure the virtual switch to accept promiscuous connections:

1. Open the host settings for the ESX Server and click the **Configuration** tab.
2. Click **Properties...** to view the properties for the virtual switch.
3. Edit the properties, then click the **Security** tab.
4. Click **Accept** from the **Promiscuous Mode** drop-down list, then click **OK**.

2.3.6 Configuring a monitoring port on the external network

Setting up the LANGuardian VMware appliance to monitor an external network prepares it to accept traffic data from the network, but you must also configure the core switch on the external network to provide traffic data to the appliance.

Network core switches typically have a port mirroring capability that enables you to set up a monitoring port (called a SPAN port on Cisco switches) through which you can capture network traffic for analysis. For details, see Section 1.2 Architecture.

The steps to configure a monitoring port are specific to each switch. See the core switch documentation page on the NetFort website for links to documentation for popular switches:

www.netfort.com/downloads/documentation/core-switch-documentation

If you need help configuring a monitoring port on your switch, contact our support team for free, no-obligation assistance.

2.4 Using the LANGuardian Configuration Wizard

After you install LANGuardian from the ISO image, or deploy it as a VMware virtual appliance, you can access the user interface from a web browser.

The first time you access the LANGuardian user interface, it displays the Configuration Wizard. Use the wizard to complete your LANGuardian installation and begin monitoring traffic data.

Note

If your browser displays a note about a potential issue with the security certificate for the website, you can ignore the message and continue to the website.

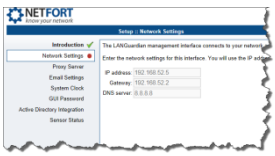
The configuration steps are as follows:

1. Accept the license agreement.

You must accept the license agreement to complete the configuration.

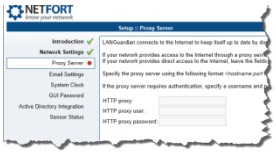
You also have the option to enable diagnostic feedback on this page.

2. Verify the network settings.



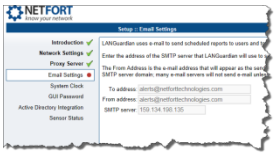
Verify the network settings that you entered when booting the ISO image or deploying the VMware appliance.

3. Specify a proxy server for LANGuardian updates. This page is not displayed if LANGuardian can successfully contact the NetFort website.



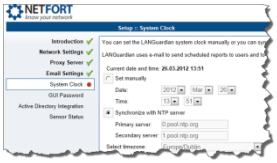
LANGuardian connects to the Internet to download software updates from the NetFort Technologies website. If your network provides access to the Internet through a proxy server, enter the proxy address, proxy user, and password.

4. Specify the SMTP server to use for email.



LANGuardian uses email to send scheduled reports to users and issue alerts when specified incidents occur or thresholds are breached. Enter the address of the SMTP server that LANGuardian uses to send email.

5. Set the system clock.



You can set the LANGuardian system clock manually or you can synchronize it automatically with a reference clock on the Internet.

6. Set the GUI password.

Set the password that you will use to log on to the LANGuardian user interface. The default username, which you will use when you first log on, is **Administrator**.

7. Specify the Active Directory details.

If you plan to integrate LANGuardian with Microsoft Active Directory, enter the details here.

You must ensure that the appropriate services are started and firewall rules are in place on the domain controller to enable LANGuardian to access it over TCP ports 445 and 139.

8. Review the sensor status.

Review the sensor status to make sure LANGuardian is connected to your network and is capturing traffic.

9. Click **Finish** to complete the configuration. LANGuardian displays the login page.

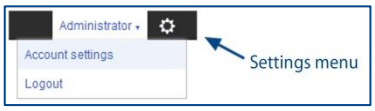
You are now ready to begin using LANGuardian to monitor activity on your network. You may need to modify your switch configuration to control what traffic is monitored by LANGuardian. See Chapter 3 for information on using LANGuardian.

2.5 Logging on to LANGuardian

After you complete the wizard steps, LANGuardian will display the LANGuardian logon page. You can log on with the default username **Administrator** and the password you specified in the configuration wizard.

LANGuardian comes pre-configured with a number of standard dashboards and reports, which you can use as-is or customize according to your requirements. LANGuardian begins monitoring your network immediately after installation, so you should see traffic data appearing in the reports within a few minutes. Please contact us if you encounter any problems when installing or configuring LANGuardian.

You can log out by choosing **Logout** from the **Administrator** menu in the top right corner of the LANGuardian window.



To log on again, use the default username **Administrator** and the password you specified in the configuration wizard. You can create additional usernames and change passwords in the **Configuration** page, which is accessible from the **Settings** menu.

You can create additional usernames and change passwords in the **Configuration** page, which is accessible from the **Settings** menu.

2.6 Integrating LANGuardian with Active Directory

With the Directory Services Integration module enabled, LANGuardian integrates with a Microsoft Windows® environment to access additional information that it incorporates into reports, trends, and dashboards. The Directory Services Integration module provides LANGuardian with:

- User names and department information from Active Directory.
- Logon and logoff information from the domain controller event logs.

LANGuardian includes this information in the reports and dashboards that it creates, making them more readable and more useful for troubleshooting and monitoring activity on your network.

Integrating LANGuardian with Windows is a two-part process:

1. Configure your Windows server to accept connections from LANGuardian, return information from Active Directory, and record details of every network logon.

2. Configure LANGuardian to connect to Windows.

When you complete this process, LANGuardian reports will include details from your Windows domain controller.

2.6.1 Active Directory domain account

Integrating LANGuardian with Active Directory requires use of an account in the Active Directory domain. You specify the account credentials in the Configuration Wizard when you first install LANGuardian, which uses the credentials to authenticate itself when querying the domain.

LANGuardian never makes changes to the information stored in Active Directory. All queries that it submits to the domain controller are read-only. LANGuardian uses the SMB (System Message Block) protocol to query the domain controller.

We recommend that you create a dedicated account to associate your LANGuardian instance with Active Directory. If you do this, ensure that the account has the following rights: **Deny logon locally** and **Manage auditing and security log**. The account does not require Administrator privileges.

2.6.2 Configuring your Windows server

To configure your Windows server to work with LANGuardian, you must create a LANGuardian-specific account on the Windows domain, give the account the required permissions, and enable event log auditing.

You must also ensure that the appropriate services are started and firewall rules are in place to enable LANGuardian to access the server over TCP ports 445 and 139.

2.6.2.1 Create a LANGuardian account

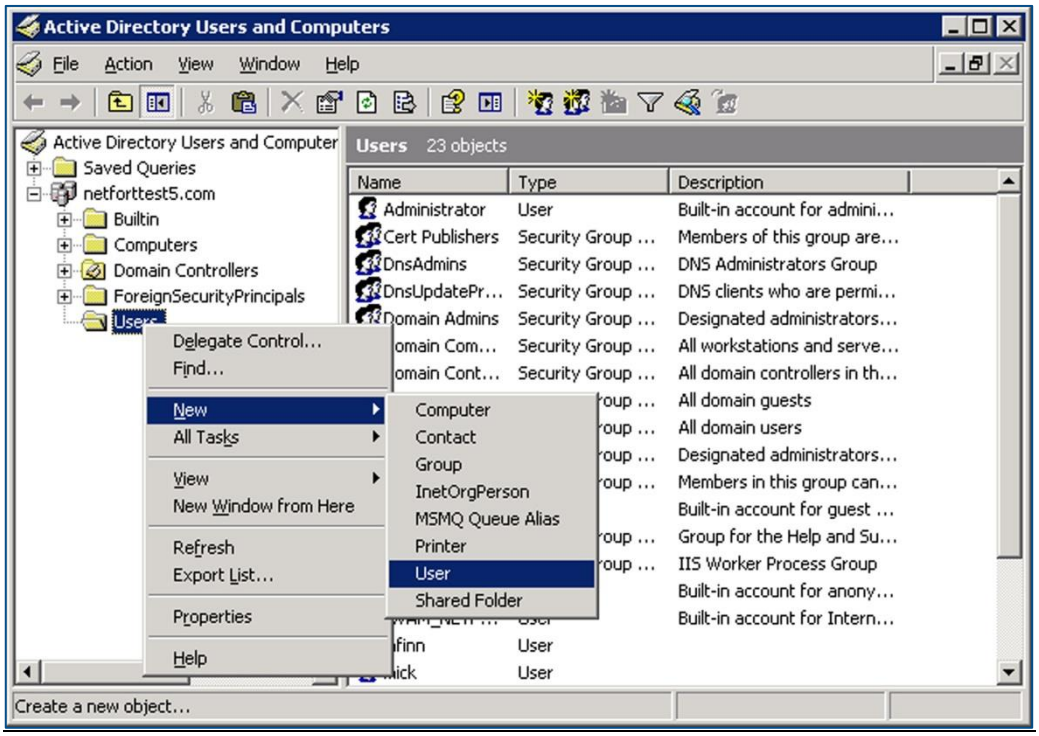
Follow these steps to create a LANGuardian account in the Windows domain:

1. Log on to a domain controller.

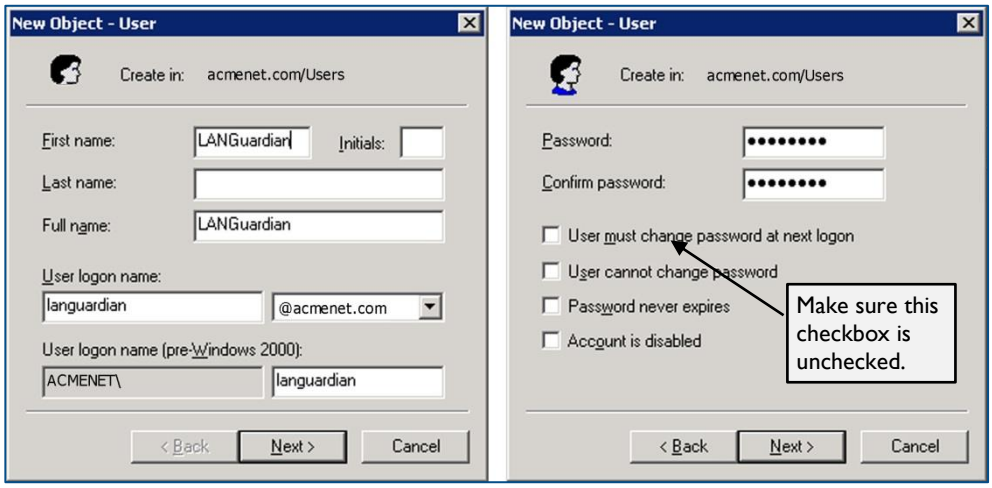
2. Click **Start → Administrative Tools → Active Directory Users and Computers**.

3. Select the domain to which you want to add the LANGuardian user.

4. Click **Users → New → User**.



5. Enter the user account details and password.



Make sure the **User must change password at next logon** checkbox is left unchecked.

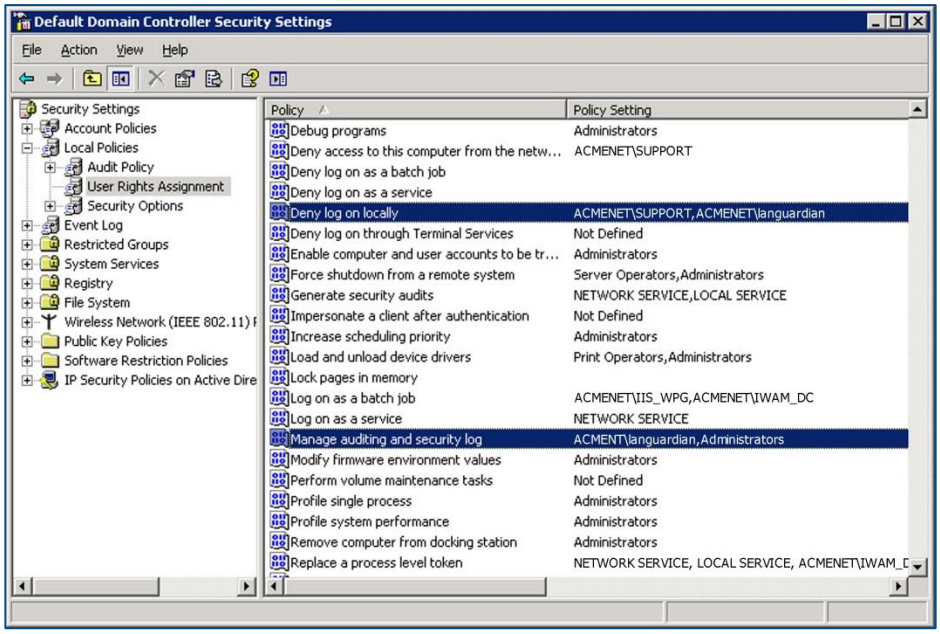
2.6.2.2 Configure the account security attributes

Follow these steps to configure the appropriate security on the LANGuardian Windows account:

1. Click **Start → Administrative Tools → Domain Controller Security Policy**.

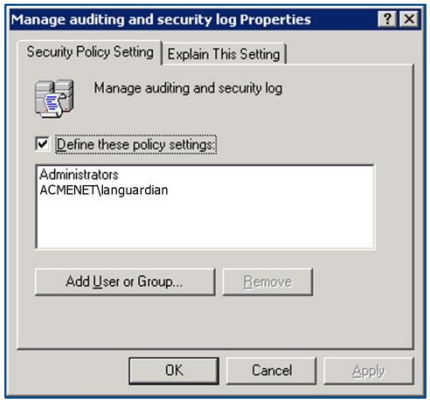
2. Click **Local Policies → User Rights Assignment.**

3. Add the LANGuardian user account to the policy settings **Deny log on locally** and **Manage auditing and security log.**



Double-click each policy name to display its **Properties** dialog box.

4. In the Properties dialog box, click **Add User or Group…** and add the LANGuardian account to the list of users.



2.6.2.3 Configure event log auditing

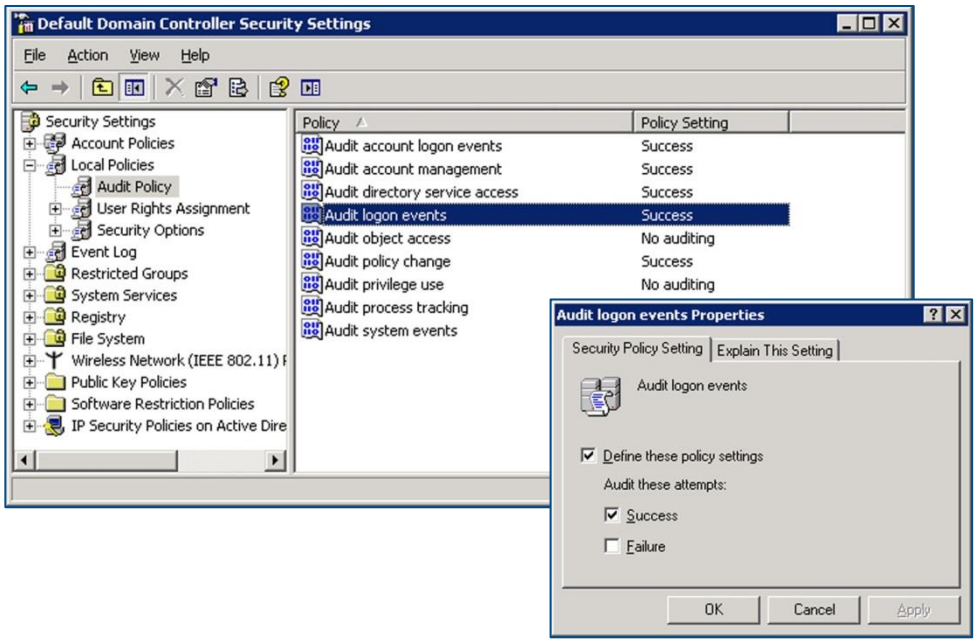
In a Windows server, the event log records details of all system and user activity (events). There are many different types of event, and you can configure the Windows server to record only the events that are of interest. If you record logon events, LANGuardian can include details of user logons in its reports, trends, and dashboards.

Follow these steps to enable event log auditing:

1. Click **Start → Administrative Tools → Domain Controller Security Policy.**

2. Click **Local Policies → Audit Policy.**

3. Double-click the policy **Audit logon events.**



4. Check the **Success** checkbox to audit successful logon attempts in the event log.

In a default Windows Server installation, the maximum event log size is set to 512 KB. We recommend increasing the size of the security log to 20 MB.

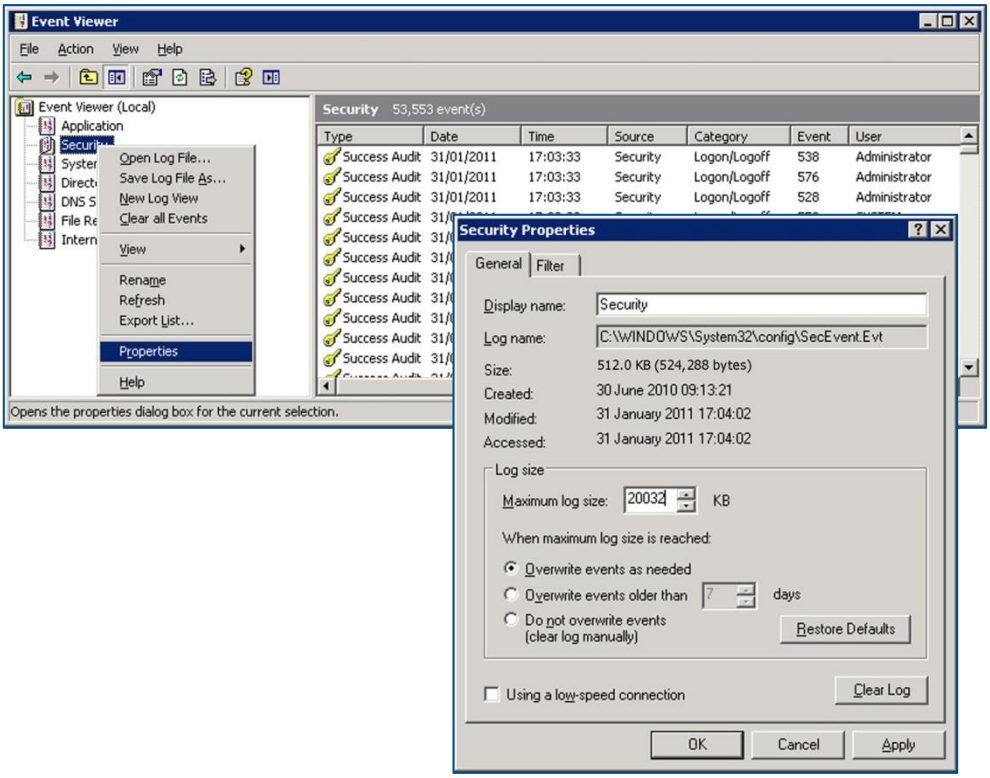
Follow these steps to set the maximum event log size:

1. Click **Start → Administrative Tools → Event Viewer.**

2. Right-click on the **Security** log.

3. Click **Properties** on the pop-up menu.

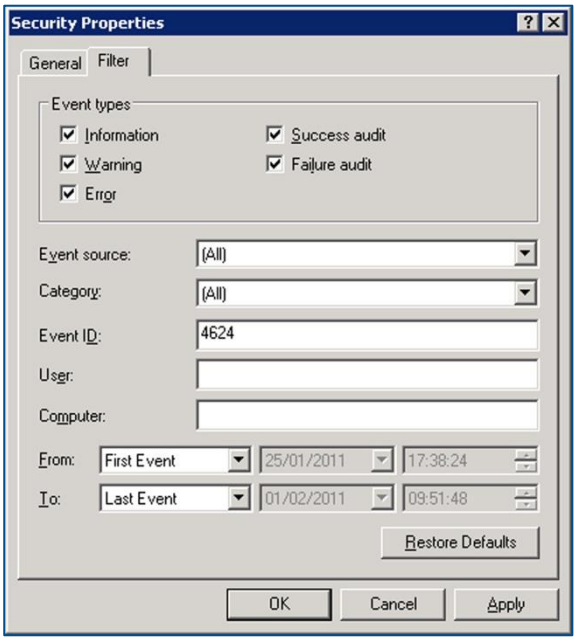
4. On the General tab, set the **Maximum log size** to 20032 MB.



5. Under **When maximum log size is reached,** click the **Overwrite events as needed** radio button.

6. To verify that the Windows domain controller is correctly recording logon events, click the **Filter** tab and in the **Event ID** field, enter the ID that matches network logon events on the version of Windows Server your domain controller is running:

If the domain controller is running…	The Event ID is…
Windows Server 2008 R2	4624 (Logon Event)
Windows Server 2008	4624 (Logon Event)
Windows Server 2003	540 (Logon Event) 672 (Account Logon Event)
Windows 2000 Server	672 (Account Logon Event)



7. Click OK. If the Event Viewer displays some events, your event log auditing is configured correctly.

2.6.3 Configuring LANGuardian to connect to Active Directory

LANGuardian uses a Windows domain account to authenticate itself and query the server for user information and login activity. The domain account must have the necessary privileges to access the Active Directory global catalog and Windows event logs.

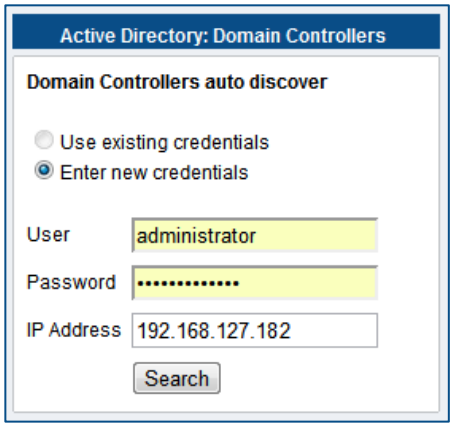
LANGuardian has an auto-discover facility that identifies every domain controller (DC) in a domain. To enumerate the DCs, it directs an LDAP query to a seed server, which returns a list of all DCs in the domain. LANGuardian then queries each DC to request its version.

From the list of DCs, select the ones you want LANGuardian to know about. LANGuardian will save the details in its configuration database and query them periodically for up-to-date information. We recommend that you add all DCs unless you are sure they do not authenticate users. If a DC authenticates users and LANGuardian does not know about it, the information you see in LANGuardian graphs and reports might be incomplete.

Follow these steps to connect LANGuardian with Active Directory:

1. Click on ⚙ in the LANGuardian menu bar and select **Configuration**.
2. On the Configuration page, scroll down to the section on **Identity Configuration**.
3. Click **Configure support for Active Directory identity logging**.

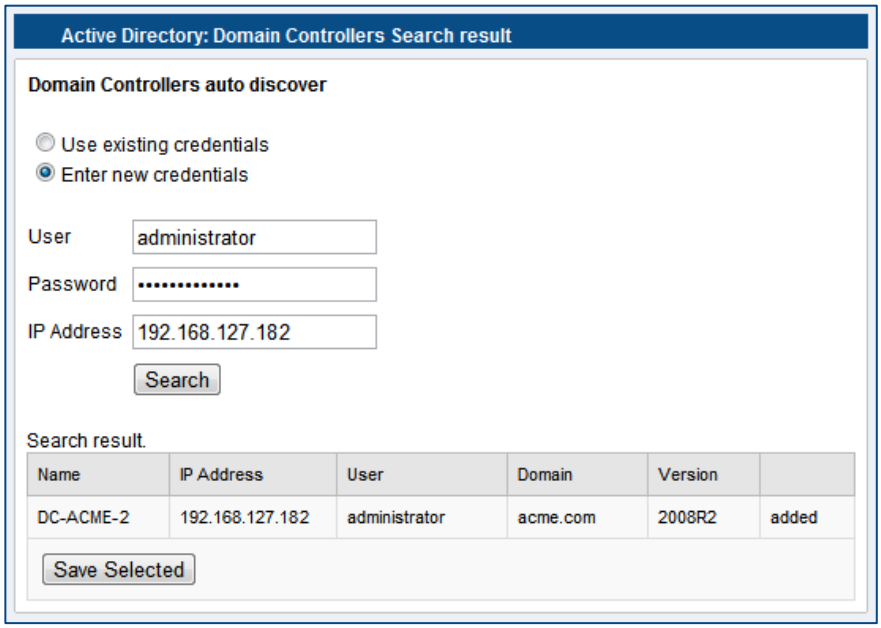
4. LANGuardian displays the **Active Directory: List of servers** page. No servers will be listed when you first access the page. To add a server, click **Add new server**.
5. Click the **Enter new credentials** radio button.
6. LANGuardian displays the **Domain controllers auto discover page**.



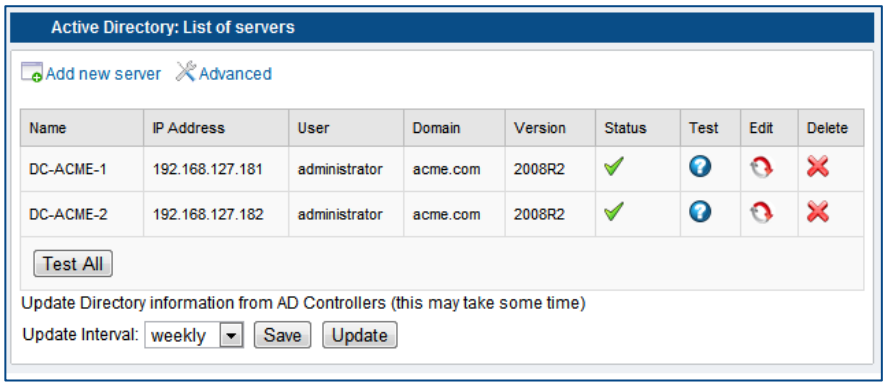
Enter the following details:

- **User**: the username of the domain account.
- **Password**: the password for the domain account.
- **IP Address**: the address of a domain controller.

7. Click **Search**. LANGuardian will search for and display all Active Directory domain controllers in the domain.
8. If LANGuardian finds a match for the IP address, it displays the details. If you want to add the domain controller, tick the checkbox opposite the controller name then click **Save Selected**.



9. LANGuardian adds the domain controller to the list of servers.



Notes

You may want to consider creating a dedicated account to associate your LANGuardian instance with Active Directory. If you do this, ensure that the account has the following rights: **Deny logon locally** and **Manage auditing and security log**.

On your domain controllers, configure the security settings to audit logon events.

2.6.4 Configuring the update interval

LANGuardian maintains a database of Active Directory user and group membership information, which it incorporates into the reports and graphs that it creates. To keep this database up-to-date, LANGuardian issues LDAP queries against the domain at regular intervals. You can configure LANGuardian to execute these queries hourly, daily, weekly, monthly, or never.

To configure the interval:

1. In the **Active Directory: List of servers** page, select a value from the Update Interval drop-down list.

2. Click **Save.**

As well as scheduling regular updates, you can update the directory information at any time by clicking the **Update** button.

2.6.5 Eventlog Queries

LANGuardian periodically reads the Security event log of all DCs that are configured in its database, and it extracts details of all Logon and Account Logon events. The details it extracts are as follows:

- Account name that logged on
- Time of domain logon
- IP address of client system

LANGuardian stores this information in its database and incorporates it in reports and graphs. For example, you can see who was the last user to log on to each client system in the domain, who opened or deleted a specific file, or when a specific user logged on to or logged of a client machine.

2.7 Storage management, archiving, and backup

There are no specific storage requirements for LANGuardian because it uses whatever locally attached storage is available to it. The larger the disk, the more traffic data you can store. The amount of storage you need for your network traffic depends on factors such as the overall traffic volume, the types of traffic and events you want to monitor, the number of sensors, and the amount of historical data you want to have available online.

A storage example

A recent examination of a university site where LANGuardian is deployed shows that a 150 GB disk can store 11 weeks' worth of traffic and event data for a user population of over 12,000 users. Extrapolation of this figure implies that a 1 TB disk could store over 70 weeks' worth of data. But remember, every network is different.

2.7.1 How storage works

When LANGuardian is running on your network, it continually generates data from traffic analysis and intrusion detection events. It stores the data in the proprietary LANGuardian database until a specified upper limit of the available locally attached storage space is used. This limit is referred to as the **high point,** and it is set to 80% of the available storage by default.

When the database size reaches the high point, LANGuardian frees storage space by deleting or archiving the oldest data, purging it from the database until a specified lower limit of the available storage is reached. This limit is referred to as the **low point**, and it is set to 50% of the available storage by default.

2.7.2 How archiving works

In its default configuration, LANGuardian purges traffic from the database when the high point is reached, reducing the database to the size specified by the low point. However, many networks have security policies or compliance obligations that require traffic to be retained for long periods. To meet these requirements, you can configure LANGuardian to archive the traffic it purges from the database.

With archiving enabled, LANGuardian creates an archive when the database reaches the high point, reducing the database size to the low point. You can configure LANGuardian to store the archives on its locally attached storage or copy them to a network location via FTP (File Transfer Protocol) or SCP (Secure Copy Protocol).

When you configure LANGuardian to store archives locally, it uses the storage space not allocated to the traffic database. For example, if the high point is set to 80% of available storage, the remaining 20% is available for storing archives. If the space available for archives is full when LANGuardian tries to create an archive, it deletes the oldest archive to create space.

Each time LANGuardian creates a new database archive locally, it notifies the system administrator by email. The email includes a link to the archive so that the administrator can download the file and store it externally. Archives are created as compressed tar files and have the file extension **.tar.gz**.

As an alternative to storing database traffic locally and manually downloading the archives, you can configure LANGuardian to automatically store the archives at a remote location.

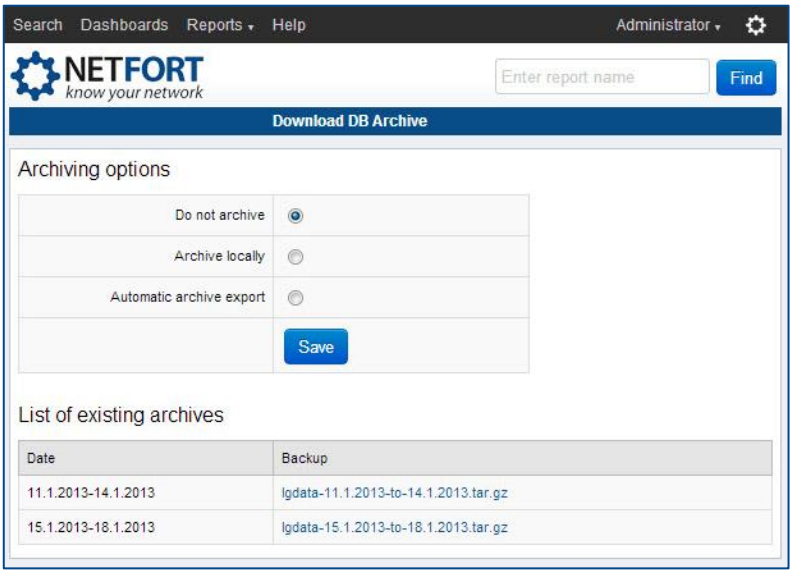
2.7.3 Configuring LANGuardian archiving

Follow these steps to configure LANGuardian database archiving::

1. Click on  in the LANGuardian menu bar and select **Configuration**.

2. On the Configuration page, scroll down to the section on **Archives**. Click **Export a LANGuardian database archive**.

3. LANGuardian displays the **Download DB Archive** page.

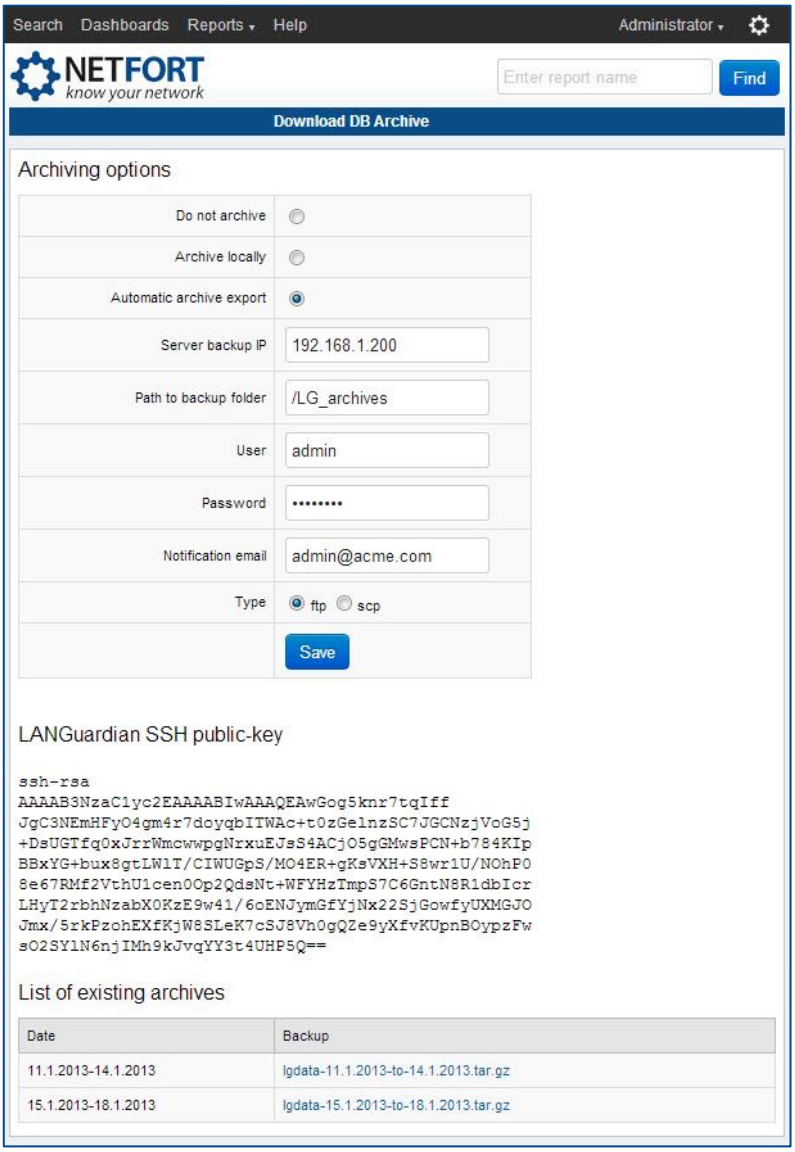


The default setting is **Do not archive**.

4. If you change the archiving option to **Archive locally**, LANGuardian will create an archive when the database size reaches the high point. When local archiving is enabled, LANGuardian shows a list of archives that are available for download.

5. If you change the archiving option to **Automatic archive export**, Each time the database storage reaches the high point, LANGuardian will create an archive each time the database storage reaches the high point, export it to the specified location, and send an email to the specified address.

   When you select the **Automatic archive export** option, the **Download DB Archive** page expands to display additional fields into which you can enter details of the remote location where the archives will be stored.



The fields are as follows:

- Server backup IP – the IP address of the FTP or SCP server on which you want to store the archives.
- Path to backup folder – the path to the backup folder on the FTP or SCP server.
- User – the username for the account on the FTP or SCP server.
- Password – the password for the account on the FTP or SCP server.
- Notification email – the email address to which notifications will be sent each time an archive is exported.
- Type – the protocol to use when exporting the archive.

If you use SCP to archive the LANGuardian database, you can use password-free authentication by leaving the Password field blank and adding the LANGuardian SSH public key to the list of authorized keys on your server.

On Unix-based systems, authorized keys are typically stored in

```
/home/username/.ssh/authorized_keys
```

6. Click **Save** to store the archive option in the LANGuardian configuration settings.

2.7.4 Checking storage usage

After you install LANGuardian and run it for a few days, you can accurately estimate the amount of storage you need on an ongoing basis. LANGuardian allows you to check to storage usage as follows:

1. Click on  in the LANGuardian user interface and select **Configuration**.

2. Click on **Check the database usage**. LANGuardian displays the amount of storage used since the date displayed.

2.7.5 Importing database archives

Note

We strongly recommend that you contact the NetFort support team at support@netfort.com before you import any archived data.

If you want to analyze network traffic data that is no longer available online, you can import archived data back into LANGuardian. This feature is useful in situations where you need to investigate past events such as file deletions, database transactions, or Internet downloads.

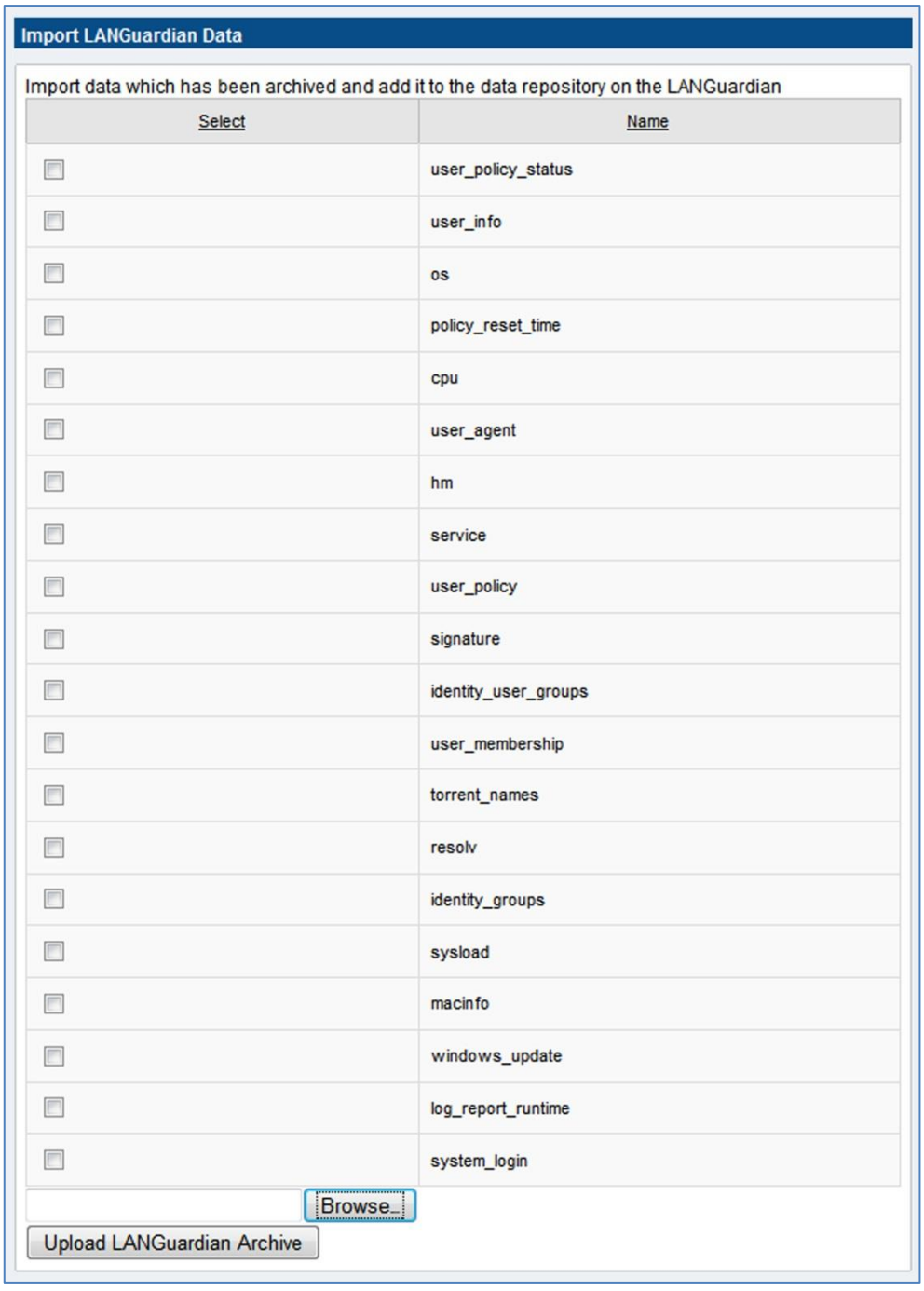
Some of the information that LANGuardian includes in database archives can change between the time a database is exported and the time it is imported back into LANGuardian (for example, a computer might have an upgraded operating system, or an IP address might resolve to a different hostname). Because of this, when LANGuardian creates a database archive, it supplements the traffic data with additional information that enables it to accurately report on the state of the network at the time of archive creation. This additional information can, when imported back into LANGuardian, conflict with the corresponding information on the live system.

To prevent this from happening, LANGuardian allows you to choose which items of additional information to import when you import a database

archive. We recommend that you include only the information that is relevant to the analysis you want to perform on the imported data.

Follow these steps to import a database archive:

1. Click on ⚙ in the LANGuardian menu bar and select **Configuration**.
2. On the Configuration page, scroll down to the section on **Archives**. Click **Import a LANGuardian database archive.**
3. LANGuardian displays the **Import LANGuardian Data** page.



4. Check the boxes to select the additional data items you want to include in the import.

5. Click the **Browse** button and select the archive you want to import.

6. Click **Upload LANGuardian Archive** to complete the import.

After you import the data, it will become available through the LANGuardian user interface and be included in all of the existing dashboards, reports, and trends. If you want to focus specifically on the imported data, you might need to create custom reports that focus on the dates covered by the archive.

2.7.6 Customizing the database high point and low point

In a default LANGuardian installation, the database high point is set to 80% of the available disk space and the low point is set to 50%. These have been shown to be the optimal values for typical networks where the available storage is well matched to the amount of traffic on the network. In rare situations, LANGuardian can benefit from changes to the high and low points. It is not possible to change these values through the user interface. Please contact NetFort Technologies Technical Support if you think the values need to be changed for your network.

2.8 Managing LANGuardian from the command line

If you cannot use a web browser to access the LANGuardian user interface, you can manage LANGuardian from the command line. To start the command line interface, go to the system where LANGuardian is installed and log on to the Rescue account. When LANGuardian is installed but not yet configured, you do not need a password to access the Rescue account. When LANGuardian is configured, you need a password to access the Rescue account. To reset the Rescue account password, click on  in the LANGuardian menu bar, select **Configuration**, and select **Change the password for the rescue account**.

When you log on to the Rescue account, the Management Utility is displayed. The menus on the Management Utility vary depending on whether the LANGuardian system is operating as a central manager or a probe. See Section 1.4.5 Monitoring large-scale enterprise networks with LANGuardian for more information about central manager and probe mode.

Note

Please use the command line with caution. You may make the LANGuardian system inoperable by issuing commands from the command line.

2.8.1 Managing a central manager

When you start the Management Utility on a LANGuardian system that is acting as a central manager, the following window is displayed:

```
LANGuardian Management Utility
------------------------------

Copyright 2012 NetFort Technologies Limited. All rights reserved.

Welcome to the management utility for LANGuardian 10.0.

Use this utility to modify LANGuardian network settings, reset the
Administrator password, and change the operating mode.

+-------------------------------------------------------------------------+
| PLEASE NOTE:                                                            |
|                                                                         |
| Some of the commands available in the management utility can make your   |
| LANGuardian system inoperable. Please be very careful when using them.  |
|                                                                         |
| For day-to-day operation and configuration of your LANGuardian system,  |
| you can access LANGuardian through the web user interface at this URL:  |
|                                                                         |
| https://192.168.127.200/                                                |
+-------------------------------------------------------------------------+

Press ENTER to access the management utility menu:
```

Press Enter to view the Management Utility menu.

```
LANGuardian Management Utility
------------------------------

System commands                 System configuration

1. View status                  5. Select network device
2. Restart LANGuardian          6. Configure network device
3. Shutdown LANGuardian         7. Set operating mode
4. Ping command                 8. Reset web user interface password

Enter a command [1-8] (or type EXIT to exit):
```

The Management Utility menu is divided into system commands and system configuration. To select a menu option, type a number and press Enter.

2.8.1.1 Viewing the status of a LANGuardian central manager

To view the status of the LANGuardian central manager, type 1 and press Enter. The status of the system is displayed.

```
LANGuardian Management Utility
------------------------------

Status
------
Network interface:      em0 (Intel PRO/1000 Network Connection)
Management IP address:  192.168.127.200
Netmask:                255.255.255.0
Default gateway:        192.168.127.1
DNS server:             16.20.1.232

Operating mode:         Central Manager
LANGuardian version:    10.0
Web user interface URL: https://16.20.154.200
Uptime:                 3 hrs 40 mins

Press ENTER to return to the main menu:
```

2.8.1.2 Restarting the LANGuardian central manager

To restart the LANGuardian Central Manager, type 2 and press Enter. You are prompted to type Y or N to confirm whether or not you want to restart the system. The default is N.

2.8.1.3 Shutting down the LANGuardian central manager

To shut down the LANGuardian Central Manager, type 3 and press Enter. You are prompted to type Y or N to confirm whether or not you want to shut down the system. The default is N.

2.8.1.4 Running the ping command

To run the ping command and check that your LANGuardian system is connected to the network, type 4 and press Enter. The following screen is displayed.

```
LANGuardian Management Utility
------------------------------

Ping command

Use the ping command to verify that your LANGuardian system is correctly
connected to the network.

Enter the IP address to ping:
```

Type the IP address that you want to ping and press Enter.

2.8.1.5 Selecting a network device for the user interface

To select a network device for the LANGuardian browser-based user interface, type 5 and press Enter. The following screen is displayed.

```
LANGuardian Management Utility
------------------------------

Select a network device for the LANGuardian management interface

LANGuardian requires at least two network interface cards (NICs). One NIC will
be assigned to the browser-based user interface. LANGuardian will use the
other NICs to capture network traffic data.

The following NICs are available on your system:

NIC ID  Description                                    Status
-------------------------------------------------------------------------------
1       Intel PRO/1000 Network Connection              Connected
2       Intel PRO/1000 Network Connection              Connected
3       Intel PRO/1000 Network Connection              Connected
4       Marvell Yukon 88E805 PCI-E Gigabit Ethernet...  Not connected

NIC ID 1 is currently assigned to the management interface.

If you want to be sure of the ID of each NIC, disconnect all network cables
and reconnect them one at a time, pressing the R key after you connect each one.

Enter the NIC ID number or press the R key to refresh the list [R]:
```

The screen displays the network interface cards (NICs) that are available to your system and whether or not the devices are connected. The line below the list indicates which device is currently assigned to the user interface. To select another device, type the NIC ID number from the list

of NIC IDs and press Enter. To refresh the list of NICs, type R and press Enter.

2.8.1.6 Configuring a network device

After you select which network device you wish to use for the user interface, you need to configure the device. To configure the device, type 6 and press Enter. The following screen is displayed.

```
LANGuardian Management Utility
------------------------------

Configure the network device

You have chosen to assign this device to the LANGuardian management interface:

Description                                     Status
-------------------------------------------------------------------------------
Intel PRO/1000 Network Connection               Connected

Please enter the following network settings:

LANGuardian computer IP address [192.168.127.200]: 192.168.127.200
LANGuardian computer network mask [255.255.255.0]: 255.255.255.0
Default gateway IP address [192.168.127.1]: 192.168.127.1
DNS server IP address [16.1.20.232]: 16.1.20.232

Press ENTER to return to the main menu:
```

Enter the following:

- The IP address of the LANGuardian system.
- The network mask of the LANGuardian system.
- The default gateway IP address.
- The IP address of the DNS server.

This completes the configuration of the network device.

2.8.1.7 Switching to probe mode

To change the operating mode from central manager mode to probe mode, type 7 and press Enter. The following screen is displayed.

```
LANGuardian Management Utility
------------------------------

Set operating mode

In central manager mode, LANGuardian captures network traffic data through
its own network interfaces or from probes elsewhere on the network. In
probe mode, LANGuardian captures network traffic and sends it to a central
manager.

This LANGuardian system is currently operating in central manager mode. If
you convert it to a probe, it will no longer act as a central manager.
All traffic data previously recorded will be lost.

Do you want to convert to probe mode [NO]?
```

If your system is currently acting as a central manager and you want to change it to a probe, all of the traffic data that was previously recorded will

be lost. To confirm that you want to convert the system to a probe, type `Y` and press Enter. To abort the conversion to probe mode, type `N` and press Enter.

If you enter `Y`, the following screen is displayed:

```
LANGuardian Management Utility
------------------------------

Set operating mode

To convert this LANGuardian system to probe mode, please enter the IP
address and Administrator password for the web browser user interface
on the central manager to which you want to send the network traffic
data.

Central manager IP address: 16.20.154.200
Central manager Administrator password: xxxxx
```

Enter the following:

- The IP address of the LANGuardian Central Manager to which you want to connect.
- The password for the Administrator account on the LANGuardian central manager.

To complete the conversion to probe mode, LANGuardian automatically restarts the system as a probe. When the system restarts, the status of the probe is indicated in the text below the Management Utility menu. For example:

```
LANGuardian Management Utility
------------------------------

System commands                 System configuration

1. View status                  5. Select network device
2. Restart LANGuardian          6. Configure network device
3. Shutdown LANGuardian         7. Set operating mode
4. Ping command                 8. Bind to a central manager

This LANGuardian system is set to operate in probe mode. It keeps the software
version up to date with the LANGuardian central manager. If the central manager
software version changes, this probe system will automatically download the
latest version, install it, and restart.

Enter a command [1-8]:
```

The text displayed can indicate three scenarios as follows:

- The text in the above example is displayed when the probe successfully authenticates with the central manager and is ready for use. No further action is required.
- If the probe can connect to the central manager but it fails to authenticate with the central manager, the following text is displayed:

```
WARNING! This LANGuardian system is set to operate in probe mode but it
failed to authenticate itself with its central manager. To re-enter your
central manager settings, press 8.
```

In this situation, you should use option 8 to reenter the central manager IP address and password.

- If the probe cannot connect to the central manager at all, the following text is displayed:

```
WARNING! This LANGuardian system is set to operate in probe mode but it is
unable to contact the central manager it is associated with. You can use the
ping command to verify connectivity with the central manager IP address
(16.20.154.200). To use the ping command, press 4. To bind to a different
central manager, press 8.
```

In this situation, you can use the option 4 to ping the central manager to see if it is responding. Alternatively, use option 8 to connect to a different central manager IP address.

2.8.1.8 Resetting the user interface password

To reset the Administrator password that you use to access the user interface, type 8 and press Enter. The following screen is displayed.

```
LANGuardian Management Utility
------------------------------

Reset Administrator password for web user interface

You are about to change the Administrator password for the web user interface
of the LANGuardian system located at:

https://192.168.127.200/

Type the new password: **********
Confirm the new password: **********

The Administrator password has been changed.

Press ENTER to return to the main menu:
```

Enter a new password, then enter the new password again to confirm the password. The password is changed and you can log into the user interface using the new password.

2.8.2 Managing a probe

When you start the Management Utility on a LANGuardian system that is acting as a probe, the following screen is displayed:

```
LANGuardian Management Utility
------------------------------

Copyright 2012 NetFort Technologies Limited. All rights reserved.

Welcome to the management utility for LANGuardian 10.0.

Use this utility to modify LANGuardian network settings, reset the
Administrator password, and change the operating mode.

+-------------------------------------------------------------------------+
| PLEASE NOTE:                                                            |
|                                                                         |
| Some of the commands available in the management utility can make your   |
| LANGuardian system inoperable. Please be very careful when using them.  |
|                                                                         |
| For day-to-day operation and configuration of your LANGuardian system,  |
| you can access LANGuardian through the web user interface at this URL:  |
|                                                                         |
| https://192.168.127.200/                                                |
+-------------------------------------------------------------------------+

Press ENTER to access the management utility menu:
```

Press Enter to view the Management Utility menu.

```
LANGuardian Management Utility
------------------------------

System commands                 System configuration

1. View status                  5. Select network device
2. Restart LANGuardian          6. Configure network device
3. Shutdown LANGuardian         7. Set operating mode
4. Ping command                 8. Bind to a central manager


This LANGuardian system is set to operate in probe mode. It keeps the software
version up to date with the LANGuardian central manager. If the central manager
software version changes, this probe system will automatically download the
latest version, install it, and restart.

Enter a command [1-8] (or type EXIT to exit):
```

The Management Utility menu is divided into system commands and system configuration. To select a menu option, type a number and press Enter.

2.8.2.1 Viewing the status of a LANGuardian probe

To view the status of a LANGuardian probe, type `1` and press Enter. The status of the system is displayed.

```
LANGuardian Management Utility
------------------------------

Status
------
Network interface:              em0 (Intel PRO/1000 Network Connection)
Management IP address:          192.168.127.200
Netmask:                        255.255.255.0
Default gateway:                192.168.127.1
DNS server:                     16.20.1.232

Operating mode:                 Probe
LANGuardian version:            8.7.0.3
Central manager IP address:     16.20.154.200
Probe authentication status:    Authenticated
Web user interface URL:         https://16.20.154.200
Uptime:                         12d 14h 25m

Press ENTER to return to the main menu:
```

The `Probe authentication status` line indicates the connection status of the probe with the central manager, as follows:

- `Authenticated` means that the probe has been authenticated against the central manager and is talking to the central manager.
- `Not authenticated` means that the probe can connect to the central manager but it cannot authenticate itself. This could indicate that you entered an incorrect password for the central manager. Use option 8 to reenter the IP address and password for the central manager.
- `Unknown – unable to contact the central manager` means that the probe is not able to connect to the central manager. Use option 4 to ping the central manager to see if it is responding. You can also use option 8 to reenter the IP address and password for the central manager or to bind to a different central manager.

2.8.2.2 Restarting a LANGuardian probe

To restart a LANGuardian probe, type `2` and press Enter. You are prompted to type `Y` or `N` to confirm whether or not you want to restart the system. The default is `N`.

2.8.2.3 Shutting down a LANGuardian probe

To shut down a LANGuardian probe, type `3` and press Enter. You are prompted to type `Y` or `N` to confirm whether or not you want to shut down the system. The default is `N`.

2.8.2.4 Running the ping command

This task is identical for both a central manager and a probe. See Section 2.8.1.4 Running the ping command for more information.

2.8.2.5 Selecting a network device for the user interface

This task is identical for both a central manager and a probe. See Section 2.8.1.5 Selecting a network device for the user interface for more information.

2.8.2.6 Configuring a network device

This task is identical for both a central manager and a probe. See Section 2.8.1.6 Configuring a network device for more information.

2.8.2.7 Switching to central manager mode

To change the operating mode from probe mode to central manager mode, type 7 and press Enter. The following screen is displayed.

```
LANGuardian Management Utility
------------------------------

Set operating mode

In central manager mode, LANGuardian captures network traffic data through
its own network interfaces or from probes elsewhere on the network. In
probe mode, LANGuardian captures network traffic and sends it to a central
manager.

This LANGuardian system is currently operating in probe mode. If you convert
it to central manager mode, it will no longer act as a probe and all traffic
data will be stored locally.

Do you want to convert to central manager mode [NO]?
```

To confirm that you want to convert the system to a central manager, type Y and press Enter. The following screen is displayed:

```
After restarting, this LANGuardian system will operate in central manager mode.

Press ENTER to restart the LANGuardian system:
```

Press Enter again to restart the system and complete the conversion to Central Manager mode.

To abort the conversion to central manager mode, type N and press Enter. If you enter N, the conversion process is cancelled and the following is displayed:

```
This system will continue to operate in central manager mode. No changes have
been made.

Press ENTER to return to the main menu:
```

2.8.2.8 Binding to a different central manager IP address

To bind the current probe to a different central manager or to re-authenticate the probe with the current central manager, type 8 and press Enter. The following screen is displayed.

```
LANGuardian Management Utility
------------------------------

Bind to a central manager

This LANGuardian system is operating in probe mode and is bound to the
central manager with the following IP address:

16.20.154.200.

To bind the probe to a different central manager, or to re-authenticate
the probe with the current central manager, please enter the IP address
and Administrator password for the web browser user interface on the
central manager to which you want to send the network traffic data.

Central manager IP address [16.20.154.200]: 16.20.254.100
Central manager Administrator password: xxxxx

Are you sure you want to bind to this central manager [NO]?
```

Enter the following:

- The IP address of the LANGuardian Central Manager to which you want to connect.
- The password for the Administrator account on the LANGuardian Central Manager.

Type `Y` to confirm that you want to bind to the Central Manager. Type `N` to cancel the process and revert to the existing central manager settings.

Chapter 3

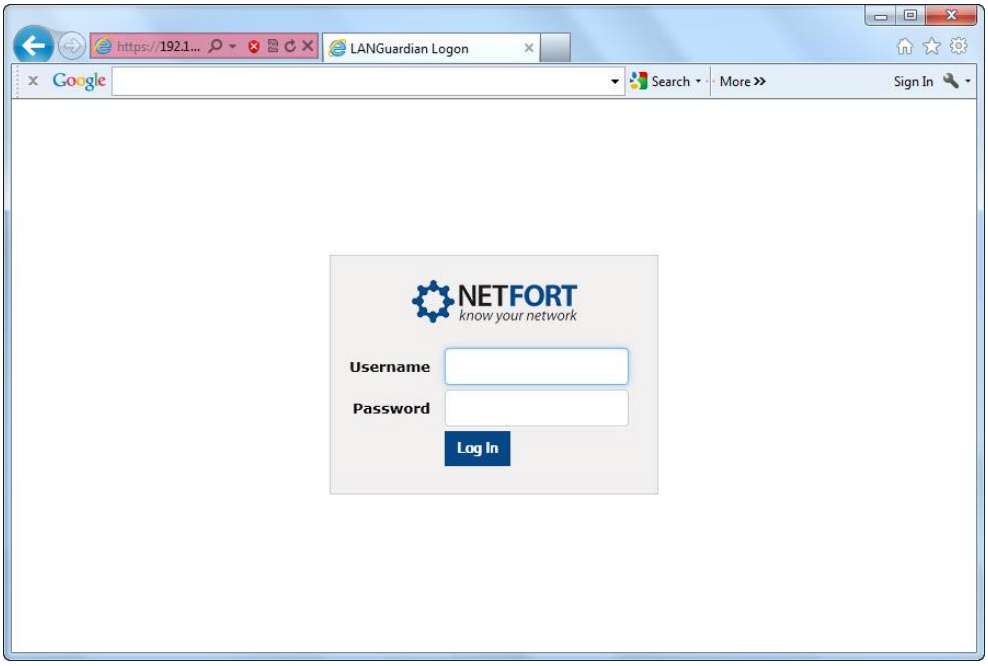
Chapter 3 - Using LANGuardian

LANGuardian has a browser-based user interface that presents dashboards, reports, and search functionality to instantly provide you with detailed information about activity on your network. You can customize the dashboards and create your own reports to create a network monitoring solution that is tailored to your specific needs.

3.1 Logging on

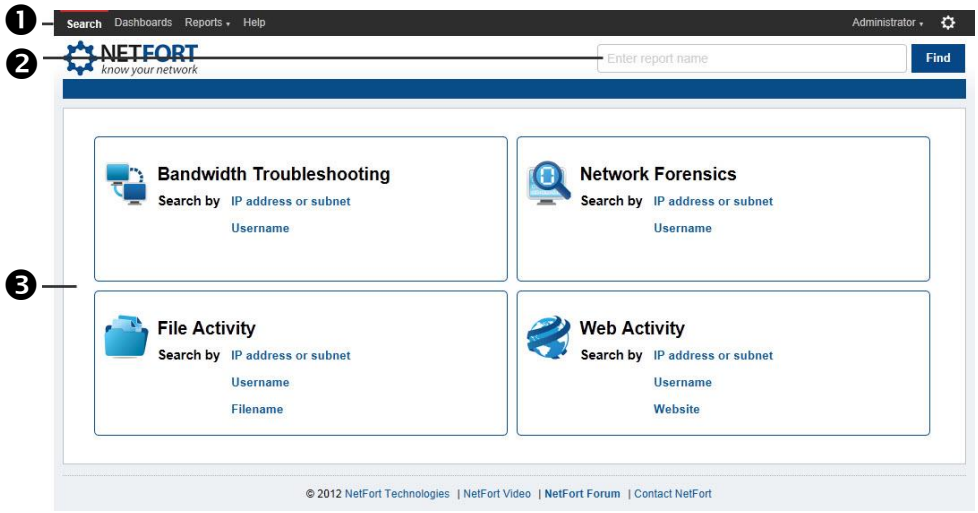
When you install LANGuardian, you specify an IP address to use for the management interface. To log on to LANGuardian, enter this address in your web browser. For example, if the IP address is 192.168.200.2, the address you enter in your browser is:

```
https://192.168.200.2/
```



When you first log on to LANGuardian, you must log on with the username **Administrator**. The password is the GUI password that you set during the Configuration Wizard.

After you log on, the LANGuardian graphical user interface (GUI) is displayed. By default, LANGuardian displays the **Search** page when you log on. If you prefer, you can modify LANGuardian to display the **Dashboards** page by default. See Section 3.8.5 Modifying the current user account for more information.



The main components of the user interface are as follows:

1. The LANGuardian menu bar, which you use to navigate LANGuardian and access all of the features.
2. The Find box, which you can use to quickly access LANGuardian reports.
3. The main display area.

3.1.1 LANGuardian menu bar

The LANGuardian menu bar allows you to navigate to all of the product features.

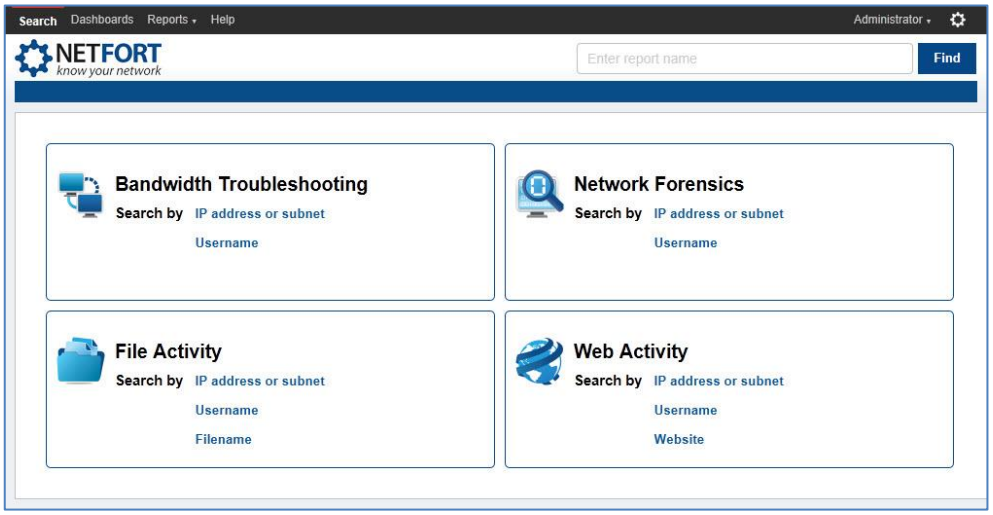
Menu	Description
Search	To display the Search page. This page contains four panels which you can use to investigate particular network activities.
Dashboards	To go to the Dashboards page and view live network information. You can customize your dashboard page to view the information that is most important to you.
Reports	To access detailed LANGuardian reports. If a report is not displayed on the dashboard you can access it using this menu.
Help	To display online help for the product.
Administrator	To modify your LANGuardian account settings or to log out.
⚙	To configure your LANGuardian installation.

All LANGuardian features are described in more detail in the following sections of this guide.

3.2 Search page

The LANGuardian Search page contains four panels that allow you to quickly access information about a particular area of the network or about a particular incident that may have occurred on the network. The four panels represent different aspects of the network as follows:

- Bandwidth troubleshooting
- Network forensics
- File activity
- Web activity



3.2.1 Performing a search

To perform a search:

1. Go to the appropriate search panel.
2. Click on the **Search by** label that you require. For example, to search for file activity by IP address, click on **IP address or subnet** in the **File Activity** panel. A search field is displayed in which you type your search criteria, as follows:
    a. To search by IP address or subnet, type an IP address or subnet. For example, 192.168.1.227 or 192.168.1.0/24.
    b. To search by username, type the full name of the user (for example, Andrea Cron) or the username (for example, Andrea). LANGuardian has an autocomplete feature that shows a drop-

down list of matching names as you type. This ensures that you can only search for names that exist in the database.

c. To search by filename, type a filename, partial filename, directory name, partial directory name, or file type. LANGuardian searches for all filenames that match the search criteria.

d. To search by website, type a full or partial domain name. For example, you can enter "youtube.com" to display data for youtube.com or enter "you" to display data for any domain name that contains the word "you".

The following table contains some examples of what you can enter in the search fields:

Examples of search entries	Displays results for …
IP Address/Subnet search	
192.168.127.1	A single IP address 192.168.127.1
192.168.127.0/24	All IP addresses in the range 192.168.127.1 to 192.168.127.254
192.168.127.1,192.168.127.2	The IP addresses 192.168.127.1 and 192.168.127.2
192.168.127.0/24,192.168.128.0/24	All IP addresses in the range 192.168.127.1 to 192.168.127.254 and 192.168.128.1 to 192.168.128.254
192.168.0.0/16,!192.168.127.0/24	All IP addresses in the range 192.168.0.1 to 192.168.255.254 but excludes IP addresses in the range 192.168.127.1 to 192.168.127.254
Username search	
Andrea	The user "Andrea"
Andrea|Sean	The users "Andrea" and "Sean"
Website search	
youtube.com	Web activity associated with youtube.com
You	Web activity associated with any website that contains "you" in the URL
youtube|facebook|bebo	Web activity associated with all websites that contain "youtube", "facebook", or "bebo" in the URLs
Filename search	
sales	Any file or directory name that contains the string "sales"
sales|profit|loss	All files or directories that contain the strings "sales", "profit", or "loss"

\\finance\\	Directories called "finance"
.mdb$	All files with the file extension .mdb
.docx$\|.xlsx$|.pptx$	All Microsoft Word, Excel, or Powerpoint files

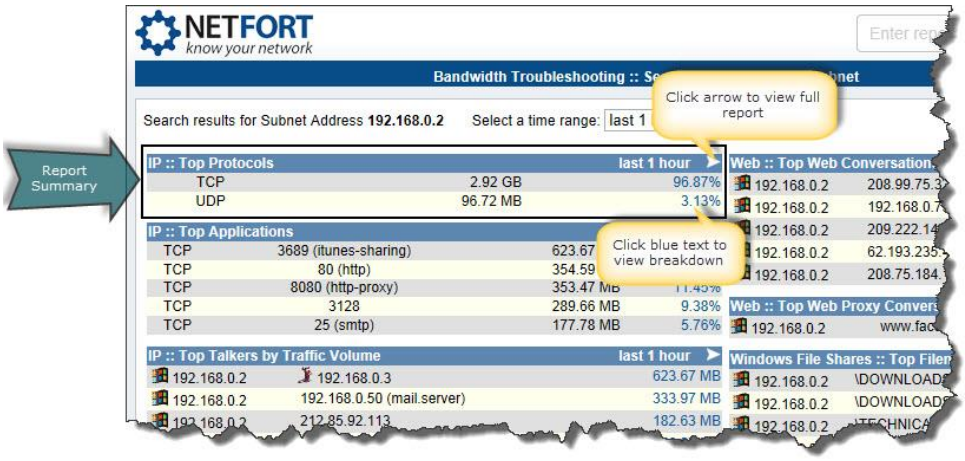
3. Click **Go** to perform the search. Depending on the type of search you are performing, the following occurs:

   - If you are using the **Bandwidth Troubleshooting** or **Network Forensics** panels, LANGuardian displays a report summary page.
   - If you are using the **File Activity** or **Web Activity** panels, LANGuardian displays a report.

   In either case, the results displayed are for the last hour. To increase the time range for the data, you can select **Last 4 hours** or **Last 24 hours** from the **Select a time range** or **Time** drop-down list.

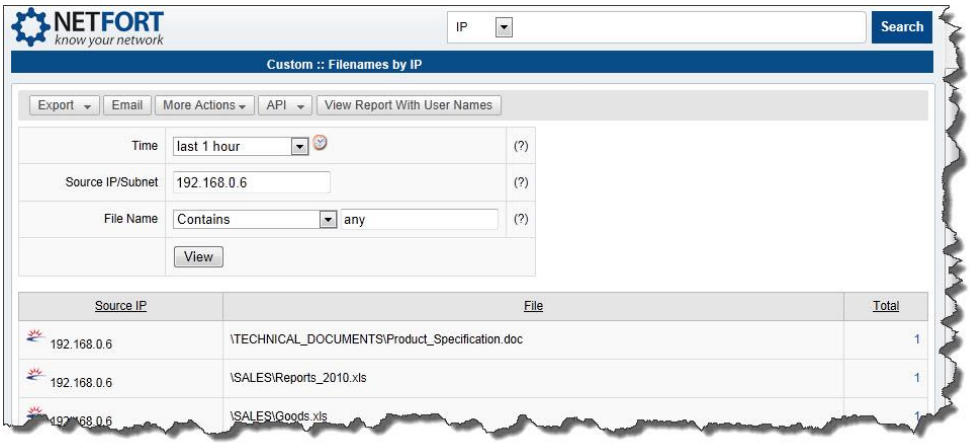
   A report summary page contains multiple report summaries. To view more details, you can click on the arrow in the report summary title to view the full report, or you can click on any of the hyperlinked text to view another report with a breakdown of the results.

Figure 1 Sample Report Summary Page



A report contains the information that is relevant to the current search. You can modify the search by editing the fields at the top of the report and click **View** to regenerate the report.

Figure 2 Sample Report



3.2.2 Bandwidth troubleshooting

The Bandwidth Troubleshooting panel allows you to troubleshoot any issues you are experiencing with bandwidth by reporting on the network activity that is affecting bandwidth. For example, "My network is very slow since lunchtime, what is going on?".

To troubleshoot bandwidth issues, you can enter an IP address, subnet address, or username.

3.2.2.1 Troubleshoot bandwidth issues by IP address or subnet

For information about how to use the search page, see Section 3.2.1 Performing a search.

The **Bandwidth Troubleshooting :: Search by IP address or subnet** report summary page displays the following report summaries:

Report Summary[1]	Description
IP :: Top Protocols	The top Ethernet protocols, the amount of data transferred using each protocol, and the percentage of the total data associated with each protocol.
IP :: Top Applications	The top application protocols, the associated Ethernet protocol, the amount of data transferred per application, and the percentage of the total data associated with each application.
IP :: Top Talkers by Traffic Volume	The top IP addresses that the specified IP address is talking to and the amount of data (in MB/GB) transferred between the IP addresses.
IP:: Top Talkers by Packets Sent and	The top IP addresses that the specified IP

[1] Report summaries display a maximum of five top results from each report.

Received	address is talking to and the number of packets transferred between the IP addresses.
Web :: Top Web Conversations by Traffic Volume	The top web servers that the specified IP address is talking to and the amount of data transferred between the IP addresses.
Web :: Top Web Proxy Conversations by Traffic Volume	The top web servers that the IP address in question is talking to through a proxy server, the IP address of the proxy server, and the amount of data transferred between the IP addresses.
Windows File Shares :: Top Filenames by Number of Actions	The top filenames accessed by the specified IP address and the number of times each file was accessed.
Web :: Top Websites by Number of Hits	The top websites accessed by the specified IP address, the number of hits for each website, and the percentage of total website hits.

3.2.2.2 Troubleshoot bandwidth issues by user

For information about how to use the search page, see Section 3.2.1 Performing a search.

The **Bandwidth Troubleshooting :: Search by user** report summary page displays the following report summaries:

Report Summary	Description
IP :: Traffic Distribution :: By User	The top application protocols, the associated Ethernet protocol, and the data usage per application.
IP :: User :: Top Conversations by Traffic Volume	The top IP addresses that the user is talking to, the source IP address of the user, and the amount of data transferred between the IP addresses.
Identity :: Directory Logins :: by IP	The IP addresses of the systems that the user is logging in to, the total number of logins to each system, the full name of the user, the login name of the user, and the department to which the user belongs.
Web :: Top Websites :: by User	The top websites that the user is accessing, the number of accesses to each website, the time of the first access and the time of the last access.
Web :: Proxy :: Sessions :: by User	The top web servers that the user is accessing through a proxy server, the source IP address of the user, the IP address of the proxy server, the proxy port number, the amount of data sent, the amount of data received, and the total data amount.

Windows File Shares :: Search by Filename :: by User	The file servers accessed by the user, the IP address of the file server, the file name or directory accessed on the file server, and the number of times each file or directory is accessed.

3.2.3 Network forensics

The Network Forensics panel allows you to view detailed information about your network activity.

To view network forensic information, you can enter an IP address, subnet address, or username.

3.2.3.1 View network forensic information by IP address

For information about how to use the search page, see Section 3.2.1 Performing a search.

The **Network Forensics :: Search by IP address or subnet** report summary page displays the following report summaries:

Report Summary	Description
IP :: Top Applications	The top application protocols, the associated Ethernet protocol, the amount of data used by each application protocol, and the percentage of data used.
Security :: by Signature	The security events that occurred on the network, the priority of each event, and the numbers of instances of each event.
Network Inventory :: Network Services	The services being offered on the network, the sensor that detected the service, and the number of instances of each service.
IP Activity :: Top Packet Generators	The IP addresses that are generating the most packets, the sensor that detected the IP address, the amount of data generated, and number of packets generated.
Web Browsers :: Web Clients	The top web client applications running on the network, the sensor that detected the client, the number of instances of each client, and the percentage of clients in use.
Network Inventory :: Operating Systems	The top operating system running on the network, the sensors that detected the operating system, and the number of instances of each operating system.
Web :: Top Websites by Number of Hits	The top websites accessed from the specified IP address, the number of accesses to each website, and the percentage of total website accesses.
Web :: Proxy Sessions	The top websites that are accessed through a proxy server, the sensor that detected the

	proxy session, the IP address of the proxy server, the proxy port number, the amount of data sent, the amount of data received, and the total data amount.
E-mail :: by Subject	The top email subjects sent from the specified IP address, the number of times each email was sent, and the percentage of the total emails sent.
Windows File Shares :: Filenames (by Clients)	The file servers accessed, the sensor that detected the file server, the IP address of the file server, the file name or directory accessed on the file server, the action taken on the file, the number of times the file action occurred, and the percentage of total file activity.
SQL Server :: Top Statement	The top SQL statements issued by the specified IP address to an SQL server, the statement type, and the number of instances of each statement.
BitTorrent :: events (torrent downloads)	The BitTorrent announce requests detected, the sensor that detected the requests, the source IP address, the time of the request, the website name of the tracker, the Info-hash of the BitTorrent file, and the name of the BitTorrent file, if found. An announce request is generated when a BitTorrent peer initiates a data transfer. The Info-hash uniquely identifies the torrent being exchanged.

3.2.3.2 View network forensic information by user

For information about how to use the search page, see Section 3.2.1 Performing a search.

The **Network Forensics :: Search by username** report summary page displays the following report summaries:

Report Summary	Description
IP :: Traffic Distribution :: by User	The full name of the user, the username, the transfer protocol, the top traffic services, and the data usage per service.
Security :: User Events	The full name of the user, the username, the department, the top user events, the priority, and the number of occurrences of each event.
Identity :: Directory Logins :: by IP	The full name of the user, the username, the department, the IP addresses of the systems that the user is logging in to, and the total number of logins to each system.
E-mail :: by User	The top emails sent by the user, the email subject, the number of times each email was

	sent, and the percentage of the total emails sent.
Web :: Top Websites :: by User	The full name of the user, the username, the top websites that the user is accessing, the number of accesses to each website, the time of the first access and the time of the last access.
Web :: Proxy :: Sessions :: by User	The sensor number and description, the username, the source IP address of the user, the IP address of the proxy server, the proxy port number, the website that the user is accessing through the proxy server, the amount of data sent, the amount of data received, and the total data transfer.
Windows File Shares :: Search by Filename :: by User	The sensor number and description, full name of the user, the username, the file servers accessed by the user, the IP address of the file server, the file name or directory accessed on the file server, and the number of times each file or directory is accessed.
SQL Server :: events (ms sql) :: by User	The sensor number and description, the full name of the user, the username, the source IP address, the IP addresses of the top SQL servers accessed, the time of the access, the username used to access the SQL server, the application used to access the SQL server, the database type, the statement type, and the statement.

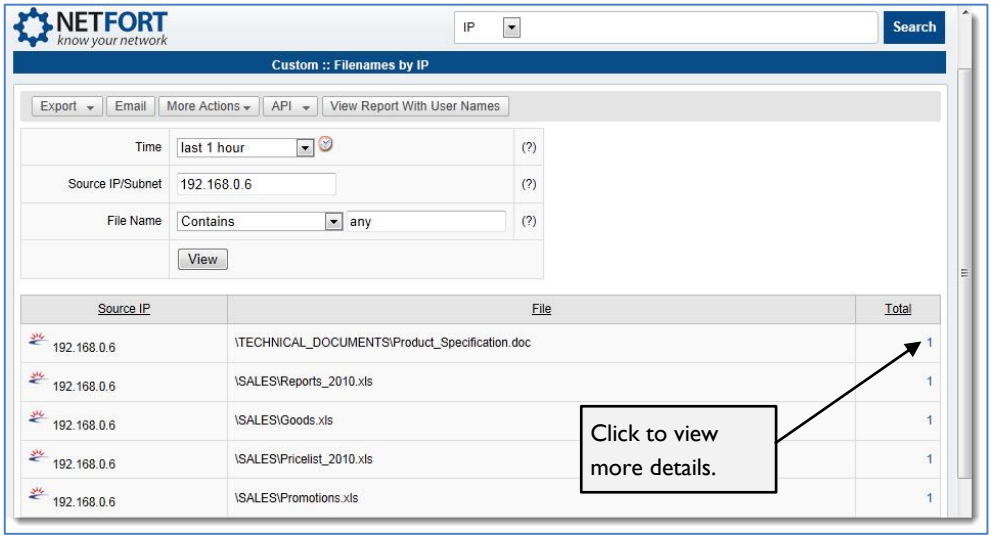
3.2.4 File activity

The File Activity panel allows you to view recent file activity for a specified IP address, user, or filename. For example, "I cannot find the presentation that I was working on for tomorrow's meeting. Can I search for the filename to see if someone moved it to a different location?" or "A number of report files have gone missing since last week? Can I see all of the file activity on the subnet since last week to see who accessed the files?".

3.2.4.1 View file activity by IP address or subnet

For information about how to use the search page, see Section 3.2.1 Performing a search.

When you search for file activity by IP address or subnet, the following report is displayed:

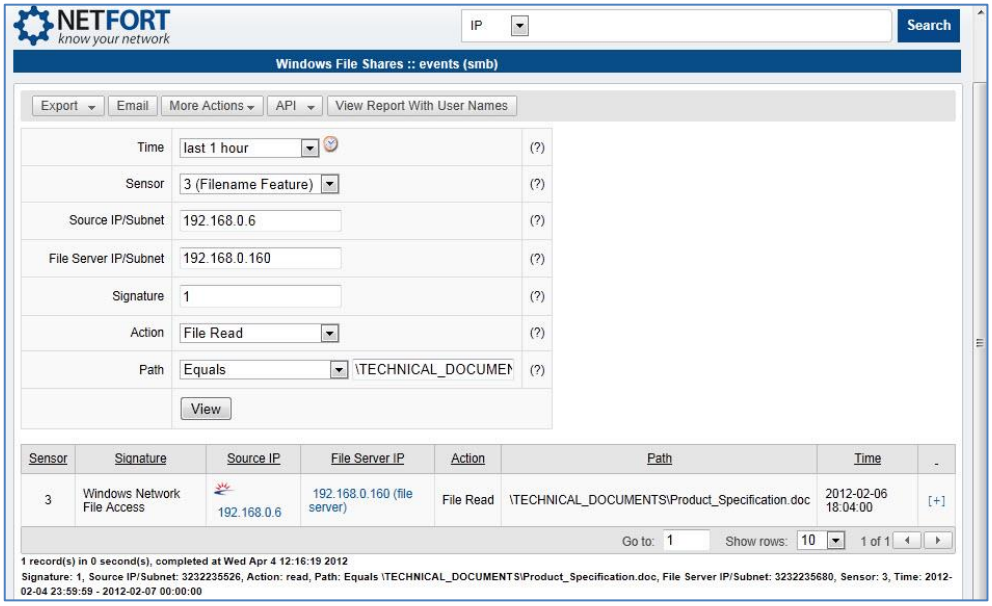


The report lists the files that were accessed from the specified IP address, and the number of times the file was accessed. To modify the search results, you can:

- Select **Last 4 hours** or **Last 24 hours** from the **Time** drop-down list to increase the duration to show more activity.
- Specify a different IP address in the **Source IP/Subnet** field. For more information about using this filter field, see Section 3.4.11.1 Using the IP/Subnet filter field.
- Select an option from the **File Name** drop-down list to focus the results on specific files. For more information about using this drop-down list, see Section 3.4.11.2 Filtering reports using common regular expressions.

Click **View** to modify the results.

To view details about a file access, click on the number in the **Total** column. A detailed report on the file activity for the specified file is displayed.



To modify the detailed report, you can use the fields at the top of the results page, as follows:

- Select **Last 4 hours** or **Last 24 hours** from the **Time** drop-down list to increase the duration to show more activity.
- Select a different sensor from the **Sensor** drop-down list.
- Specify a different IP address in the **Source IP/Subnet** field. For more information about using this filter field, see Section 3.4.11.1 Using the IP/Subnet filter field.
- Specify a file server IP address.
- Specify a signature.
- Select an option from the **Action** drop-down list to focus the results on specific file actions or events.
- Select an option from the **Path** drop-down list and enter text in the input field to filter the search results to include or exclude certain paths to the file name.

Click **View** to modify the results.

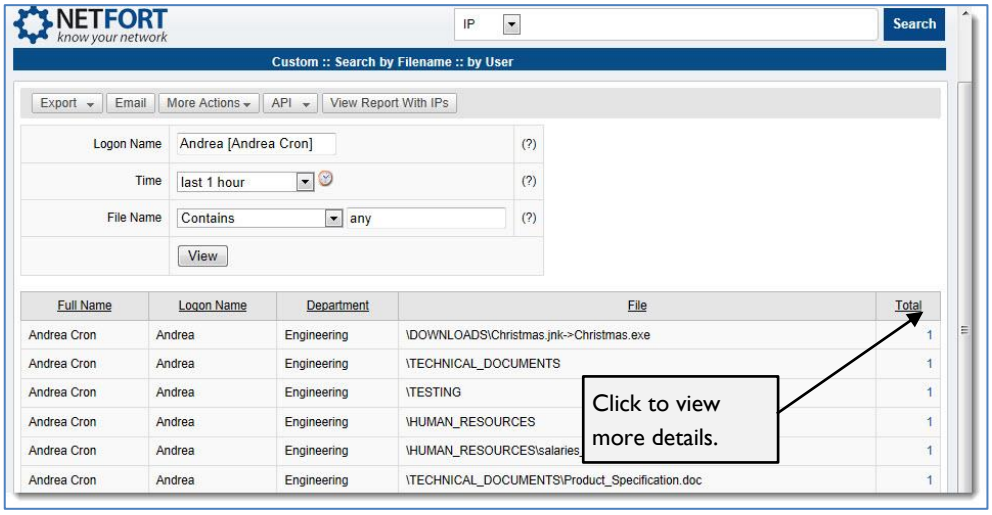
The detailed report page displays the following information:

Report Column	Description
Sensor	The sensor that detected the file activity.
Signature	The type of file activity event that took place.
Source IP	The IP address from which the file was accessed.

File Server IP	The IP address of the file server.
Action	The action taken on the file.
Path	The directory path and name of the file on the file server.
Time	The time when the action was taken on the file.

3.2.4.2 View file activity by user

When you search for file activity by user, the following report is displayed:

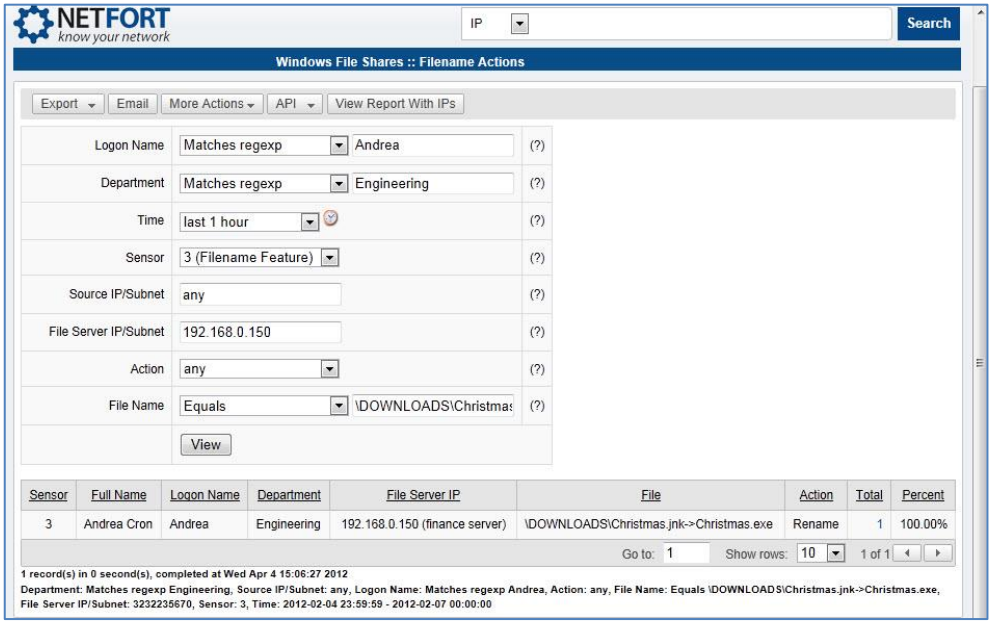


The results page lists all of the files that the specified user accessed in the last hour, and the number of times each file was accessed. To modify the search results, you can:

- Enter a different username in the **Logon Name** field.
- Select **Last 4 hours** or **Last 24 hours** from the **Time** drop-down list to increase the duration to show more activity.
- Select an option from the **File Name** drop-down list to focus the results on specific files. For more information about using this drop-down list, see Section 3.4.11.2 Filtering reports using common regular expressions.

Click **View** to modify the results.

To view more details about a file, click on the number in the **Total** column. A detailed report on the file activity for the specified file is displayed.



To modify the detailed search results, you can use the fields at the top of the results page, as follows:

- Select an option from the **Logon Name** drop-down list to focus the results on specific users or filter out users. For more information about using this drop-down list, see Section 3.4.11.2 Filtering reports using common regular expressions.
- Select an option from the **Department** drop-down list to focus the results on users from specific departments or filter out departments.
- Select **Last 4 hours** or **Last 24 hours** from the **Time** drop-down list to increase the duration to show more activity.
- Select a different sensor from the **Sensor** drop-down list.
- Specify a source IP address in the **Source IP/Subnet** field. By default, the IP address is any address that the user uses. For more information about using this filter field, see Section 3.4.11.1 Using the IP/Subnet filter field.
- Specify a file server IP address in the **File Server IP/Subnet** field.
- Select an option from the **Action** drop-down list to focus the results on specific file actions or events.
- Select an option from the **File Name** drop-down list and enter text in the input field to filter the search results to include or exclude certain file names. For more information about using this drop-down list, see Section 3.4.11.2 Filtering reports using common regular expressions.

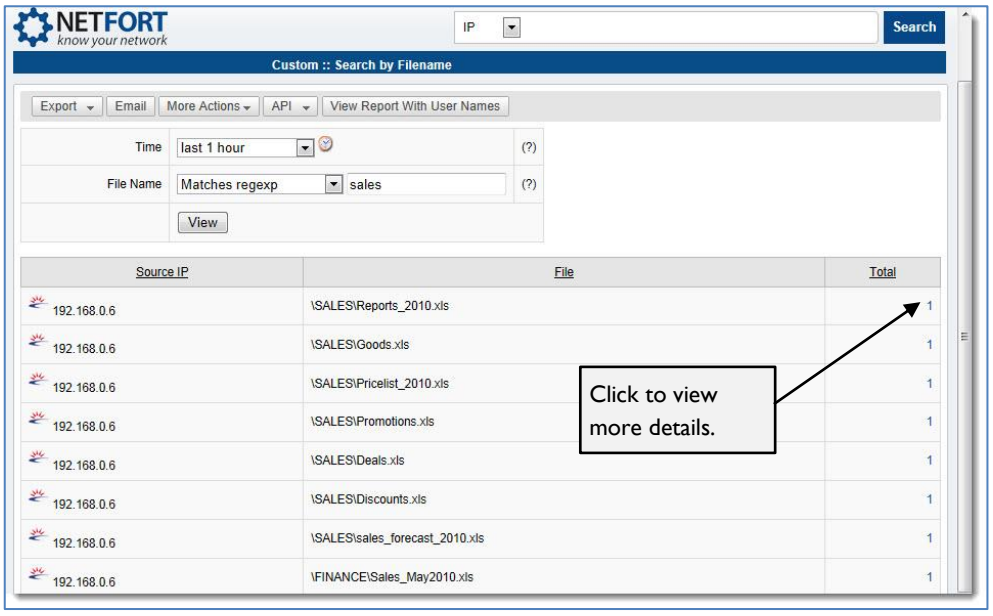
Click **View** to modify the results.

The detailed report displays the following information:

Report Column	Description
Sensor	The sensor that detected the file activity.
Full Name	The full name of the user.
Logon Name	The logon name of the user.
Department	The department to which the user belongs.
File Server IP	The IP address of the file server.
File	The directory path and name of the file on the file server.
Action	The action taken on the file.
Total	The number of times the file was accessed.
Percent	The percentage of file accesses.

3.2.4.3 View file activity by filename

You can view file activity for a specified full or partial filename or directory name. When you search for file activity by filename, the following report is displayed:



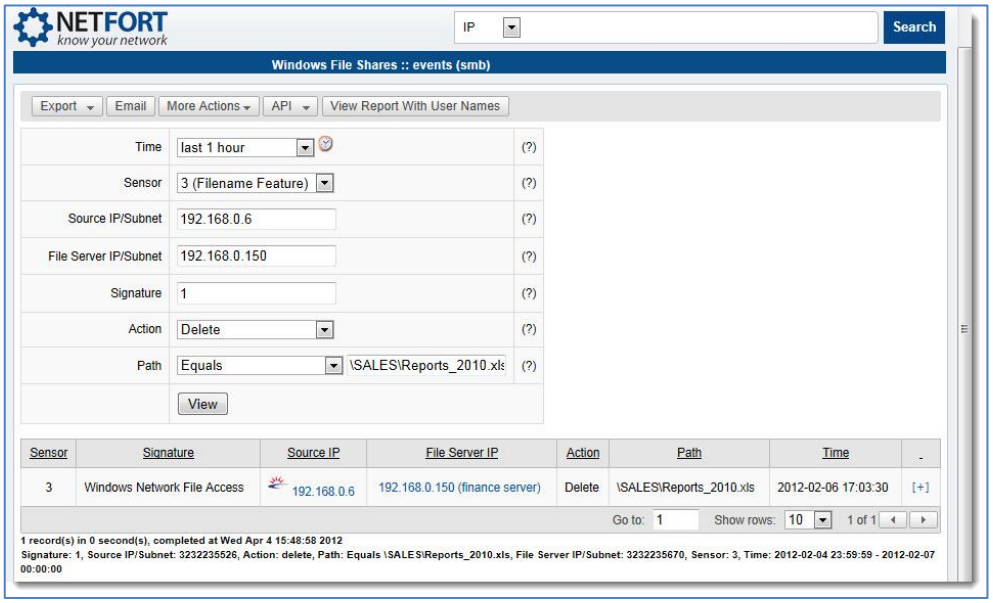
The report lists all file accesses that match the file name that you entered. To modify the search results, you can:

- Select **Last 4 hours** or **Last 24 hours** from the **Time** drop-down list to increase the duration to show more activity.
- Select an option from the **File Name** drop-down list to focus the results on specific files. For more information about using this drop-

down list, see Section 3.4.11.2 Filtering reports using common regular expressions.

Click **View** to modify the results.

To view more details about a file access, click on the number in the **Total** column. A detailed report on the file activity for the specified file is displayed.



To modify the detailed search results, you can use the fields at the top of the results page, as follows:

- Select **Last 4 hours** or **Last 24 hours** from the **Time** drop-down list to increase the duration to show more activity.
- Select a different sensor from the **Sensor** drop-down list.
- Specify a source IP address in the **Source IP/Subnet** field. For more information about using this filter field, see Section 3.4.11.1 Using the IP/Subnet filter field.
- Specify a file server IP address in the **File Server IP/Subnet** field.
- Specify a signature.
- Select an option from the **Action** drop-down list to focus the results on specific file actions or events.
- Select an option from the **Path** drop-down list and enter text in the input field to filter the search results to include or exclude certain paths to the file name.

Click **View** to modify the results.

The detailed report displays the following information:

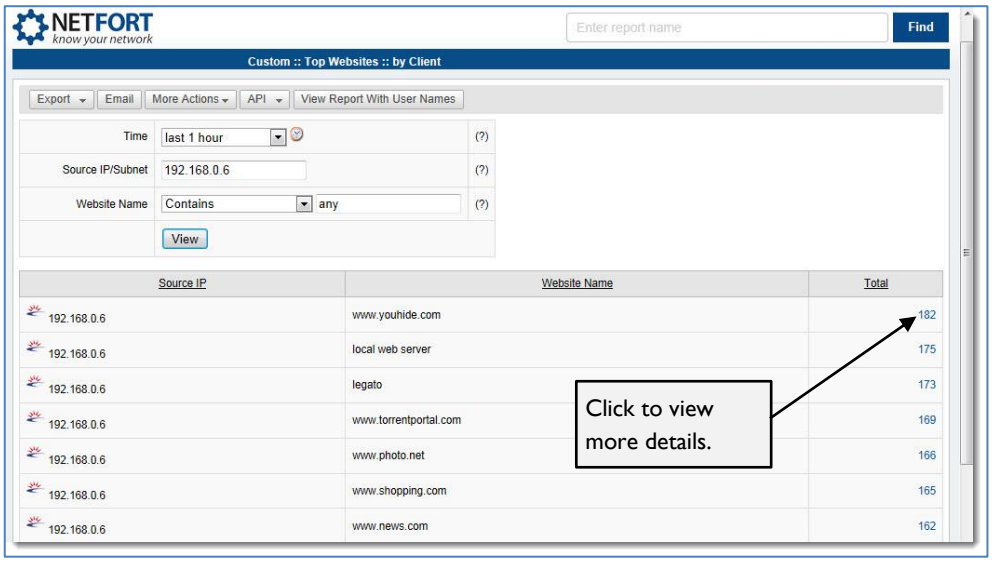
Report Column	Description
Sensor	The sensor that detected the file activity.
Signature	The type of file activity event that took place.
Source IP	The IP address from which the file was accessed.
File Server IP	The IP address of the file server.
Action	The action taken on the file.
Path	The directory path and name of the file on the file server.
Time	The time when the action was taken on the file.

3.2.5 Web activity

The **Web Activity** panel allows you to view recent web activity for a specified IP address, user, or website. For example, "I suspect that employee X is accessing online poker websites during working hours, which is against company policy. Can I see a report on recent web activity for this user?".

3.2.5.1 View web activity by IP address or subnet

When you search for web activity by IP address, the following report is displayed:



The report lists all websites accessed from the specified IP address and the number of times each site was accessed. To modify the search results, you can:

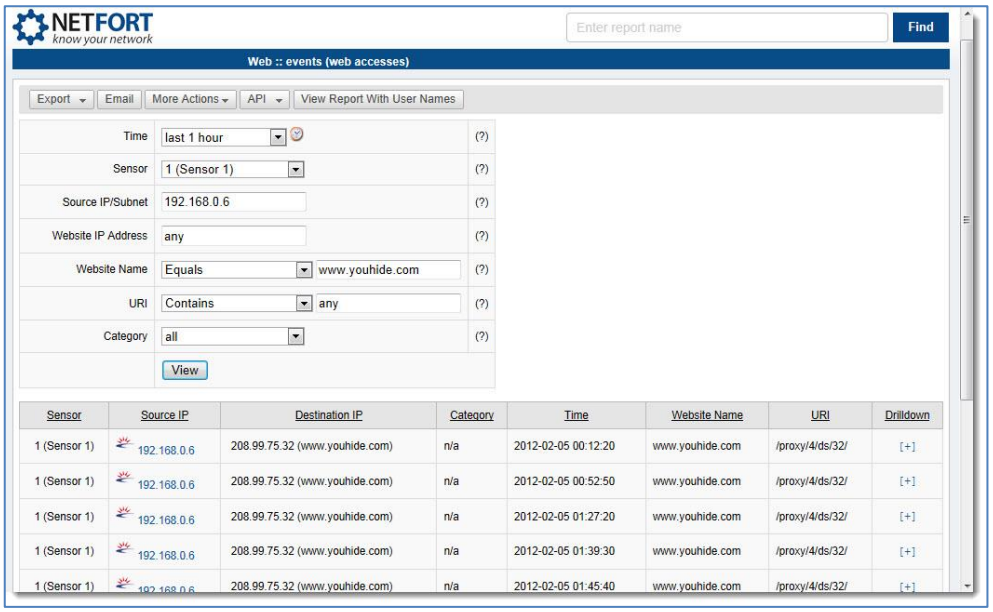
- Select **Last 4 hours** or **Last 24 hours** from the **Time** drop-down list to increase the duration to show more activity.

- Specify a different IP address in the **Source IP/Subnet** field. For more information about using this filter field, see Section 3.4.11.1 Using the IP/Subnet filter field.

- Select an option from the **Website Name** drop-down list to focus the results on specific websites or filter out specific websites. For more information about using this drop-down list, see Section 3.4.11.2 Filtering reports using common regular expressions.

Click **View** to modify the results.

The **Total** column displays the total number of visits to each website. To view more detailed information about the web activity for each website, click on the number in the **Total** column. A detailed report on the web activity for the specified file is displayed.



To modify the detailed report, you can use the fields at the top of the results page, as follows:

- Select **Last 4 hours** or **Last 24 hours** from the **Time** drop-down list to increase the duration to show more activity.

- Select a different sensor from the **Sensor** drop-down list.

- Specify a different IP address in the **Source IP/Subnet** field. For more information about using this filter field, see Section 3.4.11.1 Using the IP/Subnet filter field.

- Specify a website IP address for the destination website. By default, the IP address can be any address that the website uses.

- Select an option from the **Website Name** drop-down list to focus the results on specific websites or filter out specific websites. For more information about using this drop-down list, see Section 3.4.11.2 Filtering reports using common regular expressions.
- Select an option from the **URI** drop-down list to specify what the URI may or may not contain. For more information about using this drop-down list, see Section 3.4.11.2 Filtering reports using common regular expressions.
- Select an option from the **Category** drop-down list to narrow the search to specific website categories only.

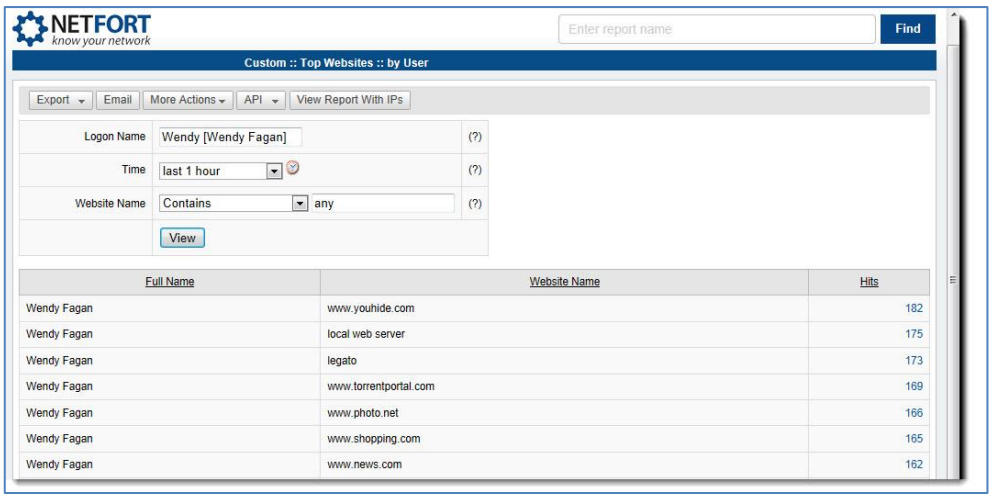
Click **View** to modify the results.

The detailed report page displays the following information:

Report Column	Description
Sensor	The sensor that detected the web activity.
Source IP	The IP address from which each web site was accessed.
Destination IP	The IP address and domain name of the destination website.
Category	The web category of the website.
Time	The time when the web activity occurred.
Website Name	The domain name of the website.
URI	The Uniform Resource Indicator (URI) accessed.
Drilldown	Click on the link to view a further breakdown of the data.

3.2.5.2 View web activity by user

When you search for web activity by user, the following report is displayed:

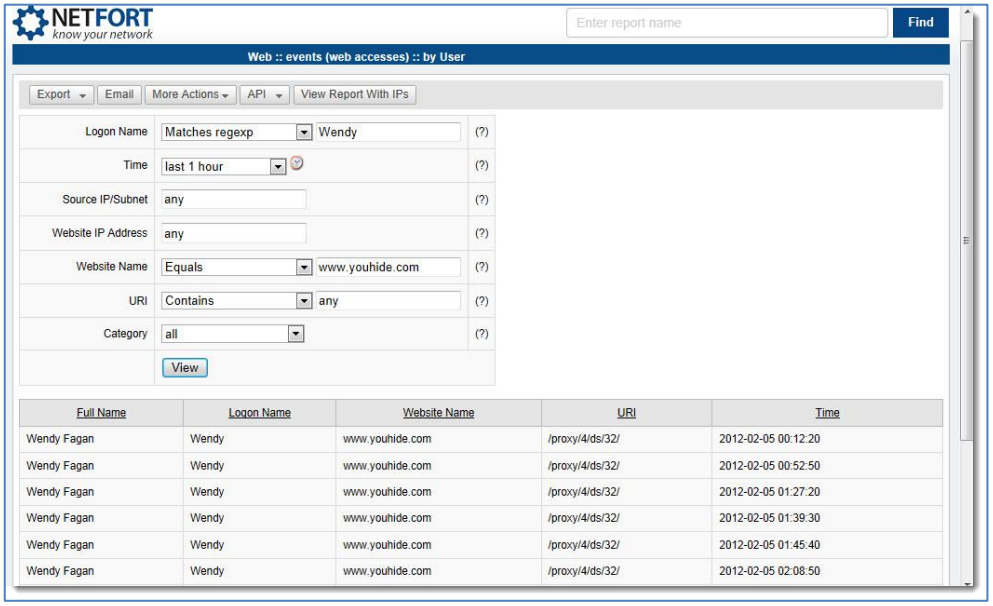


The results page lists all websites that the specified user accessed in the last hour, and the number of times each site was accessed. To modify the search results, you can:

- Enter a different username on the **Logon Name** field.
- Select **Last 4 hours** or **Last 24 hours** from the **Time** drop-down list to increase the duration to show more activity.
- Select an option from the **Website Name** drop-down list to focus the results on specific websites or filter out specific websites. For more information about using this drop-down list, see Section 3.4.11.2 Filtering reports using common regular expressions.

Click **View** to modify the results.

To view more detailed information about the web activity, click on the number in the **Total** column. A detailed report is displayed.



To modify the detailed search results, you can use the fields at the top of the results page, as follows:

- Select an option from the **Logon Name** drop-down list to focus the results on specific websites or filter out specific websites.
- Select **Last 4 hours** or **Last 24 hours** from the **Time** drop-down list to increase the duration to show more activity.
- Specify a source IP address in the **Source IP/Subnet** field. By default, the IP address is any address that the user uses.
- Specify a website IP address for the destination website in the **Website IP Address** field. By default, the IP address can be any address that the website uses.
- Select an option from the **Website Name** drop-down list to focus the results on specific websites or filter out specific websites. For more information about using this drop-down list, see Section 3.4.11.2 Filtering reports using common regular expressions.
- Select an option from the **URI** drop-down list to specify what the URI may or may not contain. For more information about using this drop-down list, see Section 3.4.11.2 Filtering reports using common regular expressions.
- Select an option from the **Category** drop-down list to narrow the search to specific website categories only.

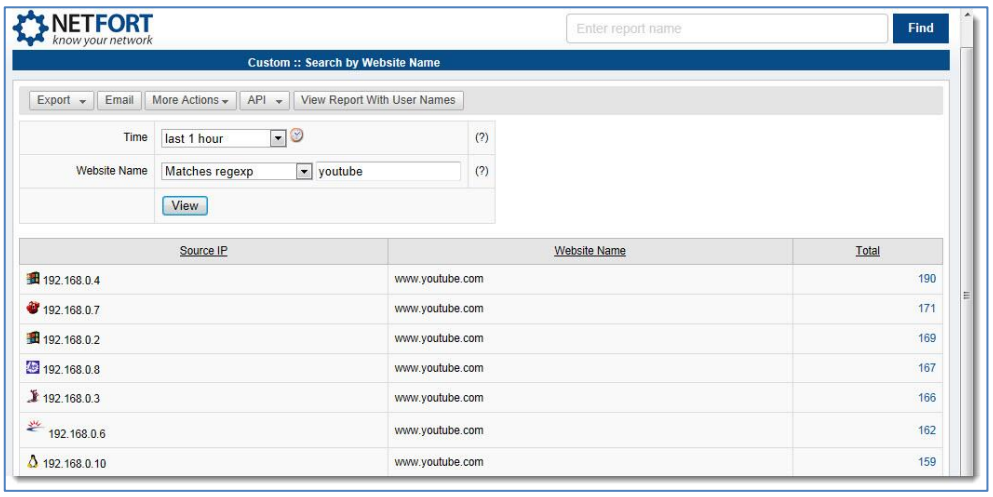
Click **View** to modify the results.

The detailed report displays the following information:

Report Column	Description
Full Name	The full name of the user.
Logon Name	The logon name of the user.
Website Name	The name of the website accessed.
URI	The URI accessed.
Time	The time the website was accessed.

3.2.5.3 View web activity by website

When you search for web activity by website, the following report is displayed:

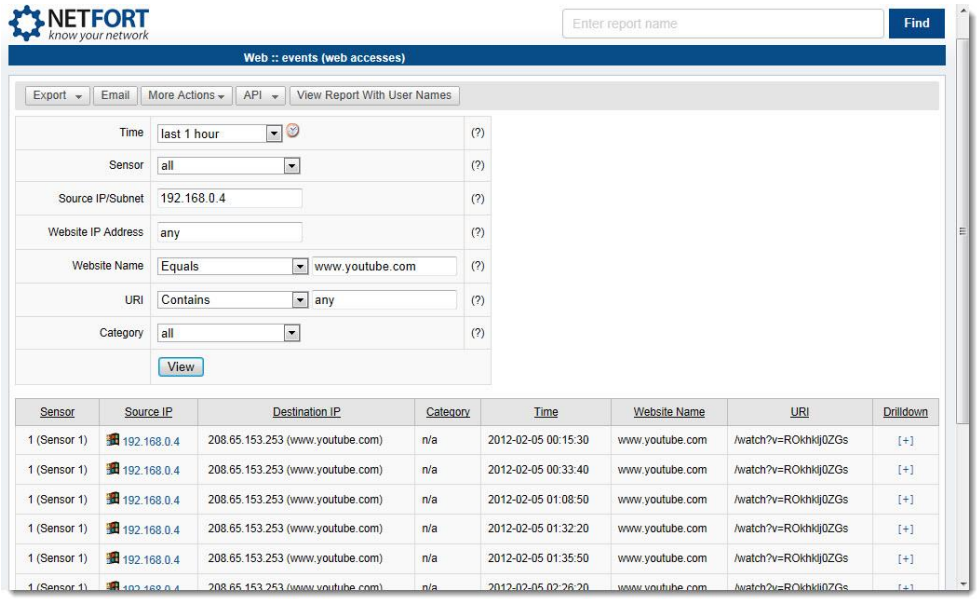


The results page lists the IP addresses that accessed the specified domain name or domain names containing the string that you entered, and the number of times each IP address accessed each site. To modify the search results, you can:

- Select **Last 4 hours** or **Last 24 hours** from the **Time** drop-down list to increase the duration to show more activity.
- Select an option from the **Website Name** drop-down list to focus the results on specific websites or filter out specific websites. For more information about using this drop-down list, see Section 3.4.11.2 Filtering reports using common regular expressions.

Click **View** to modify the results.

To view more detailed information about the web activity from each IP address to the website, click on the number in the **Total** column. A detailed report is displayed.



To modify the detailed search results, you can use the fields at the top of the results page, as follows:

- Select **Last 4 hours** or **Last 24 hours** from the **Time** drop-down list to increase the duration to show more activity.
- Select a different sensor from the **Sensor** drop-down list.
- Specify a different IP address in the **Source IP/Subnet** field.
- Specify a website IP address for the destination website. By default, the IP address can be any address that the website uses.
- Select an option from the **Website Name** drop-down list to focus the results on specific websites or filter out specific websites. For more information about using this drop-down list, see Section 3.4.11.2 Filtering reports using common regular expressions.
- Select an option from the **URI** drop-down list to specify what the URI may or may not contain. For more information about using this drop-down list, see Section 3.4.11.2 Filtering reports using common regular expressions.
- Select an option from the **Category** drop-down list to narrow the search to specific website categories only.

Click **View** to modify the results.

The detailed results page displays the following information:

Result	Description
Sensor	The sensor that detected the web activity.
Source IP	The IP address from which each web site was accessed.
Destination IP	The IP address and domain name of the destination website.
Category	The web category of the website.
Time	The time when the web activity occurred.
Website Name	The domain name of the website.
URI	The URI accessed.
Drilldown	Click on the link to view a further breakdown of the data.

3.3 Dashboards

The LANGuardian dashboards display live network information that you can use to monitor your network. To view the dashboards, click on **Dashboards** in the LANGuardian menu bar.

By default, LANGuardian displays four dashboards as follows:

- Bandwidth activity
- User activity
- File share activity
- Internet activity

You can customize the dashboards to show at a glance the network information that is most important to you. You can also create new dashboards and customize them by adding and arranging reports and graphs.

Dashboards are user-specific, so each user can have an instant view of the information that is most important to them. Each user can have a maximum of five dashboards.

You can add any LANGuardian trend or report to a dashboard. When you create new trends or reports, they immediately become available for addition to dashboards.

When you create or customize a dashboard, there are many different ways to organize the information. Here are some typical examples:

- All network activity associated with a single office location or department – file transfers, Internet access, traffic volume.
- Activity on an Internet connection – top websites, bandwidth usage, most active users.
- Compliance with internal and external policies – access to sites such as Facebook and MySpace, illegal downloading, access to file shares and databases containing sensitive information.
- Show network troubleshooting information – intrusions, worms, overloaded network links.

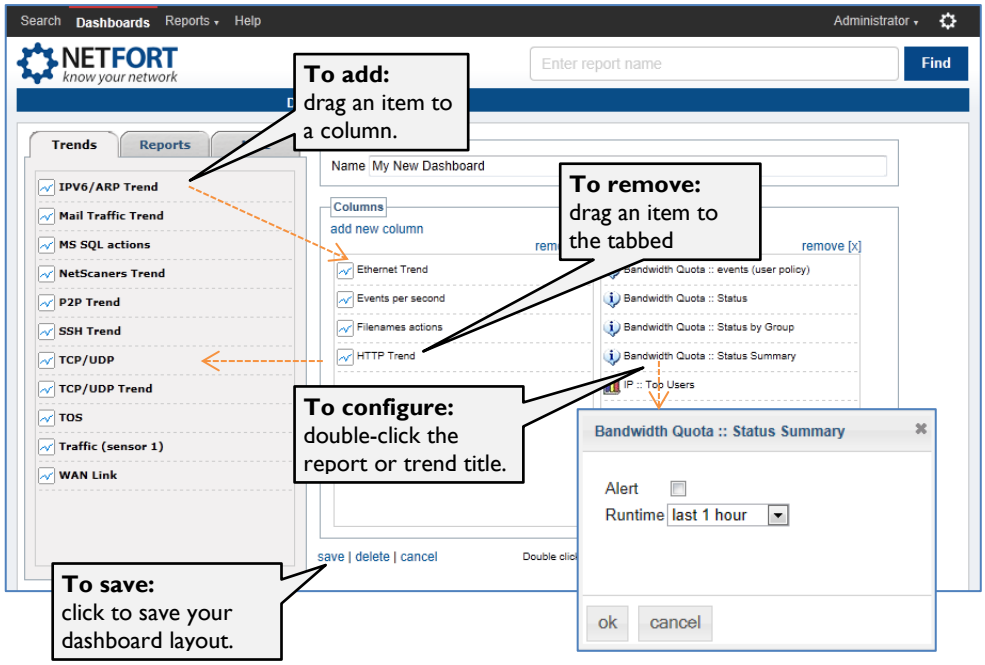
3.3.1 Creating a new dashboard

To create and populate a dashboard:

1. Click **Add** on the LANGuardian Dashboards page.

> **Note**
>
> The maximum number of dashboards that you can have is five. If you already have five dashboards, the **Add** button is not displayed.

The **Dashboard Configuration** page is displayed.



2. Type a name for the dashboard in the **Name** field. This name is displayed in the tab title.

3. To add an item to the dashboard, select the item from the **Trends**, **Reports**, or **Misc** tab, then drag it to the column in which you want it to appear. You can drag items up or down to reposition them within the column.

4. To remove an item from a dashboard column, drag it back to the tabs area.

5. By default, each new dashboard has two columns. To add a new column to the dashboard, click **add new column**. The new column is added to the right of the existing columns. To delete a column, click **remove**.

6. To configure a report or trend, double-click on its title in the dashboard column.

7. To save the new dashboard, click **save**. The new dashboard is created and displayed on the **Dashboards** page as a new tab.

3.3.2 Editing a dashboard

To edit an existing dashboard, click **Edit** on the LANGuardian Dashboard page.

The **Dashboard Configuration** page is displayed. Refer to Steps 2 to 6 in Section 3.3.1 Creating a new dashboard for information about how to edit the dashboard.

3.3.3 Deleting a dashboard

To delete a dashboard, click **Edit** on the LANGuardian Dashboard page. The **Dashboard Configuration** page is displayed. Click on **delete** to delete the dashboard. You are asked to confirm if you want to delete the dashboard. Click **Yes** to confirm the deletion.

3.4 Reports

LANGuardian captures all network traffic flowing through your core switch and, from the data it captures, creates a large number of reports. To view a report:

1. Click **Reports** on the LANGuardian menu bar.

   LANGuardian displays the reports that are most popular among our customer base at the top of each category. The **More>>** menu item allows you to view all of the reports available in each category.

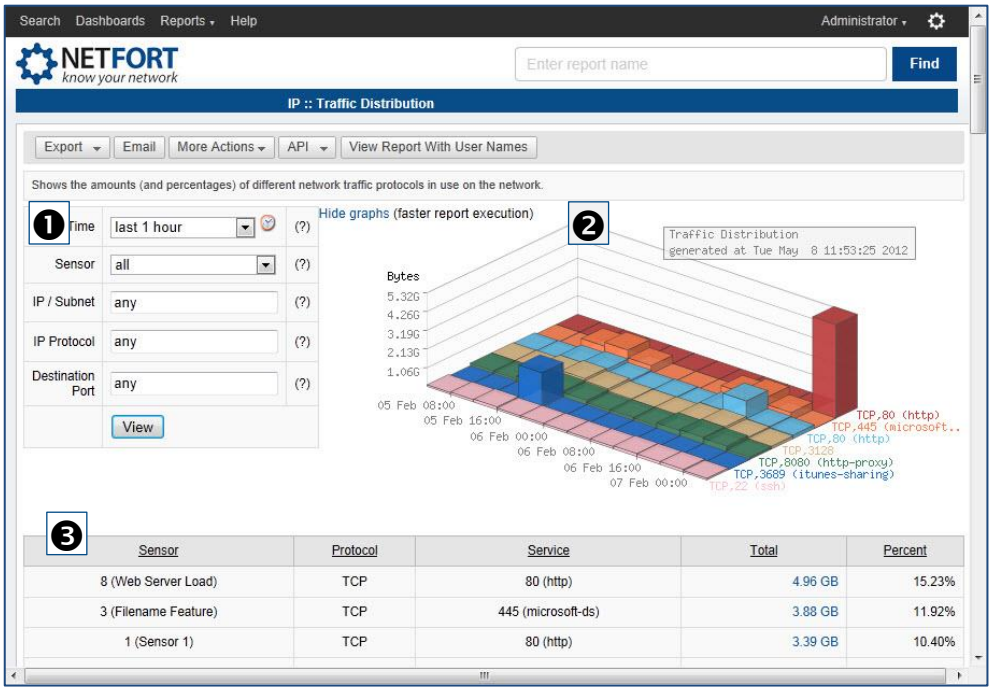
2. Select the report you require or click **More >>** and then select a report from the complete list of reports that are available.

3. (Optional) Modify the report fields to focus the report on particular information.

4. Click **View** to generate the report.

See Appendix A for a detailed list of all reports that are available.

The LANGuardian reports are displayed in three parts, as shown in the example below.



The three parts of each report are:

❶ Filter

Filtering allows you to narrow the report down to the information you want to see. The filter fields are report-specific. In the example above, you can filter the report data by sensor, operating system, or IP and subnet address.

❷ Graph

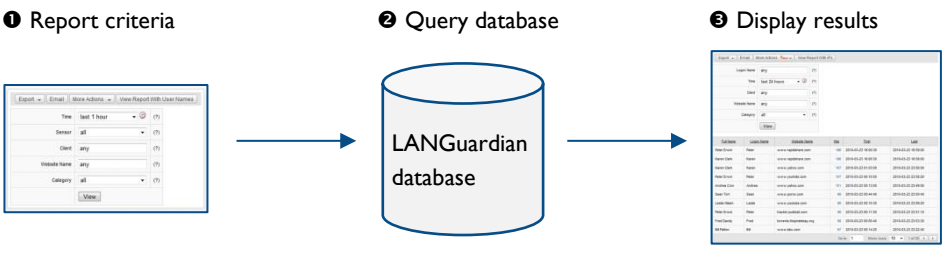
Many reports display the report data in a graph format. You can hide graphs for faster report execution.

❸ Data table

The report output data is displayed in a table after you click the **View** button. You can click on some report fields to drill down to more detailed information. In the example above, you can click on the numbers in the Total field to see which version of Windows each system is running.

3.4.1 How reports work

LANGuardian stores a copy of all network traffic in its traffic database. When you run a report, LANGuardian creates a query based on your report criteria, applies the query to the database, and displays the results in graphical and tabular format.



When you create custom reports, you can access them from the LANGuardian menu bar under **Reports > Custom**.

3.4.2 Custom reports

You can customize LANGuardian to provide exactly the data you need to meet your specific network monitoring requirements. The reports can range from general information about the whole network to details of accesses to a specific file by a specific user.

3.4.2.1 Saving a report as a custom report

If you make changes to the filter fields for a report, you may wish to save this report for future use. The report then becomes a custom report. To save a report:

1. Click **More Actions** on the report menu bar and select **Save Report**.
2. Type a name for the report in the **Name** field.
3. Type a brief description of the contents of the report in the **Description** field.
4. Click **Save**. The results are saved to a report and stored in the Custom reports section. The results are cleared from the current screen. To view the report, click **Reports** on the LANGuardian menu bar and select the report under the Custom section.

3.4.3 Exporting a report to a file

You can export any LANGuardian report to these formats:

- PDF (Portable Document Format), for viewing and printing with Adobe Reader or Adobe Acrobat.
- CSV (Comma-Separated Values) format, for importing into applications such as Microsoft Excel and Google Apps™.

You can also open LANGuardian reports in Microsoft Excel by setting up a data connection to the LANGuardian database using the REST API.

To export a report to a PDF or CSV file:

1. View the report that you want to export.
2. Click **Export** on the report menu bar and select **PDF** or **CSV** from the drop-down menu.
   - If you are exporting to PDF, the **Export to PDF** dialog is displayed. See Steps 2 and 3.
   - If you are exporting to CSV, the export operation is performed immediately and the results are displayed in Microsoft Excel.
3. In the **Export to PDF** dialog, select:
   - **Current** to export only the current page of results or **All** to export all of the results pages. The number of pages of results is indicated in the bottom right of the screen, for example, 1 of 18.

- **A4** or **Letter** to determine the paper size.
- **Portrait** or **Landscape** to determine the orientation of the pages.

4. Click **Export** to generate a PDF file.

3.4.4 Emailing a report

To email a report to an email address:

1. View the report that you want to email.
2. Click **Email** on the report menu bar.
3. Select **Current** to email only the current page of results or **All** to email all of the results pages. The number of pages of results is indicated in the bottom right of the screen, for example, 1 of 18.
4. Type the recipient email address in the **To** field.
5. Type a brief subject in the **Subject** field. For example, "Top Talkers Report from LANGuardian".
6. Type a message in the **Message** body.
7. Click **Send**.

The report is included in the message body and sent to the recipient.

You can email any LANGuardian report on demand, and you can also schedule reports to run and email the results to specific users at hourly, daily or weekly intervals.

3.4.5 Viewing the syntax of a report query

To view the syntax that was used to generate the report that you are currently viewing, click **More Actions** on the report menu bar and select **Report Syntax**. The code that was used to query the database and extract the results is displayed. This feature may be useful for advanced users who wish to create custom reports.

3.4.6 Printing a report

To print a report, click **More Actions** on the report menu bar and select **Print**. The report is displayed in a printer-friendly format in a new browser tab. Use the print options on your web browser to print the report.

3.4.7 Running a report in the background

You can run a report as a background process and request LANGuardian to send the report to a specified email address. To run a report in the background:

1. Open the report that you want to run.

2. Click **More Actions** on the report menu bar and select **Schedule Report**. The displayed fields are populated with the data that generated the report that you are viewing. You can modify any of these fields to broaden or narrow the report contents.

3. Type an email address in the **Email to** field. This is the address to which the report is sent after it is generated.

4. Type a subject for the email in the **Subject** field.

5. Select **HTML** or **CSV** to determine the format of the report.

6. Click **Schedule**. The report is run in the background once and the resultant report is sent to the email address that you specified.

3.4.8 Creating a trend report

You can create a trend from a report. Trends can then be displayed on a dashboard or you can access the trend by clicking on  in the LANGuardian menu bar and selecting **View Trends**.

To create a trend from a report:

1. View the report that you want to trend.

2. Select a sensor from the **Sensor** drop-down list. A trend must be connected to a particular sensor, so for trend reports, the default Sensor option of **all** is not acceptable.

3. Click **More Actions** on the report menu bar and select **Trend Report**.

4. Type a name for the trend in the **Trend Name** field.

5. Select the report columns that you want to include in the trend. By default, all report columns are currently included in the trend.

6. Click **Save**.

3.4.9 Embedding a report in a third-party application

To view a report from a third-party application without having to log on to LANGuardian, you can embed a link to a report in the third-party application. To do this from a results page:

1. View the report that you want to embed.

2. Click **API** on the report menu bar and select one of the following options from the drop-down list:

   - SolarWinds Orion
   - CSV

- Excel (Web Data Source)
- IFRAME

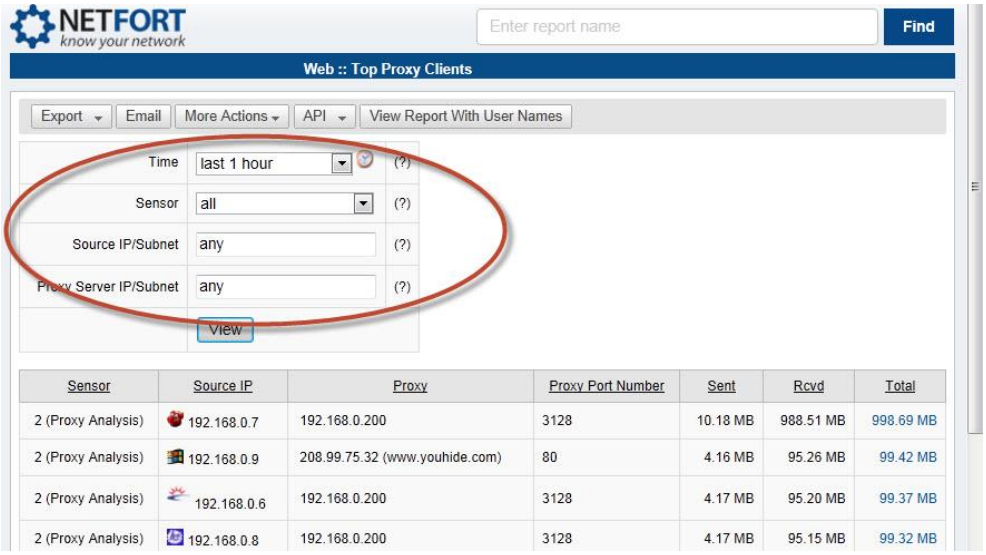
3. Follow the instructions in the window that is displayed to copy the link to the third-party application.

3.4.10 Modifying a report to view the data by IP address or username

If you are viewing a report by IP address and you want to view the data by username instead, or vice versa, click **View Report With IPs** or **View Report With User Names** on the report menu bar, as appropriate. This feature might not always be present, as it depends on the type of data being displayed.

3.4.11 Using report filters

When you run a report, there are a number of fields displayed after the report menu bar and before the report results, as shown below:



The fields that are displayed vary depending on the type of report that you are running. You can use these fields very effectively to modify the report results to display exactly the information that is of interest to you. The following sections describe some of the frequently-used report filter fields.

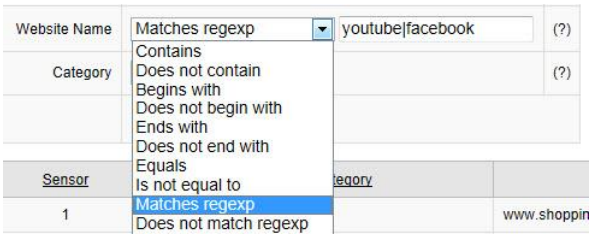
3.4.11.1 Using the IP/Subnet filter field

Many of the LANGuardian reports support the use of an **IP/Subnet** filter field to narrow the results of the report to specific IP addresses, a range of IP addresses, or to exclude certain IP addresses or ranges. The following table describes how to effectively use the **IP/Subnet** field to focus a report on the IP addresses that are of interest to you.

Examples of entries in the IP/Subnet filter field	Displays data for…
192.168.127.0/24	IP addresses in the range 192.168.127.1 to 192.168.127.254
192.168.127.1,192.168.127.2	The IP addresses 192.168.127.1 and 192.168.127.2 only
192.168.127.0/24,192.168.128.0/24	IP addresses in the range 192.168.127.1 to 192.168.127.254 and IP addresses in the range 192.168.128.1 to 192.168.128.254
192.168.0.0/16,!192.168.127.0/24	IP addresses in the range 192.168.0.1 to 192.168.255.254 but excludes IP addresses in the range 192.168.127.1 to 192.168.127.254

3.4.11.2 Filtering reports using common regular expressions

Some of the filter fields that are displayed before the LANGuardian reports contain a drop-down list to enable you to filter the report using regular expressions. For example, the following shows the drop-down list for the **Website Name** field:



The following table provides examples of some of the regular expressions that you can use to filter reports, depending on the filter field in use:

Example regular expression	Displays data for…
Website Name filter field with "Matches regexp" selected	
youtube	Websites that contain "youtube" in the URL
youtube|facebook|bebo	Websites that contain "youtube", "facebook", or "bebo" in the URL
Logon Name filter field with "Matches regexp" selected	
wendy	The user "wendy"
wendy|andrea|james	The users "wendy", "andrea", and "james"
^(?!wendy	All users excluding "wendy"
^(?!wendy)(?!andrea)(?!james)	All users excluding "wendy", "andrea", and "james"
URI filter field with "Matches regexp" selected	
\.mp3$\|\.wma$	All MP3 or WMA audio file downloads
\.torrent$	All P2P Torrent file downloads
\.rar$	All archive file downloads, typically associated

	with online file sharing services
If you first specify a search engine in the **Website Name** filter field, you can then enter one of the following in the **URI** field: • \&q= (Google) • \?q= (Bing) • search? (Yahoo)	All search strings sent to a search engine
File Name filter field with "Matches regexp" selected	
sales|profit|loss	All filenames or directory names that contain "sales", "profit", or "loss"
.mdb$	All file activity involving Microsoft Access databases
.docx$\|.xlsx$|.pptx$	All file activity involving Microsoft Word, Excel, or PowerPoint files
.mp3$\|.mp4$|.avi$\|.mpeg$|\.divx$	All file activity involving common media file types
\\itunes\\	All file activity involving a directory called "itunes"
\\itunes\\\|\\apple\\	All file activity involving directories called "itunes" and "apple"

Tip
To view file activity reports for files of a certain type, such as, all media files, all executable files, and so on, go to **Reports** > **Windows File Shares** > **More** for a comprehensive list.

3.4.11.3 Filtering SQL Server reports

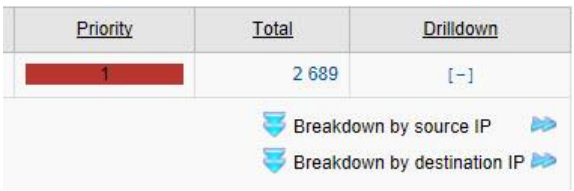
To view SQL Server reports, click on **Reports** in the LANGuardian menu bar, go to the **Other** section, and click on **SQL Server**.

To check if sensitive information such as passwords, user profiles, or addresses is being accessed on the network, you can use the **Statement** filter field in SQL Server reports. For example, to search for all SQL statements requesting password, username, or address information, select **Matches regexp** from the **Statement** drop-down list and enter **password|username|address**.

To check for instances of data drops from SQL databases, you can select **Drop** from the **Statement Type** filter field to display all drop statements.

3.4.12 Analyzing security event reports

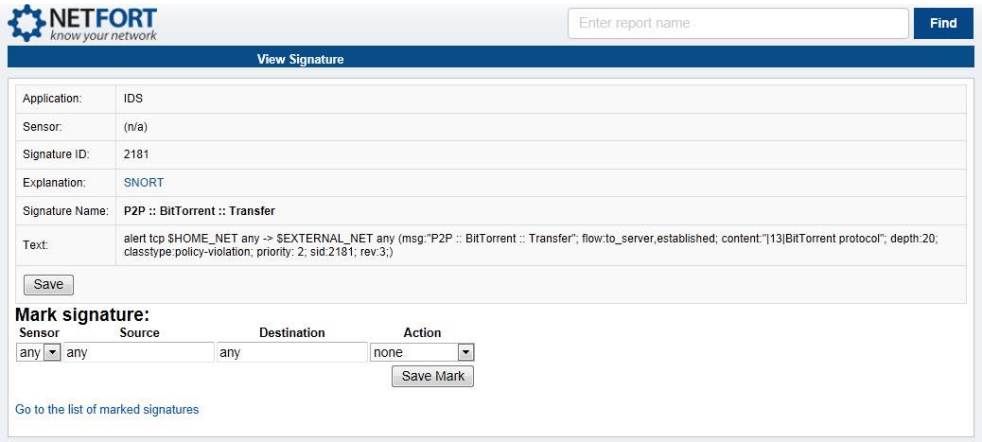
One of the key security reports in LANGuardian is the **Security :: by Signature** report. The report lists security events by signature. To view which systems are associated with the events, click on the **+** symbol in the **Drilldown** column and click on the arrows to the right of **Breakdown by source IP**.



LANGuardian displays the **Security :: by Source** report and lists the source IP address for each security event.

3.4.12.1 Working with signatures

When you view the **Security :: by Signature** report, you can click on the text of the signature in the **Signature** column to view the details of the signature. For example:



You can mark a signature so that an action is taken each time the security event occurs. To do this, select the action that you want to take from the **Action** drop-down list. The options are **Send Email** or **Ignore Events**. When you are marking a signature, you can also specify a particular sensor, source IP address, or destination IP address for the marked signature. Only security events that match the details that you provide are then alerted to you by email or ignored.

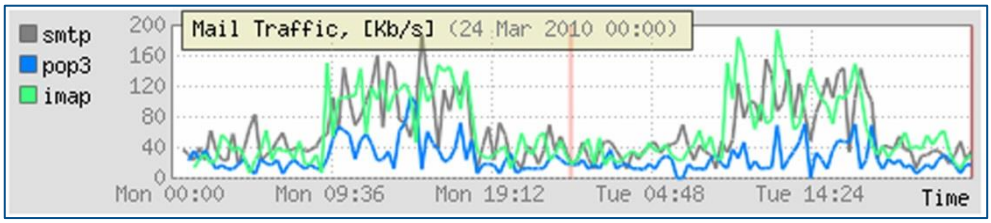
To view a list of all of the signatures that are marked, click on **Go to the list of marked signatures** at the end of the **View Signature** page.

3.5 Trends

With LANGuardian trends, you can monitor specific aspects of network activity over a period of time. A trend is a LANGuardian report that runs automatically at specified intervals, stores the data in the LANGuardian database, and displays the results in graph format. Trends allow you to identify anomalies in user behavior and traffic levels that you could not easily identify from reports. For example, a web traffic report would summarize the amount of web traffic over a specified period of time, whereas a trend based on the report would show you the variations in traffic volume during that time.

To view trends, click on ⚙ in the LANGuardian menu bar and select **View Trends**. LANGuardian displays a list of all existing trends.

The following is an example of a trend report.



The trend report is clickable. You can click on any data point in the trend graph to view a detailed report of the underlying traffic data. The detailed report is centered on the time of the selected data point.

There are two categories of trends:

- Event data

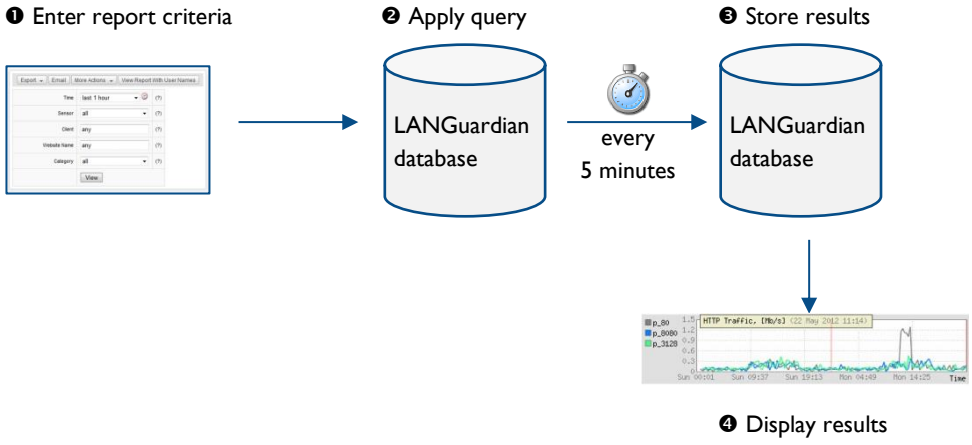
  Trends that show the number of events associated with the report filter criteria (for example, files deleted, SQL Server queries, or Active Directory logins). Event data is shown in as a graph with time on the horizontal axis and events per second on the vertical graph.

- Traffic data

  Trends that show the traffic volume associated with the report filter criteria. Traffic data is shown as a graph with time on the horizontal axis and traffic volume in kilobits or megabits per second on the vertical graph.

3.5.1 How trends work

LANGuardian stores a copy of all network traffic in its traffic database. When you create a report, LANGuardian queries the database and displays the results, but when you create a trend, LANGuardian takes the additional steps of querying the database at regular intervals and storing the results in the database.



LANGuardian queries the traffic database every five minutes to obtain the traffic volume or number of events seen over the previous five-minute period. It divides this value by 300 to obtain the average per-second value

for that time period (5 minutes = 300 seconds) and it stores this value as a trend data point in the LANGuardian database.

3.5.2 Creating trends from existing reports

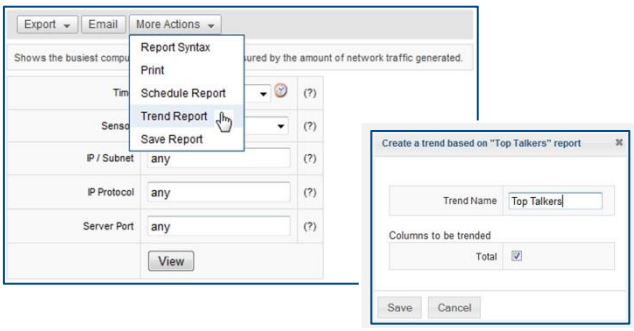
You can create a trend from any LANGuardian report that returns numerical data. The steps are as follows:

1. Display a standard report or create a custom report showing the network activity data you want to monitor over time.

2. Select a sensor from the **Sensor** drop-down list. A trend must be connected to a particular sensor, so for trend reports, the default Sensor option of **all** is not acceptable.

3. Click **More Actions** on the report menu bar.

4. Select **Trend Report** from the dropdown list.



5. Enter a name for the trend.

6. Select the report column for which you want to create a trend.

You can display the trend on a dashboard or you can access it by clicking on ⚙ in the LANGuardian menu bar and selecting **View Trends**.

3.5.3 Creating trends from scratch

Follow these steps to create a new trend without basing it on an existing report:

1. Click on ⚙ in the LANGuardian menu bar and select **Configure Trends**. LANGuardian displays a list of all existing trends.

2. To create a new trend, click **Add new trend**. The **Trend Wizard** is displayed.

3. Enter the trend details. The required fields are as follows:

Field	Description
Title	The title of your trend.
Number of sets	The number of data sets to include in the trend.
Sensors	The LANGuardian sensors whose traffic or event data you want to include in the trend.
Subnet	The subnet whose traffic data you want to include in the trend (applicable only when you select the **subnet traffic** template).
Select template	Select the type of trend report you want to create. The options are: ▪ Events ▪ Total traffic ▪ Subnet traffic ▪ Packets per second

4. Click **Add** to create the trend.

3.5.4 Adding an alarm to a trend

You can add an alarm to a trend as follows:

1. Click on ⚙ in the LANGuardian menu bar and select **Configure Trends**. LANGuardian displays a list of all existing trends.

2. To add an alarm to a trend, click on the 💡 icon in the **Alarms** column next to the trend.

3. Enter the following alarm details:

   - **Name**: Type a name for the alarm
   - **Alarm Level**: Type the level at which the alarm is triggered. For example, 100 Mb/s.
   - **Set**: Select the appropriate data type that you want to monitor for the alarm from the **Set** drop-down list. The contents of this drop-down list will vary depending on the trend type.
   - **Alert**: Select whether the alarm is triggered when the level goes **Above** or **Below** the level specified in **Alarm Level**.
   - **Action**: Select the action to take when the alarm is triggered. The options are **none**, **Send Email**, **Ignore Events**, or **send snmp trap**.
   - **Description**: Type a description for the alarm.

4. Click **save**.

When you view the list of existing trends, the trends for which alarms are set show the  icon next to the trend.

3.5.5 Default LANGuardian trends

The following trends are available when you install a new LANGuardian instance.

Trend	Description and key settings
Events per second	All security events detected in overall LANGuardian traffic.
HTTP traffic (kilobits/second)	All HTTP traffic on the network. Filters: Port: 80 IP Protocol: 6 (TCP)
IPV6/ARP usage (kilobits/second)	All IPV6 traffic on the network. Filter: EtherType: 0x86dd
Mail traffic (kilobits/second)	All outgoing e-mail traffic on the network. Filters: Port: 25 IP Protocol: 6 (TCP)
NetScans trend (events/second)	Systems that are establishing connections to multiple hosts on a specific port number.
P2P report (kilobits/second)	Peer-to-peer activity on the network. Filters: Port: 4662 IP Protocol: 6
SSH usage (kilobits/second)	Users or applications connecting to systems using Secure Shell (SSH). Filters: Port: 22 IP Protocol: 6
Traffic (kilobits/second)	All network traffic.
UDP and TCP (kilobits/second)	All UDP and TCP traffic on the network. Filter: IP Protocol: 6

3.6 Alerts

LANGuardian can generate e-mail messages to notify selected users whenever events occur or predefined thresholds are breached on the network. Alerts allow the e-mail recipient to take action immediately and, in many cases, to identify and fix problems before they affect security or end-user productivity.

LANGuardian divides alerts into five categories:

- Alert based on a report

  Generates a report and sends it to the associated distribution list at two-hour intervals.

- Alert based on a trend

  Generates a trend report and sends it to the associated distribution list whenever the threshold values specified in the trend are breached.

- Alert when a specific website is accessed

  Generates an alert whenever a user accesses a website that is listed on the remote or local watchlists.

- Alert when a system or service goes down

  Generates an alert whenever a system fails to respond to a scheduled ping or TCP connection.

- Alert when new IDS events occur

  Generates an alert whenever the LANGuardian intrusion detection system detects a network traffic pattern that matches a signature stored in the system.

3.6.1 Distribution lists for alerts

LANGuardian uses distribution lists to manage sending alerts to users. When you create an alert, you associate it with a distribution list, and the users on the distribution list receive the alerts. You can create as many distribution lists as you like and use them to ensure that users see only the alerts that are relevant to them.

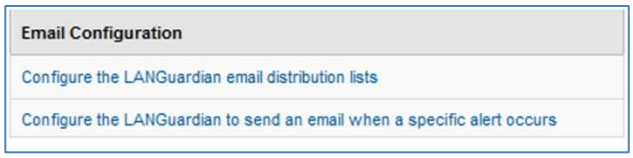
In a new LANGuardian installation, there are two predefined distribution lists:

- Alerts
- Periodic

To add a new list:

1. Click on  in the LANGuardian menu bar and select **Configuration**.

2. On the **LANGuardian Configuration** page, click **Configure the LANGuardian email distribution lists.**

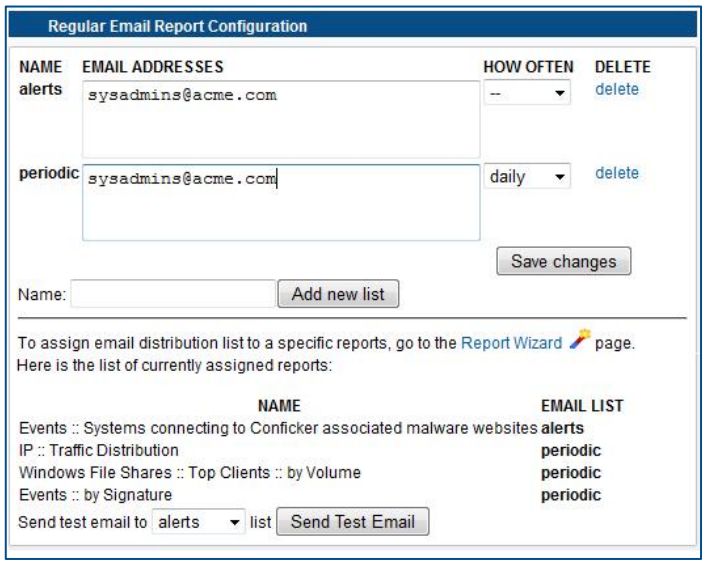


3. Enter a name for your list in the **Name** field, then click **Add new list.** LANGuardian will create the new list.

4. Add names to the list.

5. Choose **hourly, daily,** or **weekly** from the **How often** drop-down list.

6. Add names to the list and click **Save changes** when you are finished.



3.6.2 Alert based on a report

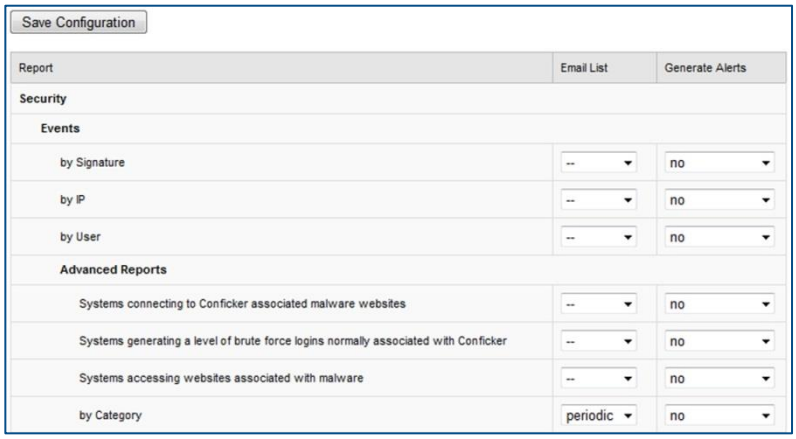
You can generate an alert based on any report in your LANGuardian system.

To create an alert based on a report:

1. Click on ⚙ in the LANGuardian menu bar and select **Configuration**.

2. On the **LANGuardian Configuration** page, click **Create an alert based on a report.**

3. The Report Wizard shows a list of all reports, built-in and custom reports. For each report, you can specify whether LANGuardian should generate alerts based on the report, and the distribution list to which the alerts will be sent.



4. Click **Save Configuration** to update the alerts list.

3.6.3 Alert when a website is accessed

LANGuardian can alert you when a user on your network accesses websites that are listed on its watchlists. There are two watchlists:

- Online

  The online watchlist is maintained by NetFort Technologies and any LANGuardian system with Internet access can look it up. The watchlist is an up-to-date list of known sites that are divided into the following categories:

  - Adult
  - Spyware
  - External proxies
  - User-defined
  - Social networking
  - Gaming and gambling
  - Malware
  - P2P

  You can choose the categories for which you want LANGuardian to generate alerts. If you find that LANGuardian is alerting you about accesses to sites you do not want to be alerted about, you can override the online watchlist locally.

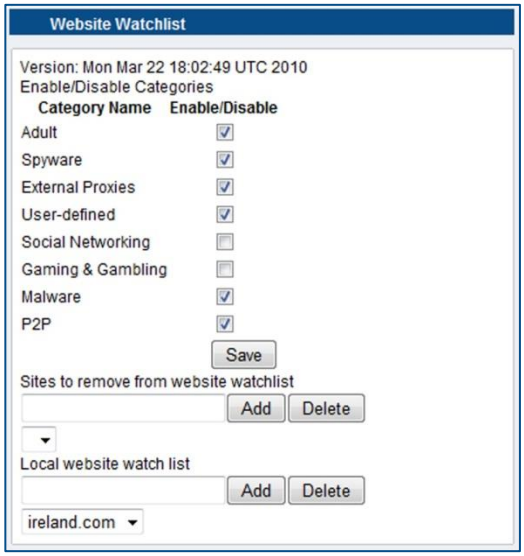
- Local

  The local watchlist supplements the online watchlist with sites that are specific to your network.

To create an alert when a specific website is accessed:

1. Click on ⚙ in the LANGuardian menu bar and select **Configuration**.
2. On the **LANGuardian Configuration** page, click **Create an alert when a specific website is accessed.**

3. LANGuardian displays the **Website Watchlist** page.



4. On the **Website Watchlist** page:

   a. Enable or disable each of the categories in the online watchlist.

   b. To prevent LANGuardian alerting you about accesses to a site on the online watchlist, enter the address of the site in the **Sites to remove from website watchlist** field.

   c. To configure LANGuardian to alert you about accesses to sites not on the online watchlist, enter the address of the site in the Local website watchlist field.

   d. Click **Save** to save your changes.

3.6.4 Alert when a system or service goes down

To create an alert when a system or service goes down:

1. Click on ⚙ in the LANGuardian menu bar and select **Configuration**.

2. On the **LANGuardian Configuration** page, click **Create an alert when a system or service goes down.**

3. Select the method that you are using to monitor the systems or services by clicking on an arrow in the **Go** column. The options are:

   - ICMP ping
   - TCP connect

4. Enter information in the following fields:

   - Title

- IP address
- Port (TCP connect only)
- Icon
- Show on a dashboard

5. Click **Save**.

3.6.5 Alert when a new IDS event occurs

To create a new IDS event and an alert for when the new IDS event occurs:

1. Click on ⚙ in the LANGuardian menu bar and select **Configuration**.
2. On the **LANGuardian Configuration** page, click **Create a new IDS signature.**
3. To create the new IDS event, edit the **Text** field to enter the details of the IDS event.
4. To create an alert when this IDS event occurs, go to the **Mark signature** section.
5. Select a sensor for detecting the event from the **Sensor** drop-down list.
6. Specify a source IP address and destination IP address. The default is any.
7. Select the action to take when the IDS event occurs from the **Action** drop-down list. The options are:
   - **None** – the event is logged in the database.
   - **Send Email** – the event is logged in the database and an email is sent.
   - **Ignore Events** – the event is ignored and not logged in the database.
   - **Send snmp trap** – the event is logged in the database and an SNMP trap is sent.
8. Click **Save Mark**.

3.7 Uploading network traffic PCAP files

There are a number of ways to capture network traffic in the form of PCAP files, for use with the LANGuardian. Examples of popular tools are Wireshark® and the UNIX `tcpdump` command. LANGuardian also accepts traffic captures from Fluke meters.

3.7.1 Capturing network traffic using Wireshark

The Windows-based Wireshark tool is effective and easy to use for capturing PCAP files of network traffic. To capture PCAP files of network traffic using Wireshark, do the following:

1. Download Wireshark from http://www.wireshark.org and install it.
2. Go to the **Capture** section. A list of the network interface cards (NICs) detected on your system is displayed.
3. To start to capture traffic, click on the NIC that is capturing the traffic of interest. The traffic capture begins.
4. To stop capturing the traffic, select **Capture** > **Stop**. You should keep the capture file under 500MB as this is the file size limit for LANGuardian utility.
5. To save the capture file, select **File** -> **Save As** and specify a name for the file.

The following table lists some useful Wireshark filter commands:

Wireshark filter	Purpose
ip.addr==10.0.0.1	Sets a filter for any packet with 10.0.0.1 as either the source or destination IP address.
ip.addr==10.0.0.1 && ip.addr==10.0.0.2	Sets a conversation filter between the two defined IP addresses.
http or dns	Sets a filter to display all http or dns traffic.
tcp.port==4000	Sets a filter for any TCP packet with the source or destination port of 4000.
tcp.flags.reset==1	Displays all TCP resets.
http.request	Displays all HTTP GET requests.
tcp contains traffic	Displays all TCP packets that contain the word "traffic". This filter is very useful when searching for a specific string or user ID.
!(arp or icmp or dns)	Masks out arp, icmp, dns, or any other protocols that you specify as background noise. This allows you to focus the results on the traffic of interest to you.
udp contains 33:27:58	Sets a filter for the HEX values of 0x33 0x27 0x58 at any offset.

tcp.analysis.retransmission	Displays all retransmissions in the trace. This filter helps when you want to track down slow application performance and packet loss.

3.7.2 Uploading a PCAP file to LANGuardian

To upload a PCAP file to LANGuardian, do the following:

1. Click on ⚙ in the LANGuardian menu bar and select **Sensors**.
2. Go to the PCAP sensor and click **PCAP File Upload**.
3. Use the **Upload File** option to add the PCAP file to the LANGuardian sensor.
4. When the file is uploaded, click **Process** to add this traffic to the database and allow reports to be run on it.

3.8 User accounts

Every user who needs to access the LANGuardian user interface requires a user account.

3.8.1 Adding a user account

To add a new user account:

1. Click on ⚙ in the LANGuardian menu bar and select **Configuration**.
2. On the **LANGuardian Configuration** page, scroll to the **System** section.
3. Click **Add/Edit LANGuardian user accounts**.
4. Click **Add new user**.
5. Enter a username and password for the new user and click **Add User**. The new user is created and listed in the **NetFort LANGuardian Accounts** page.

3.8.2 Deleting a user account

To delete a user account:

1. Click on ⚙ in the LANGuardian menu bar and select **Configuration**.
2. On the **LANGuardian Configuration** page, scroll to the **System** section.
3. Click **Add/Edit LANGuardian user accounts**.

4. Click **delete** in the **Actions** column next to the user. You are asked to confirm if you want to delete this user.

3.8.3 Editing user accounts to control access

You can control the permissions that LANGuardian users have within the system and to control access to LANGuardian reports and dashboards. To do this:

1. Click on  in the LANGuardian menu bar and select **Configuration**.
2. On the **LANGuardian Configuration** page, scroll to the **System** section.
3. Click **Add/Edit LANGuardian user accounts**. The **NetFort LANGuardian Accounts** page is displayed.
4. To control access to reports, click **edit** in the **Reports** column, then:
    a. To allow access to all reports, select the **View all** radio button.
    b. To select which reports the user can access, select the **Custom setup** radio button, and select the checkbox next to each report that you want the user to access.
    c. Click **Save Reports** to save the changes.
5. To control access to dashboards, click **edit** in the **Dashboards** column, then:
    a. To allow access to all dashboards, select the **View all** radio button.
    b. To select which dashboards the user can access, select the **Custom setup** radio button, and select the checkbox next to each dashboard that you want the user to access.
    c. Click **save** to save the changes.
6. To allow the user to use the PCAP sensor:
    a. Click **edit** in the **Permissions** column next to the user.
    b. Select the **Allow User to use PCAP Sensor** checkbox.
    c. Click **Save Permissions**.

3.8.4 Resetting a user password

To reset the password for a user:

1. Click on ⚙ in the LANGuardian menu bar and select **Configuration**.
2. On the **LANGuardian Configuration** page, scroll to the **System** section.
3. Click **Add/Edit LANGuardian user accounts**.
4. Click **reset password** in the **Actions** column next to the user. You are asked to confirm if you want to reset the password.
5. Click **Yes**. The password is reset and the new password is displayed at the top of the page.

3.8.5 Modifying the current user account

To modify your LANGuardian account settings, click on **Administrator** in the LANGuardian menu bar and select **Account settings**.

You can use the **Account settings** page to:

- Change your login password
- Select the page that is displayed when you log in to LANGuardian. The options are the **Search** page or the **Dashboards** page.

To save any changes to your account settings, click **Save**.

3.9 Monitoring a WAN connection

If LANGuardian is deployed in a large enterprise network, as described for example in Section 1.4.5 Monitoring large-scale enterprise networks with LANGuardian, there are some basic steps that you can take to start monitoring the sites in the WAN. The following procedure describes five basic steps to start monitoring a WAN connection:

1. Determine the IP address or subnet range for each WAN site.

   Before you can start monitoring a WAN, you must first determine the IP address range or subnet range for each site in your organization. The following table shows some examples of typical IP information:

IP Address/Subnet	Monitors traffic for …
192.168.127.0/24	IP addresses in the range 192.168.127.1 to 192.168.127.254
192.168.127.1,192.168.127.2	The IP addresses 192.168.127.1 and 192.168.127.2
192.168.127.0/24,192.168.128.0/24	IP addresses in the range 192.168.127.1 to 192.168.127.254 and 192.168.128.1 to 192.168.128.254
192.168.0.0/16,!192.168.127.0/24	IP addresses in the range 192.168.0.1 to 192.168.255.254 but excludes IP addresses in the range 192.168.127.1 to 192.168.127.254

2. Set up a Traffic Distribution Report.

   a. Click on **Reports** in the LANGuardian menu bar.

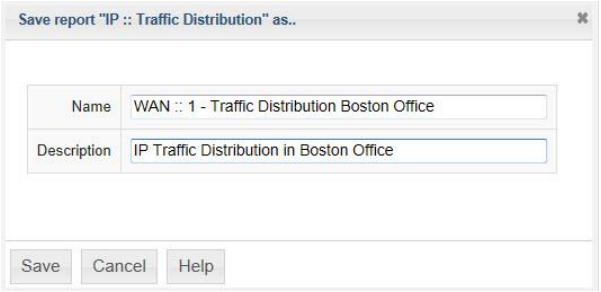
   b. In the **IP** section, click on **Traffic Distribution**. The **IP** :: **Traffic Distribution** report is displayed.

   c. Enter the IP information that you gathered in Step 1 in the **IP/Subnet** field.

   d. Click **View**.

   e. When the report is displayed, click **More Actions** on the report menu bar and select **Save Report**.

   f. Enter a name and description for the report, then click **Save**. We recommend that you use a naming convention similar to that shown in the following example to ensure that all WAN reports are grouped together when they are listed in the **Custom Reports** section:



3. Set up a File Share Analysis Report, if you use Microsoft files shares on your network.

    a. Click on **Reports** in the LANGuardian menu bar.

    b. In the **Windows File Shares** section, click on **More >>**. A list of Windows File Share reports is displayed.

    c. Scroll down through the list and click on **Top Clients :: by Volume**.

    d. Enter the IP information that you gathered in Step 1 in the **Source IP/Subnet** field.

    e. Click **View**.

    f. When the report is displayed, click **More Actions** on the report menu bar and select **Save Report**.

    g. Enter a name and description for the report, then click **Save**. We recommend that you use a naming convention similar to that shown in the example given in Step 2, for example "WAN :: 2 - Windows File Share Traffic Boston Office".

4. Set up a Proxy Analysis Report, if you use proxy servers on your network. This allows you to monitor traffic on the WAN that is associated with clients connecting to Internet sites through proxy servers.

    a. Click on **Reports** in the LANGuardian menu bar.

    b. In the **Web** section, click on **More >>**. A list of Web reports is displayed.

    c. Click on **Top Proxy Clients by IP**.

    d. Enter the IP information that you gathered in Step 1 in the **Source IP/Subnet** field.

    e. Click **View**.

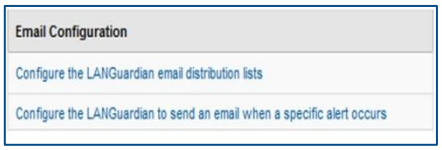
f. When the report is displayed, click **More Actions** on the report menu bar and select **Save Report**.

g. Enter a name and description for the report, then click **Save**. We recommend that you use a naming convention similar to that shown in the example given in Step 2, for example "WAN :: 3 – Top Proxy Clients Boston Office".

5. Create a trend. This allows you to plot the WAN site traffic on a graph, which you can use for troubleshooting or to analyze site capacity.

a. Click on ⚙ in the LANGuardian menu bar and select **Configure Trends**. LANGuardian displays a list of existing trends.

b. To create a new trend, click **Add new trend**. The **Trend Wizard** is displayed.



c. Enter the trend details. The required fields are as follows:

Field	Description
Title	Enter a title for the trend.
Number of sets	The number of data sets to include in the trend.
Sensor	Select the LANGuardian sensor that is monitoring the data for the WAN site.
Subnet	Enter the IP information for the WAN site. This is the information that you gathered in Step 1 of this procedure.
Select template	Select one of the following options for the type of trend report that you want to create: ▪ Total traffic – the graph displays a single line showing the total traffic to and from the site. ▪ Subnet traffic – the graph displays two lines; one line showing the outbound traffic to the site, and the other line showing the inbound traffic from the site.

d. Click **Add** to create the trend.

Chapter 4

Chapter 4 - Integrating LANGuardian with SolarWinds® ORION®

This chapter describes how to integrate NetFort LANGuardian into a SolarWinds ORION® Network Performance Monitor (NPM) environment. With the LANGuardian Integration Pack for SolarWinds Orion installed, you can view LANGuardian reports and data in your SolarWinds Orion environment.

4.1 LANGuardian and SolarWinds

NetFort LANGuardian monitors traffic flowing through a network, while SolarWinds Orion monitors the performance of devices connected to the network. Together, they provide a single point of access to all the information a network engineer needs to monitor and troubleshoot a network.

4.1.1 System requirements and permissions

Before you integrate LANGuardian with Orion, you must have both products installed and running correctly on your network.

The version requirements are as follows:

- LANGuardian 8.8 or higher.
- SolarWinds Orion Network Performance Monitor 10.1 or higher.

To complete the installation, you must have the following permissions:

- Administrator access to the Windows server on which Orion is installed.
- Administrator rights on the Orion implementation into which LANGuardian will be integrated.
- Administrator access to the LANGuardian system you want to integrate with Orion.

4.1.2 How the integration works

Orion views are made up of resources. You can customize views by adding, removing, and reordering resources. The integration pack creates some additional, NetFort-specific, resources in your Orion environment. These resources enable you to add the most commonly used LANGuardian reports to your Orion environment. You can display or hide the reports by customizing the Orion user interface.

If you want to display LANGuardian reports in Orion that are not included in the integration pack, you can manually create Orion custom HTML resources for them. See Displaying LANGuardian reports in the Orion view for instructions on how to do this.

From a technical point of view, integration between LANGuardian and Orion is made possible by the LANGuardian REST API. The integration is at the user interface level only. No data is transmitted from LANGuardian to the Orion database. The integration does not affect the performance of the Orion installation.

4.1.3 Security and authentication

When you access the LANGuardian web browser user interface you must authenticate yourself by entering a username and password. Similarly, when you integrate LANGuardian into an Orion view, the NetFort resource on the Orion view must authenticate itself with LANGuardian so that it can retrieve the data it needs.

We recommend that you create an Orion-specific user profile on LANGuardian and give it access to all reports. Use this profile when configuring the Orion system.

Warning! Do not embed the **LANGuardian** administrator user name and password in your Orion views.

Follow these steps to add an Orion-specific account to LANGuardian:

1. Click **Configuration** on the **Administration** menu.
2. On the **Configuration** page, scroll down to the **System** section.
3. Click **Add/Edit LANGuardian user accounts**.
4. On the **LANGuardian Accounts** page, click **Add new user**.
5. Enter the username (for example, **OrionUser)** and password details for the new account.
6. Click **Add User** to create the account.

Follow these steps to give the Orion-specific user access to all reports:

1. On the **LANGuardian Accounts** page, click the edit button in the **Reports** column for the Orion user you have just added.

2. On the **Edit existing reports for user** page, click **View all**, then scroll down to the bottom of the page and click **Save Reports**.

4.2 Installing the integration pack

The integration pack is provided as a zip file.

4.2.1 Download location

You can download the integration pack from the NetFort website:

www.netfort.com/downloads/

On this page, click the link to the LANGuardian Integration Pack for SolarWinds Orion, and follow the instructions.

4.2.2 Installation folder location

Orion is deployed as a web application hosted by Internet Information Services (IIS) on Microsoft Windows Server 2003 or Windows Server 2008.

To install the LANGuardian integration pack, you must add the LANGuardian files to the folder on the server where the Orion web application is hosted. Usually, the path to this folder is:

```
C:\inetpub\SolarWinds
```

Check if this folder exists on your server. If it does not exist, or if it exists and does not contain any files, then it is likely SolarWinds is installed in a different folder or on a different drive. You can find out exactly where it is installed by querying the Windows registry:

```
C:\> reg query "HKLM\Software\SolarWinds.net\SolarWinds 2002\Orion"
```

This command will return the location of the Orion installation folder, for example:

```
HKEY_LOCAL_MACHINE\Software\SolarWinds.Net\SolarWinds 2002\Orion
     Web Root Dir    REG_SZ    d:\websites\SolarWinds
```

4.2.3 Extracting files

After you download the zip file, you must extract the files and place the contents of the zip file in the SolarWinds installation folder, as follows:

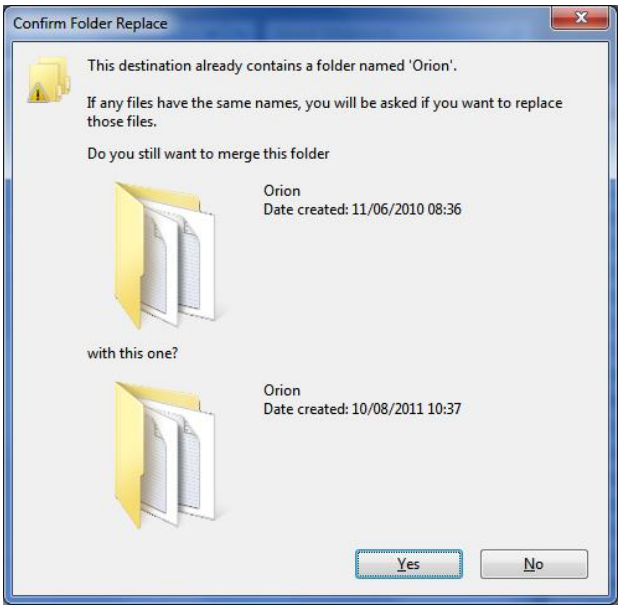
1. Open the zip file with Windows Explorer or an application such as WinZip, WinRAR, or 7-zip.

   The zip file contains a folder called **Orion**.

2. Extract the **Orion** folder from the zip file to the folder where SolarWinds is installed, for example:

   `C:\inetpub\SolarWinds`

   Because the folder already contains a subfolder called **Orion**, Windows will ask you if you want to merge the existing folder and the new folder containing the integration pack files.



   Click **Yes** to merge the folders and complete the installation.

You might experience permission problems copying the NetFort files into the SolarWinds folder if you are not logged in to the server as Administrator. There are several ways to work around this problem:

- Log in to the server as Administrator.
- Run your zip file extraction program as Administrator (right-click on the program icon, then choose **Run As…** from the pop-up menu).
- Make sure the account you are using to log on to the server has write access to the installation folder.

4.2.4 Connecting to LANGuardian

After you have installed the files, the next step is to configure Orion with the address and authentication details of the LANGuardian system.

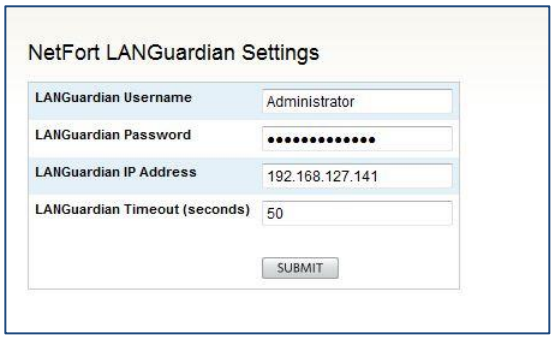
1. Open a web browser and navigate to the Orion home page.
2. Relative to the Orion home page, the address of the LANGuardian settings page is **NetFort/Settings.aspx**. To access the settings page, append this address to the URL in the browser address bar.

   For example, if the address of your Orion home page is

   http://192.168.1.127/Orion

   The address of the LANGuardian settings page will be

   http://192.168.1.127/Orion/NetFort/settings.aspx
3. On the **NetFort LANGuardian Settings** page, enter:
   - The username and password of the Orion-specific user account that you set up in Section 4.1.3
   - The IP address of the LANGuardian system you want to integrate with Orion
   - A timeout value, after which the LANGuardian resources that are embedded in the Orion views will display an error. The default is 30 seconds.



Note

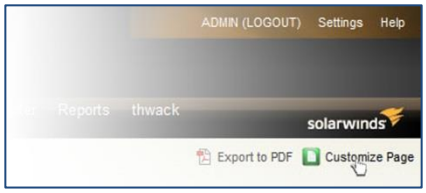
Some LANGuardian customers access the system using a hostname (for example, http://languardian.local) instead of an IP address. If you access LANGuardian this way, enter the hostname in the IP address field instead of the IP address.

4. Click **Submit** to complete the integration pack installation.

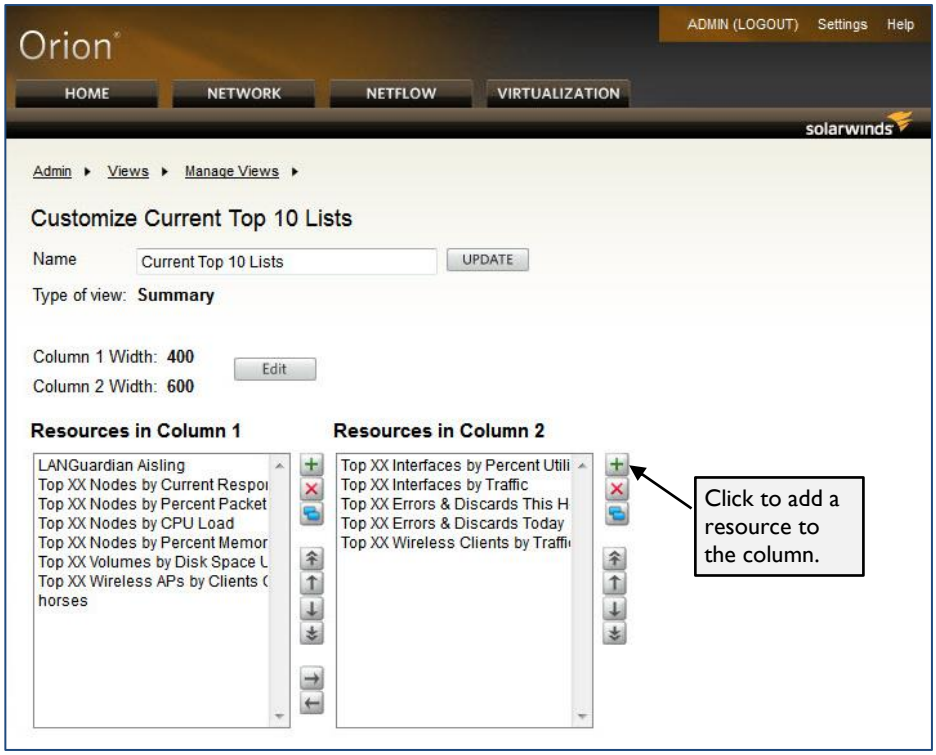
4.2.5 Adding LANGuardian reports to an Orion view

Installing the integration pack makes LANGuardian reports available as resources in your Orion environment. To display a report, you must add the corresponding resource to an Orion view.

1. In the Orion user interface, browse to the page where you want the LANGuardian information to be displayed. For example, to add the report to the Orion Top 10 page, click **Home** on the Orion main menu, then click **Top 10**.
2. Click **Customize Page**.



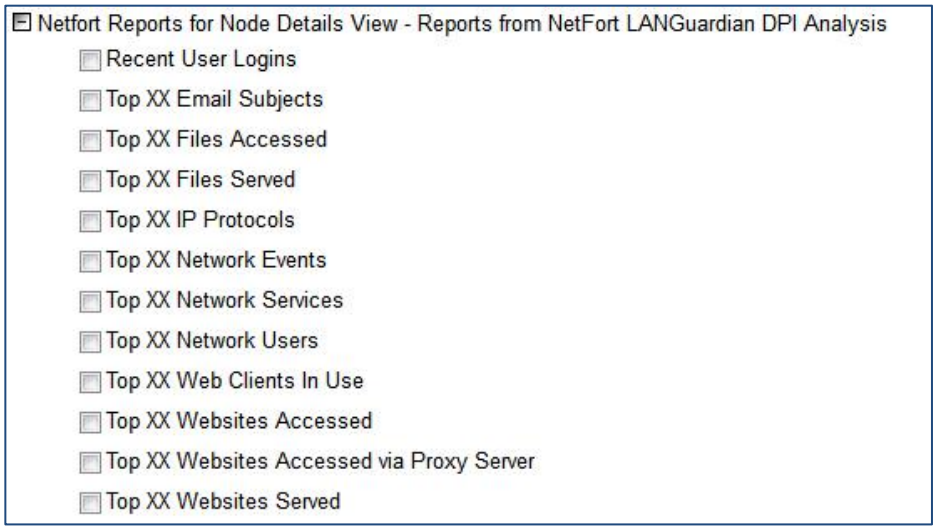
3. Select the column to which you want to add the LANGuardian report and click the + icon to add a resource to the column.



4. Orion displays the **Add Resources to Column** page. Scroll down to the NetFort Reports resources. These are divided into three categories:

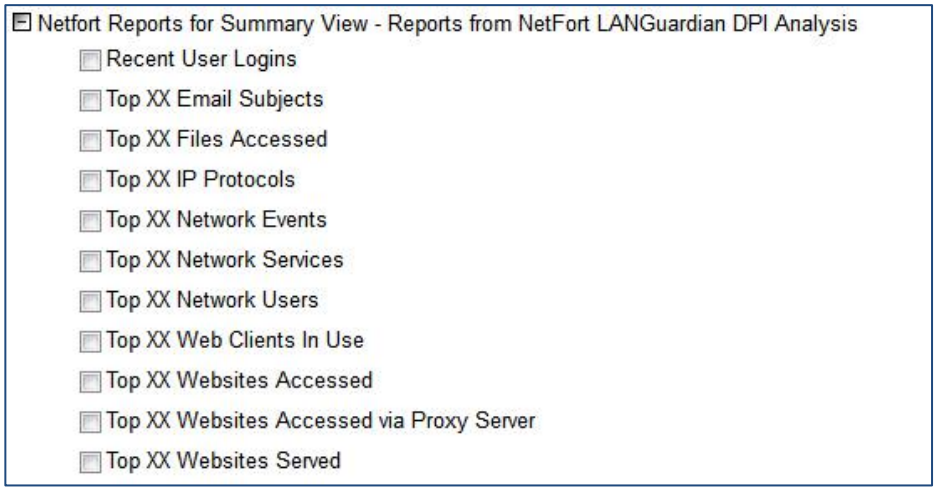
5. Click the + icon beside the **NetFort Reports** sections to expand the lists of available LANGuardian reports.

   On Node Details View pages, the available reports are:



Orion Node Details View pages contain reports and alerts that are relevant to a specific node, identified by IP address. When LANGuardian reports are embedded in these views, the system IP address is passed to LANGuardian to use as a report filter, so only information pertaining to this IP address is displayed. For example, if you are viewing the Node Details View page for web server 10.0.0.8, only websites served by this web server are listed in the websites served report, even though there may be other web servers on the network.

On Summary View pages, the available reports are:



Orion Summary View pages contain general purpose reports, maps, and alerts that do not pertain to any individual system or IP address. LANGuardian reports embedded in these views do not use any report filters.

On Interface Details View pages, the available report is:

Orion Interface Details View pages contain reports and alerts that are relevant to a specific network interface. LANGuardian provides a single report for this view. The report, called Switch Interface Drilldown, is designed to operate on layer 2 and layer 3 interfaces on network switches. The report queries the switch to determine which systems are communicating over the interface. It then matches this data with the LANGuardian traffic analysis database to determine which systems are using the most bandwidth on the interface, and what the network traffic consists of, for example, web traffic, fileshare traffic, and so on.

6. Enable the checkbox next to each report you want to include, then click the **Submit** button.
7. Click **Done** to finish customizing the page. The LANGuardian reports will be displayed when the page refreshes.

Note

When you add LANGuardian reports as Orion resources in your Orion views, be careful to ensure that the reports match the page type. For example, you should only add Summary View reports to a Summary View page. If you add a report to the wrong page type, the Orion resource for the report will display an error message as shown in the example below:

4.3 Troubleshooting

If LANGuardian reports fail to display in Orion views, the tips in this section might help you to resolve the problem. If you need further assistance, please contact support@netfort.com.

4.3.1 Ensure LANGuardian is running

If you cannot see LANGuardian data in Orion, the first thing to check is that your LANGuardian system is running correctly. Go to the LANGuardian home page and log in using the account and password you specified when you installed the Orion integration pack. If you can log in successfully and see report data, then the problem is likely to be with your Orion configuration settings and not LANGuardian.

4.3.2 Permission errors when extracting or copying integration pack files

If you get "permission denied" errors when copying files to the installation folder or extracting them with an application such as WinZip, make sure you have write access to the folder.

Also, make sure you are logged in to the Administrator account on the Windows server where Orion is installed.

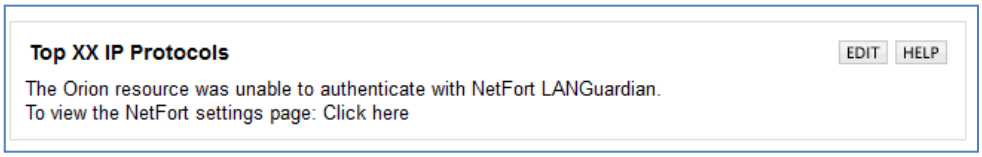
4.3.3 Report returns no data

If a LANGuardian report does not return any data, it might simply be a case of there being no data available that matches the report criteria.

The screenshot below shows a correctly returned report that contains no data.

You can verify this by viewing the same report directly in LANGuardian. If the report returns no data and you suspect it should, check the sensor configuration in LANGuardian to make sure the correct data is being captured.

4.3.4 Report displays "unable to authenticate" message



This message is displayed if Orion is unable to authenticate itself with the LANGuardian system. The most likely cause is incorrectly entered credentials.

Click on the **Click here** link in the error message to go to the **NetFort LANGuardian Settings** page. Re-enter the username and password to make sure they are correct.

4.3.5 Report displays "data might be incorrect" message

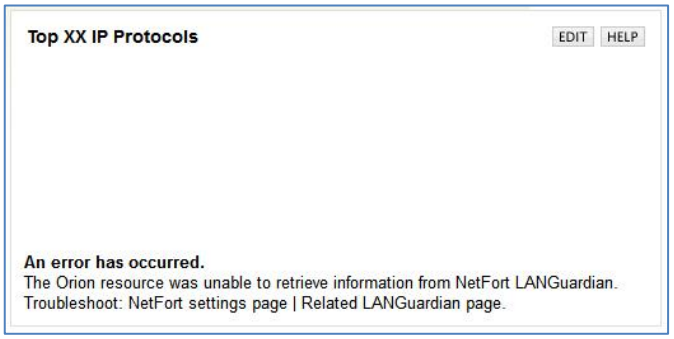
This message is displayed when you add a NetFort report to the wrong type of page.

LANGuardian reports are divided into three categories that correspond to the views available in Orion, as follows:

- Interface Details View
- Node Details View
- Summary View

You should place reports from each category only on the page type for that categor. For example, you should not place a report from the Node Details category on a Summary page. If you see this error message, delete the report from the page.

4.3.6 Report displays "an error has occurred" message



This message is displayed when Orion fails to receive a valid response from the LANGuardian system after 30 seconds (default timeout value). The error message displays two troubleshooting links to help you track down the problem. The possible causes of this error are shown in the table below.

Possible cause	Possible solutions
The IP address for the LANGuardian system is incorrect.	Click on the **NetFort settings page** link in the error message window. This link takes you to the **NetFort LANGuardian Settings** page, which is the Orion page where you specify the address and credentials for the LANGuardian system. On this page, verify that you have entered the correct IP address for the LANGuardian system. Click on the **Related LANGuardian page** link in the error message window. This link takes you to the LANGuardian page for the report that Orion is unable to display. This will help you to identify the cause of the error. If you can see the report in LANGuardian but not in Orion, it means there is a problem with how Orion connects to LANGuardian. If you cannot see the report in LANGuardian, make sure the LANGuardian system is running and that it is capturing data correctly.
It takes longer to execute the report on LANGuardian than the timeout value specified in the LANGuardian settings page. The default timeout value is 30 seconds. For example, if it takes 60	Click on the **NetFort settings page** link in the error message window. This link takes you to the NetFort LANGuardian Settings page. Increase the **LANGuardian Timeout** value. For example, you could set the value to 250 seconds. However, do not set this value higher than the Orion view refresh interval.

seconds to run a report, you will see the above error after 30 seconds.	
This problem might occur if it takes longer for the LANGuardian report to run than the Orion view refresh rate. In this case, the refresh of the Orion view restarts the report continuously.	To resolve this issue, try increasing the interval between automatic refreshes of the view. For more information, refer to the section "Orion Web Console and Chart Settings" in the Orion NPM Administrator Guide, available here: http://tinyurl.com/OrionNPMguide

4.3.7 Report displays "this connection is untrusted" message

The LANGuardian REST API is accessed via https and presents an X.509 certificate. By default, this is a self-signed certificate that is generated when the system was installed. Because of this, your web browser will not recognise the certifcate and will assert a security exception, such as shown below for Firefox 5.

You will see similar errors in other browsers.

The easiest way to resolve this issue is to open the home page of your LANGuardian installation and take the option to accept the untrusted certificate. This will add the certificate to the certificate store on your browser and prevent this error from occurring.

Note

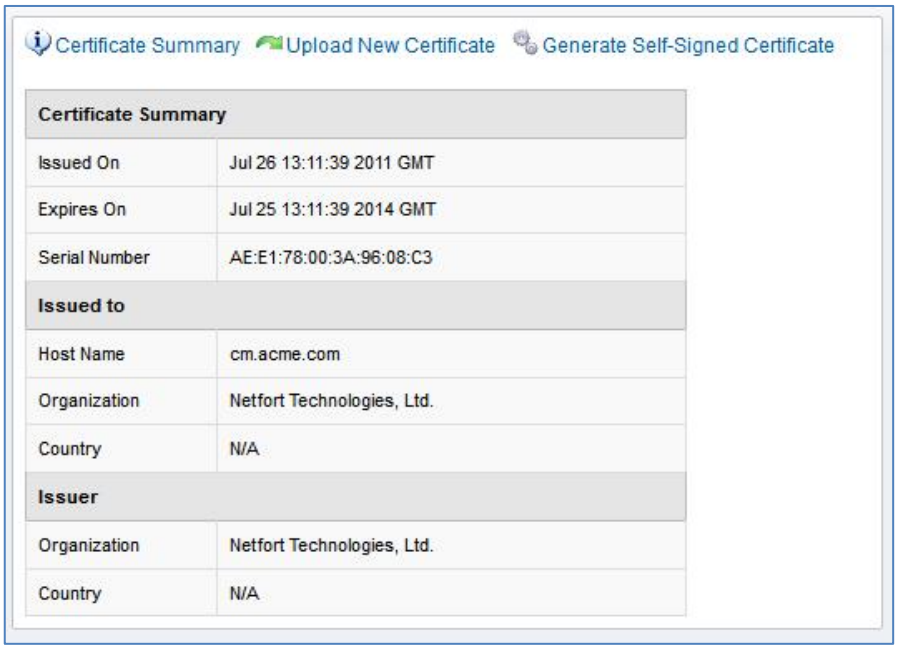
Some LANGuardian customers access the system using a hostname (for example, http://languardian.local) instead of an IP address. If you access the main LANGuardian this way, make sure to specify the hostname in the **NetFort LANGuardian Settings** page in Orion, and specify the hostname when visit the LANGuardian home page to trust the certificate.

You can also resolve this issue by manually adding the untrusted certificate to the certificate store on your web browser. The steps for doing this are browser-specific. For details, see the following links:

Chrome	http://www.google.com/support/chrome/bin/answer.py?answer=98884
Firefox	http://support.mozilla.com/en-US/kb/This%20connection%20is%20untrusted
Internet Explorer	http://windows.microsoft.com/en-US/windows-vista/About-certificate-errors
Safari	http://docs.info.apple.com/article.html?path=Safari/5.0/en/22093.html

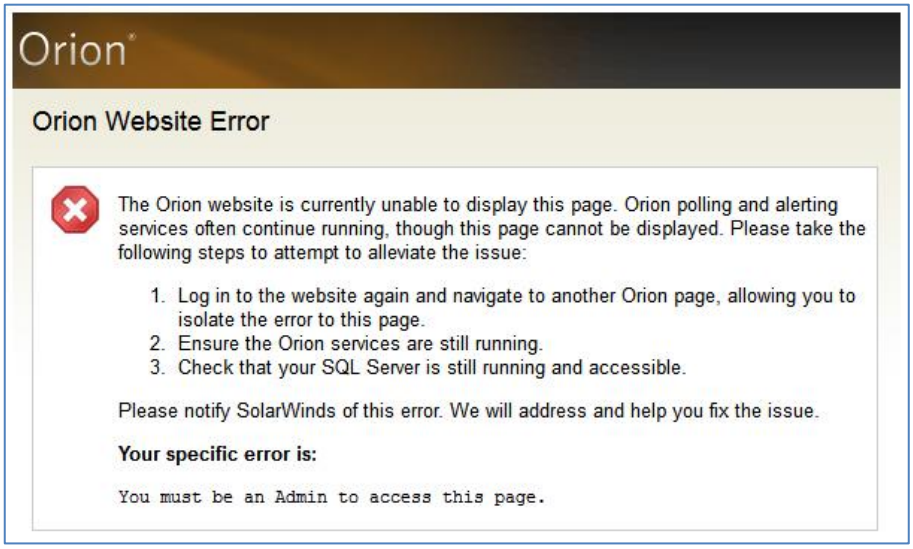
Alternatively, you can upload a signed certificate to LANGuardian, as follows:

1. Log on to the LANGuardian home page.
2. Click the **Configuration** link in the **Administration** section.
3. On the **Configuration** page, scroll down to the **System** section.
4. Click **Change the SSL certificate used by the web server.**
5. On the SSL Certificate Management page, click **Upload New Certificate** or **Generate Self-Signed Certificate** and follow the on-screen instructions.



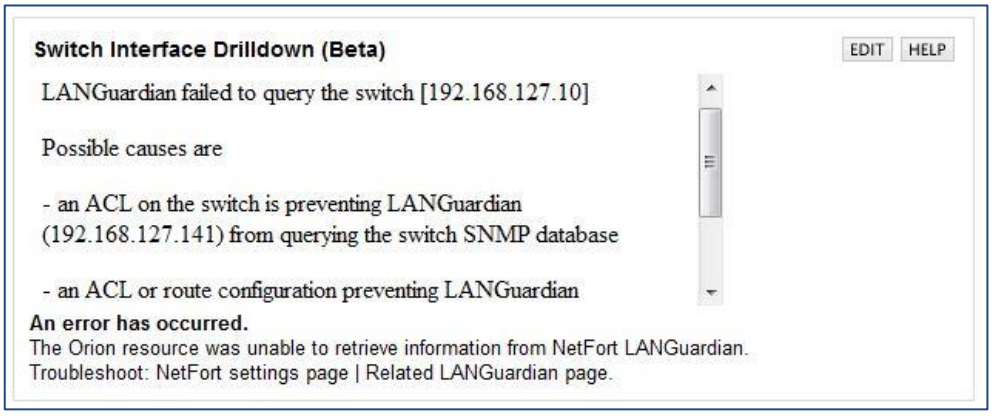
4.3.8 Orion displays "Orion Website Error" message

This message is displayed when you try to access the **NetFort LANGuardian Settings** page in your Orion implementation while logged in to Orion with an account that does not have administrator rights.



To customize Orion settings or pages, you must be logged in to Orion with administrator rights.

4.3.9 ACL problem (Switch Interface Drilldown Report only)



The possible causes of this problem are as follows:

- An ACL on the switch is preventing the LANGuardian IP address from querying the switch SNMP database.
- An ACL or route configuration is preventing the LANGuardian IP address from connecting to the switch.
- An incorrect community string has been specified.

The error means that LANGuardian attempted to query the SNMP database of a switch, but failed to do so. To resolve the issue, add the LANGuardian IP address to the ACL for the switch.

It is also possible that Orion provided an incorrect SNMP public string to LANGuardian. However, this is unlikely to happen.

4.3.10 Other problems

If you encounter other problems integrating LANGuardian with Orion, please contact NetFort Support using the email address support@netfort.com.

4.4 Advanced integration

When you install the integration pack, it makes the most commonly used LANGuardian reports available in Orion. If you want to display other LANGuardian built-in or custom reports in Orion, you can manually add them.

4.4.1 How it works

LANGuardian includes a SolarWinds menu item on each report page, which allows you to generate HTML code that you can include in the Orion Custom HTML resource you have created for that report.

The LANGuardian HTML code embedded in the Orion view uses JavaScript Object Notation (JSON) to continuously fetch data from the LANGuardian database and keep the Orion Custom HTML resource updated.

From a technical point of view, integration between LANGuardian and Orion is made possible by the LANGuardian REST API.

4.4.2 LANGuardian REST API

REST (representational state transfer) is a software design architecture that is used in the implementation of client-server applications. Applications based on REST use the HTTP protocol to create, read, and update data over the network.

A REST API (application programming interface) is a set of definitions that specify the parameters that can be used by clients in the HTTP operations they use when interacting with a server.

LANGuardian includes a REST API that you can use to incorporate traffic data from the LANGuardian database into other applications and formats, including:

- SolarWinds Orion
- Microsoft Excel (using the Get Data From Web command in Excel 2007 and higher versions)
- Comma-separated values (CSV), the *de facto* standard for incorporating data files into databases and spreadsheet applications
- HTML IFRAME content that you can include in any web page

Only SolarWinds Orion integration is covered in this guide. Please contact NetFort Support for information about other uses of the LANGuardian REST API.

4.4.3 Displaying LANGuardian reports in the Orion view

You can configure views in Orion that consist of a mixture of Orion and LANGuardian reports.

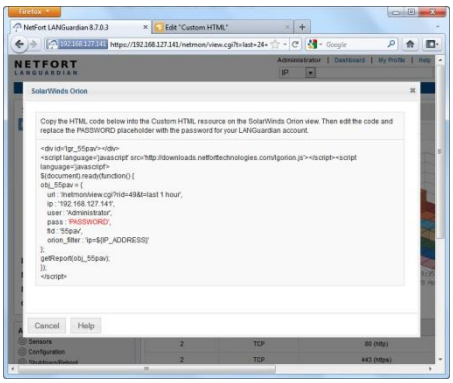
For example, the Orion Node Details page typically provides details of system status parameters such as memory use and packet loss for a given node on the network. By adding LANGuardian reports to the page, you can see additional information such as websites visited, files accessed, and bandwidth used.

4.4.3.1 Preparation

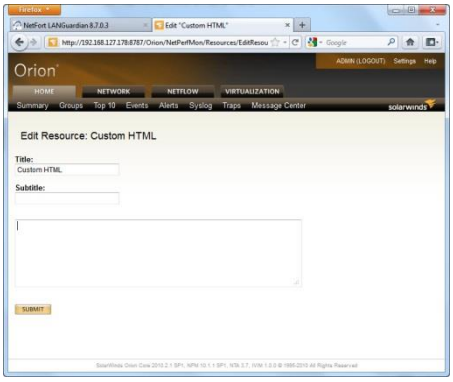
To prepare for adding your LANGuardian report to a SolarWinds view, we recommend you open two browser tabs (or windows).

Open the LANGuardian home page in one tab and open the Orion home page in the other tab.

Follow the LANGuardian-related instructions in the LANGuardian tab and follow the Orion-related instructions in the Orion tab. Then, when it is time to paste the LANGuardian HTML code into Orion, you will be able **Select** and **Copy** in the LANGuardian tab, then switch to the Orion tab and click **Paste**.



❶ LANGuardian tab: Copy



❷ Orion tab: Paste

4.4.3.2 Generating the HTML code in LANGuardian

Follow these steps to generate the HTML code that will enable you to incorporate a LANGuardian report into an Orion view:

1. In the LANGuardian user interface, browse to the report you want to include.

   For example, to include the **Traffic Distribution** report:

   a. Click on the **Bandwidth** menu and then click on **IP**.

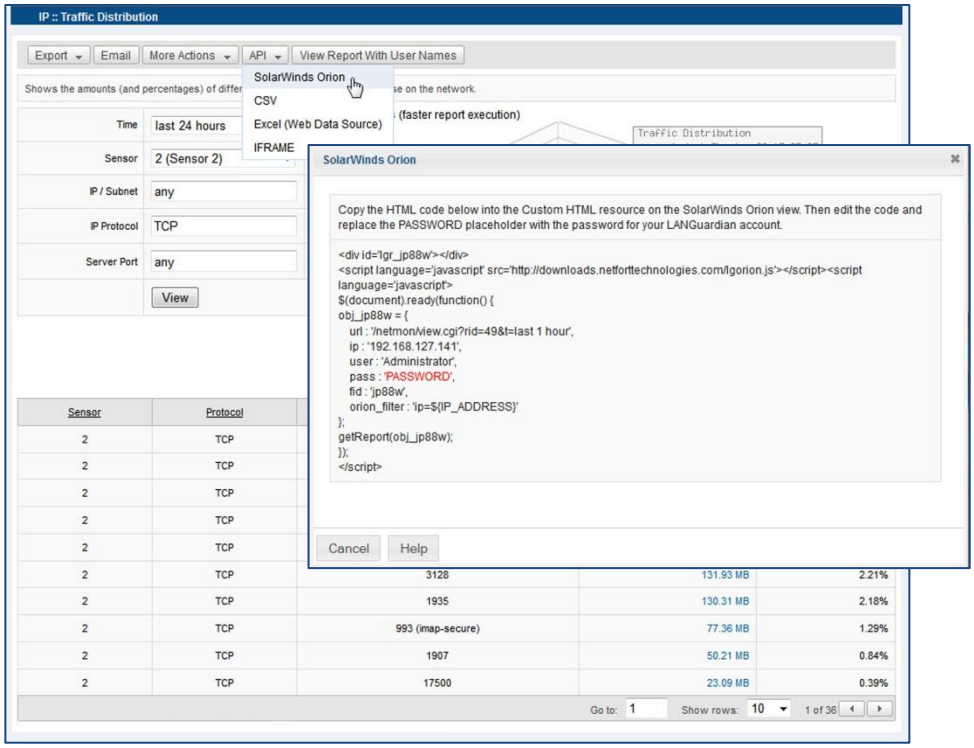
b. On the **IP** menu, click **Traffic Distribution**.

c. When LANGuardian displays the report, customize it according to your requirements by specifying parameters in the **Time, Sensor, IP/Subnet, IP Protocol,** and **Server Port** fields.

d. Click **View** to display the report.

2. When the report is displayed, click the **API** menu button and select **SolarWinds** from the drop-down list.

   LANGuardian will display a pop-up window containing the HTML code that you must paste into the Orion Custom HTML Resource when you create it.

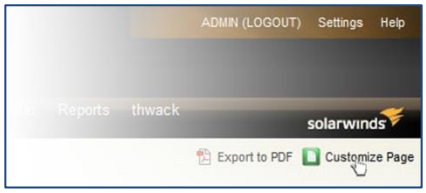


4.4.3.3 Creating the Custom HTML resource in Orion

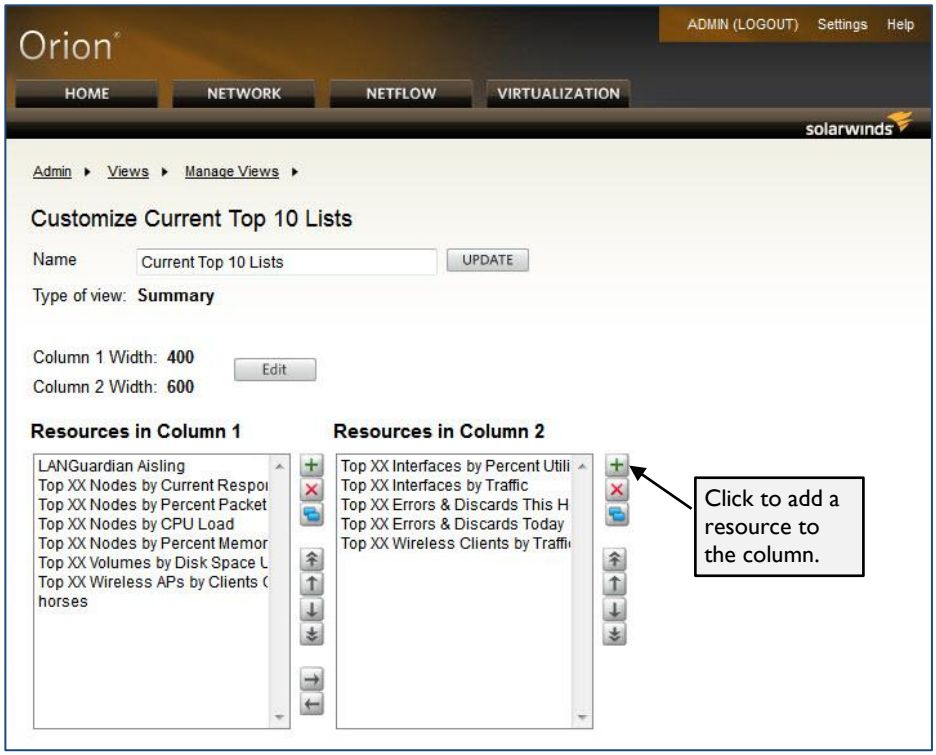
Follow these steps to create the Orion HTML Resource into which you will paste the report HTML code you generated with LANGuardian:

1. In the Orion user interface, browse to the page where you want the LANGuardian information to be displayed. For example, to add the report to the Orion Top 10 page, click **Home** on the Orion main menu, then click **Top 10**.

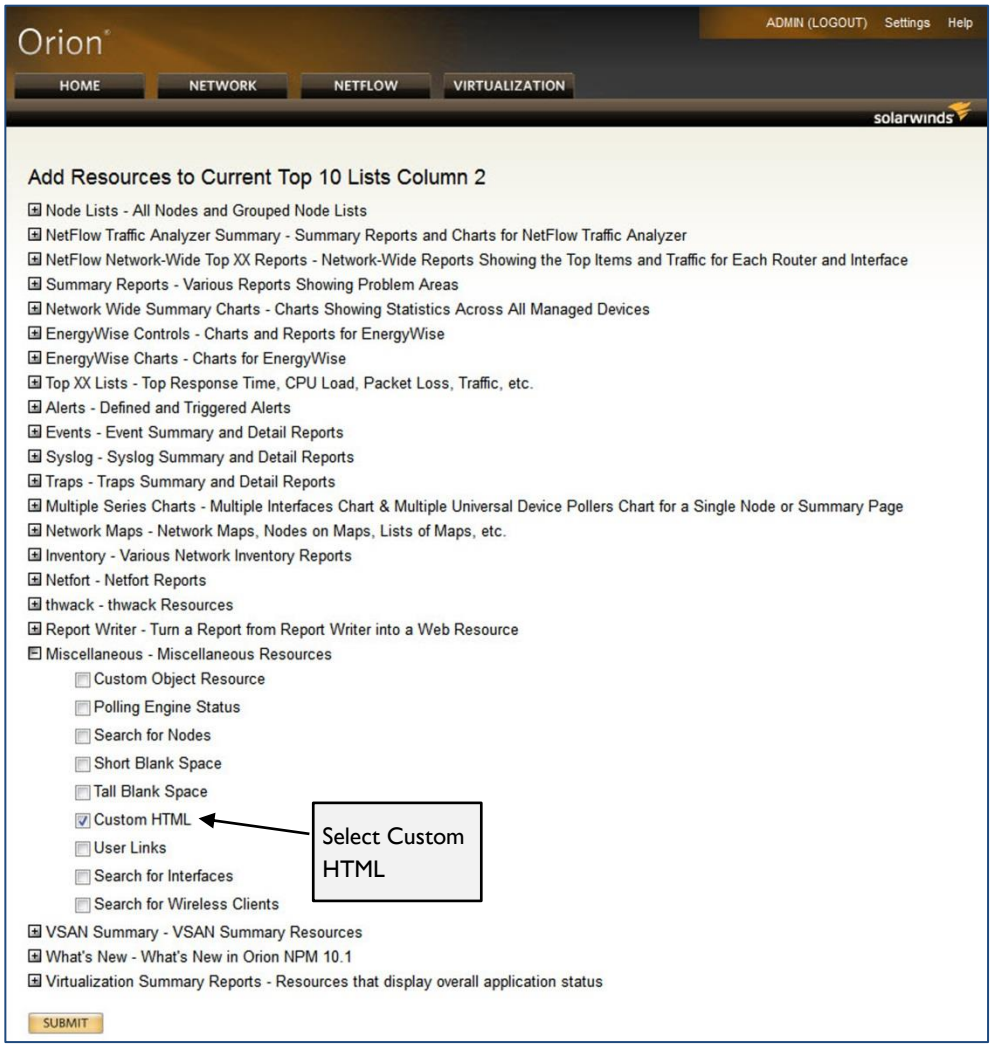
2. Click **Customize Page**.



3. Select the column to which you want to add the LANGuardian report and click the  icon to add a resource to the column.

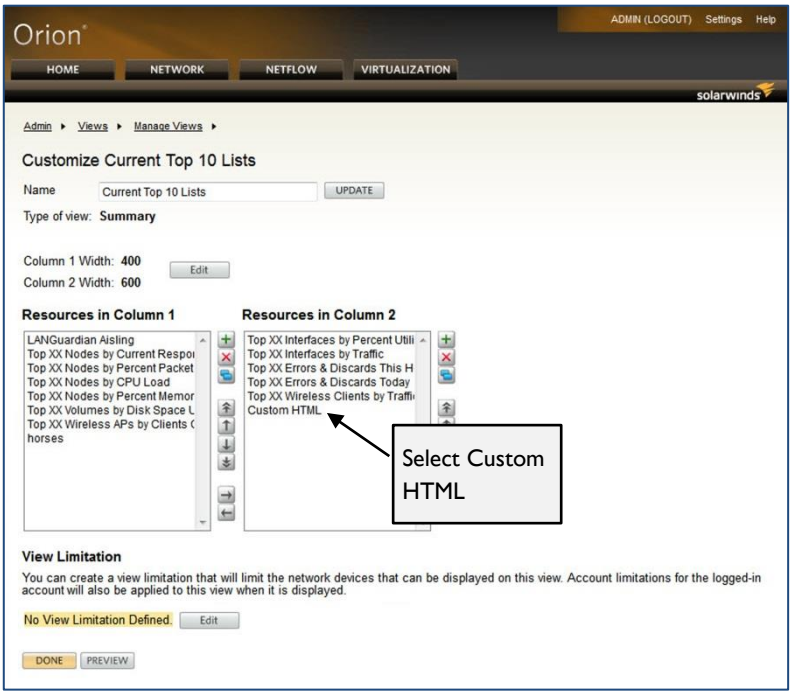


4. Orion displays the **Add Resources to Column** page. Scroll down to the **Miscellaneous – Miscellaneous Resources** section and expand it.



5. Enable the **Custom HTML** checkbox and click **Submit**.

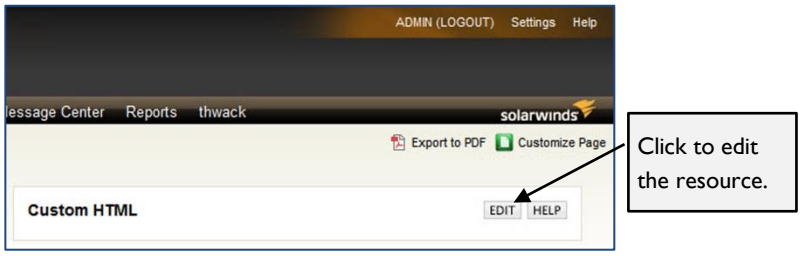
   Orion will return to the customization page and you will see the new Custom HTML resource included in the column to which you added it.



You can change the location of the Custom HTML resource on the page by using the arrow buttons to the right of the column.

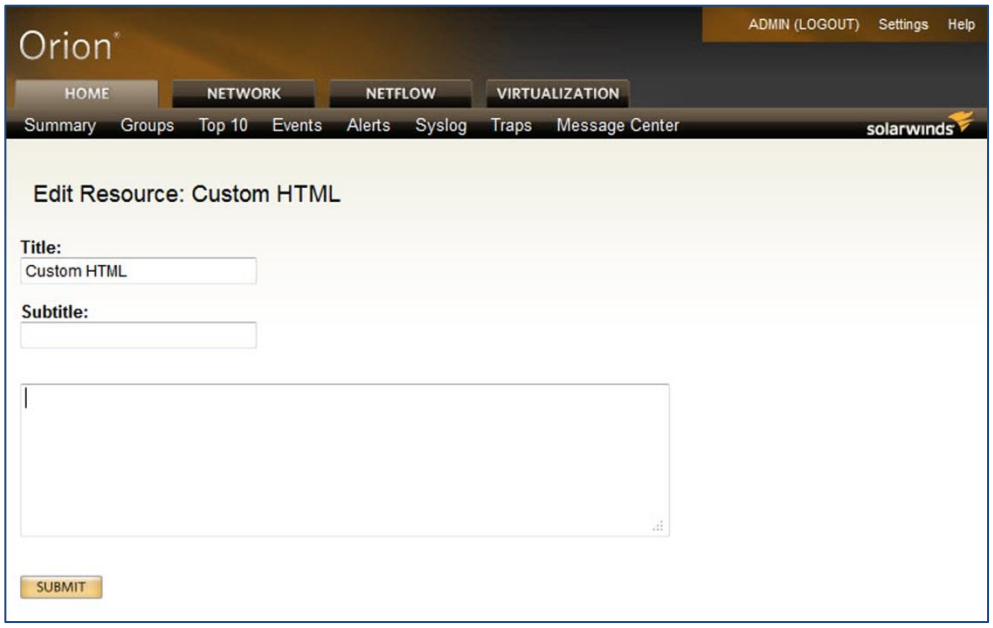
Click the **Done** button to return to the Orion page.

6. Locate the newly added Custom HTML resource on the Orion page. You may need to scroll down the page to bring the new resource into view.



7. Click the **Edit** button to edit the Custom HTML resource.

   Orion will display the **Edit Resource** page.



Modify the **Title** field to reflect the title of the LANGuardian report you will display in the resource.

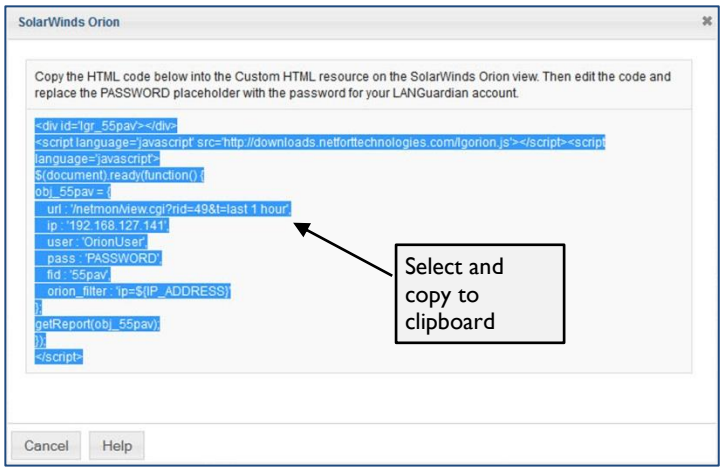
You are now ready to paste the LANGuardian code into the Custom HTML resource.

4.4.3.4 Adding LANGuardian HTML code to the Orion resource

Follow these steps to add the LANGuardian HTML code to the Orion resource:

1. In the LANGuardian browser tab:

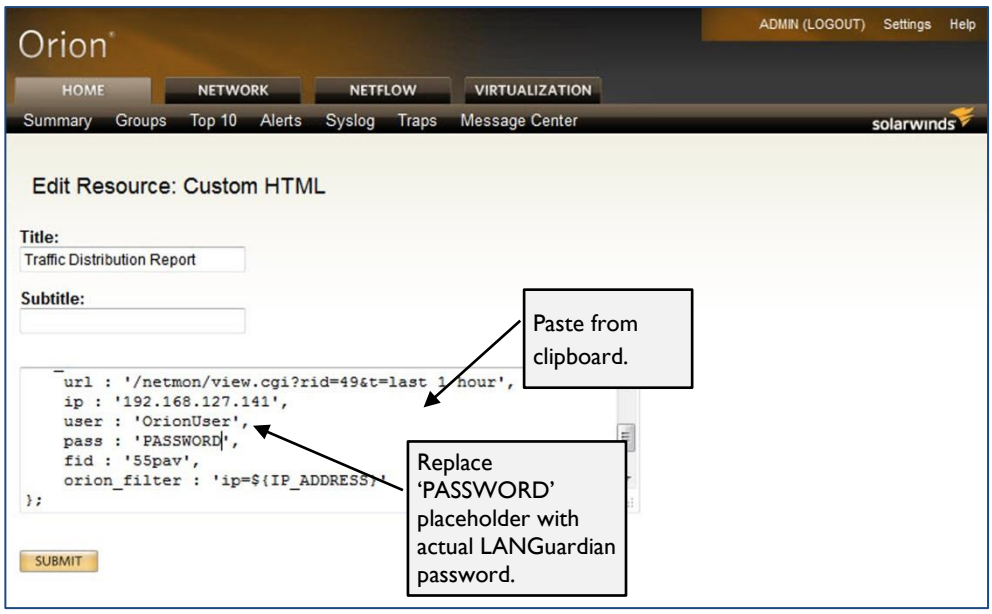
   Select the HTML code in the pop-up window and copy it to the clipboard (press Ctrl-C or right-click and select Copy from the pop-up menu).



2. In the Orion browser tab:

   Position the cursor in the empty text box on the **Edit Resource** page. Press Ctrl-V or right-click and select Paste from the pop-up menu.

3. The HTML code you paste into the Orion window contains a placeholder instead of the password for the account that Orion will use to access LANGuardian data.



4. Edit the 'PASSWORD' placeholder and replace it with the actual LANGuardian account password.
5. Click **Submit** to save your changes.

Appendix A

Appendix A - Report reference

This appendix lists the reports that are available when you first install LANGuardian.

Security reports

Security reports are divided into three categories: Events, Netscan, and Behavior.

Basic security reports

Events	Netscan	Behavior
by Signature	by Port	Net Exporters of Data
by IP	by Source	
by User	Port 445, 139	

Advanced security reports

Events	Netscan	Behavior
by Category	Netscans by IP	
by Destination	Netscans by user	
by Source		
Systems accessing websites associated with malware		
Systems connecting to Conficker-associated malware websites		
Systems generating a level of brute-force logins normally associated with Conficker		

Low-level security event reports

events (all) by Category	event list (Conficker)	events (all) by IP	events (all) by User
events (dns_mx_lookups, possible SPAM)	events (Conficker Worm Brute Force Logins, drilldown)	events (DNS lookup) by IP	events (DNS lookup) by User
events (emails)	events (ids) by IP	events (ids) by User	events (info_hash) by IP
events (info_hash) by User	events (mac)	events (report alert)	events (Signature Breakdown) by User
events (trend)	events (volume overflows) by IP	events (volume overflows) by User	Spyware Http Requests by IP
Spyware HTTP Requests by User	User Events		

Bandwidth reports

Bandwidth reports are divided into two categories: IP and Ethernet.

Basic bandwidth reports

IP	Ethernet
Traffic Distribution	Traffic Distribution
Top Talkers	Top Talkers
Top Clients	
Top Servers	
Top Users	
Top Departments	

Advanced bandwidth reports

IP	Ethernet
Top Packet Generators	Top Broadcasters
TOS Distribution	
Traffic Distribution::TCP	

Low-level Bandwidth Reports – IP

Flows by IP	Flows by User	Flows with RTT	Flows (Packets sent/received)
Sessions by IP	Sessions by User	Sessions (In) by IP	Sessions (In) by User

Sessions (In/Out)	Traffic (In/Out)	Traffic Distribution by User	Traffic In (Top Receivers)
Traffic In (Top Senders)	Traffic In (Top Users)	Traffic Out (Top Receivers)	Traffic Out (Top Senders)
Traffic Out (Top Users)			

Low-level Bandwidth Reports – Ethernet

Flows by IP	Flows by User	Sessions	

Policy reports

Policy reports are divided into two categories: P2P Signatures and Skype Activity.

P2P Signatures	Skype Activity
P2P Signature Report	Activity by IP
	Activity by User
	Social Networking HTTP Requests

Network inventory reports

Network inventory reports are divided into two categories: Network Services and Operating Systems.

Basic network inventory reports

Network services	Operating systems
Network services	Operating systems
Network services by IP	Operating systems by IP
DHCP servers	
MAC addresses	
Resolve hostname to IP	

Modules

Use the Modules menu to access LANGuardian modules. The following modules are available:

Basic module reports

Trends	Web	Windows File Shares
View Trends	By User	Search by User
	Top Websites	Search by Filename
	Top Proxy Clients	
Identity	**Service Inspector**	**E-mail**
Directory Logins	Current Status	By Subject
		By Sender
		By User
		Yahoo::Outbound file
		Attachments
Web Browsers	**SQL Server**	**Bandwidth Quota**
Web Clients	Top Database	Status Summary
		Status by Group

Advanced module reports

Trends	Web	Windows File Shares
	Departments with the most Web Activity	Access databases
	Top Proxy Servers	Deleted Office documents
	Top Proxy Users	Executable files
	Top Websites & URI	Microsoft Office files
	Website accesses broken down by category	Music files
	Website accesses broken down by category (with RTT)	PDF files
		Video files
		Most active clients
		Most active servers
		Deleted folders
		Finance folders
		HR
		Legal folders
		User folder activity
		Show directories that have been deleted

		Data totals
		Most active users
		MS Office files
		Music file sharing
Identity	**Service Inspector**	**E-mail**
Directory Logins by IP	Hosts Down	By Source IP
Web Browsers	SQL Server	Bandwidth Quota
Mobile devices connected to the network	Compliance :: Automatic Database Discovery	Events (user policy)
Systems connecting to Microsoft SMS Server	Compliance :: Data Modification	Status
Systems not running Windows Update	Compliance :: Privileged DB Users	
Systems running Linux	Compliance :: Schema Modification	
Systems running MacOS X	Compliance :: Statement Audit Log	
Systems running multiple web clients	Top Active Directory User	
Systems running Windows 2000/2003	Top MS SQL Client by Number of Queries	
Systems running Windows 7	Top MS SQL Clients by Data Volume	
Systems running Windows Update	Top MS SQL Servers by Data Volume	
Systems running Windows XP	Top MS-SQL Application	
	Top Statement	
	Top Statement Type	
	Top Username	

Appendix B

Appendix B - Port and protocol reference

This table shows...

TCP Port	Name	Description
7	echo	Echo
9	discard	Discard
13	daytime	Daytime
17	qotd	Quote of the day
19	chargen	Character generator
20	ftp-data	File transfer
21	ftp	FTP control
23	telnet	Telnet
25	smtp	Simple mail transfer
37	time	Time
42	nameserver	Host name server
43	nicname	Whois
53	domain	Domain name server
70	gopher	Gopher
79	finger	Finger
80	http	World wide web
88	kerberos	Kerberos
101	hostname	NIC host name server
102	iso-tsap	ISO-TSAP Class 0
107	rtelnet	Remote telnet service
109	pop2	Post office protocol – Version 2
110	pop3	Post office protocol – Version 3
111	sunrpc	Sun remote procedure call

113	auth	Authentication service
117	uucp-path	UUCP path service
119	nntp	Network news transfer protocol
135	epmap	DCE endpoint resolution
137	netbios-ns	NETBIOS name service
139	netbios-ssn	NETBIOS session service
143	imap	Internet message access protocol
158	pcmail-srv	PC mail server
170	print-srv	Network PostScript
179	bgp	Border gateway protocol
194	irc	Internet relay chat protocol
389	ldap	Lightweight directory access protocol
443	https	Secure HTTP
445	cifs	Microsoft CIFS
464	kpasswd	Kerberos (v5)
512	exec	Remote process execution
513	login	Remote login
514	cmd	Automatic authentication
515	printer	Listens for incoming connections
520	efs	Extended file name server
526	tempo	Newdate
530	courier	RPC
531	conference	IRC chat
532	netnews	Readnews
540	uucp	Uucpd
543	klogin	Kerberos login
544	kshell	Kerberos remote shell
556	remotefs	RFS server
636	ldaps	LDAP over TLS/SSL
749	Kerberos-adm	Kerberos administration
1109	kpop	Kerberos POP
1433	ms-sql-s	Microsoft-SQL Server
1434	ms-sql-m	Microsoft-SQL Monitor
1512	wins	Microsoft Windows internet name service
1524	ingreslock	Ingres
1723	pptp	Point-to-point tunneling protocol

2053	knetd	Kerberos de-multiplexer
9535	man	Remote man server

This table shows…

TCP Port	Name	Description
7	echo	Echo
9	discard	Discard
13	daytime	Daytime
17	qotd	Quote of the day
19	chargen	Character generator
37	time	Time
39	rlp	Resource location protocol
42	nameserver	Host name server
53	domain	Domain name server
67	bootps	Bootstrap protocol server
68	bootpc	Bootstrap protocol client
69	tftp	Trivial file transfer
88	kerberos	Kerberos
111	sunrpc	Sun remote procedure call
123	ntp	Network time protocol
135	epmap	DCE endpoint resolution
137	netbios-ns	NETBIOS name service
138	netbios-dgm	NETBIOS datagram service
161	snmp	SNMP
162	snmptrap	SNMP trap
213	ipx	IPX over IP
443	https	Secure HTTP
445	cifs	Microsoft CIFS
464	kpasswd	Kerberos (v5)
500	isakmp	Internet key exchange (IPSec)
512	biff	Notifies users of new mail
513	who	Database of who is logged on (average load)
514	syslog	0
517	talk	Establishes TCP connection
518	ntalk	0

520	router	RIPv.1, RIPv.2
525	timed	Timeserver
530	courier	RPC
533	netwall	For emergency broadcasts
550	new-rwho	New-who
560	rmonitor	Rmonitor
561	monitor	0
749	kerberos-adm	Kerberos administration
1167	phone	Conference-calling
1433	ms-sql-s	Microsoft-SQ Server
1434	ms-sql-m	Microsoft-SQL Monitor
1512	wins	Microsoft Windows internet name service
1701	l2tp	Layer Two tunneling protocol
1812	radiusauth	Radius authentication protocol (RRAS)
1813	radacct	Radius accounting protocol (RRAS)
2049	nfsd	Sun NFS server
2504	nlbs	Network load balancing

Appendix C

Appendix C - Glossary of terms

Flow

Cisco defines a **flow** as a unidirectional sequence of packets that share the following pieces of information:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Protocol

This is called the *5-tuple (quintuple) traffic definition*. LANGuardian can use flow information to produce reports that can be used for network monitoring, traffic analysis, and billing.

Index