



Installing the LANGuardian ISO image

24 April 2012

This document describes how to install LANGuardian using the ISO image that is available for download from the NetFort website:

www.netfort.com/software-download

Warning! NetFort LANGuardian does not require a host operating system. You deploy it as a bare-metal install onto dedicated hardware or into a virtualized environment. 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.

Before you begin

During the installation, you will configure LANGuardian to join your network. You must use a fixed IP address. Please make sure you have obtained a valid address and subnet mask, and know the address of the default gateway, before starting the installation.

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

1. First, you 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.
2. Then, you configure a monitoring (SPAN) port on your core switch and connect the LANGuardian machine to this port.
3. Finally, you 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.

LANGuardian runs on industry-standard hardware. The system on which you install it should be similar to, or more powerful than, a dual-core processor with 2 GB RAM. If you are installing LANGuardian in a virtualized hardware environment, the equivalent resources should be available. Please contact us if you have any questions about hardware specifications.

LANGuardian requires at least two network adapters: one for the management (user) 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. You should have to hand the usual information needed to join a network:

- IP address
- Subnet mask
- Gateway address

The network adapter for the monitoring interface connects to a monitoring (SPAN) port on your core switch.

Installing the software

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).
4. Complete the LANGuardian setup process.

The LANGuardian Setup utility runs when you boot the LANGuardian CD. There are seven steps. After you complete these steps, the LANGuardian machine will be available on your network. You can then access the Configuration Wizard with a web browser to complete the configuration process.

```
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.
```

Step 1: Select the installation disk

```
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:
```

The disk on which you install LANGuardian should have a capacity of at least 50 GB. You can install on smaller disks but performance and storage capacity will be affected.

Enter the disk ID number and press Enter to continue.

Step 2: Confirm the installation disk

```

LANGuardian Setup
-----

Step 2 of 6: Confirm the installation disk

You have chosen to install LANGuardian on this disk:

Disk ID   Description                                     Size
-----
2         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]?

```

When you install LANGuardian, any existing data on the installation disk will be erased. To avoid accidental loss of data, the setup utility asks you to confirm that you want to proceed with the installation.

Type YES to continue with the installation. If you type NO, the setup utility will exit without making any changes to the disk.

Step 3: Select a network device

```

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 computer:

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]:

```

The setup utility lists the network interface cards (NICs) it finds on the system. Choose the NIC you want to assign to the LANGuardian user interface. You can determine the number of each NIC by disconnecting all network cables and reconnecting them one at a time and pressing the R key.

Step 4: Configure the network device

```
LANGuardian Setup
-----

Step 4 of 6: Configure the user interface network device

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

NIC ID      Description                                     Status
-----
3           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. The setup utility asks you to confirm your settings once again before beginning the actual installation.

Step 5: Confirm settings

```
LANGuardian Setup
-----

Step 5 of 6: Confirm settings

LANGuardian Setup will now complete the installation using these settings:

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

NIC ID   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]?

Type YES to complete the installation. If you type NO, the setup utility will exit
without making any changes to your system.
```

Step 6: 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...
```

When the setup utility finishes the installation, remove the LANGuardian CD and restart the system.

After the system restarts, you can visit the URL shown in step 7 to access the Configuration Wizard and complete the installation. Before you do

that, you must configure a monitoring port on your core switch to enable LANGuardian to capture traffic data.

Configure a monitoring port

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 the architecture and network monitoring concepts pages.

The steps to configure a monitoring port are specific to each switch. The video on this page gives an overview of the steps involved. 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.

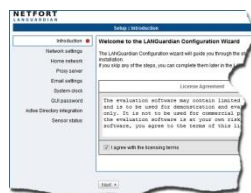
Using the Configuration Wizard

When the system reboots after you finish running the LANGuardian Setup Utility, the home page of the browser-based user interface is available at the IP address you specified during the installation. You must use the HTTPS protocol. 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 visit the home page after installation, LANGuardian will display the Configuration Wizard. Follow the steps to complete the installation. The steps are as follows:

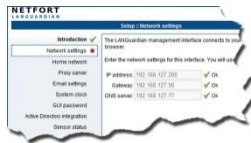
The steps are as follows:

I. Accept the license agreement



You must accept the license agreement to complete the configuration

2. Verify the network settings



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

3. Specify the Home network



In large networks, the Home network setting specifies the subnet in which the LANGuardian system is located. Do not change this setting unless you know what you are doing.

4. Specify a proxy server for LANGuardian updates



LANGuardian connects to the Internet to keep itself up to date by downloading updates from the NetFort Technologies website. If your network provides access to the Internet through a proxy server, enter the address and port number.

5. Specify the SMTP server to use for email



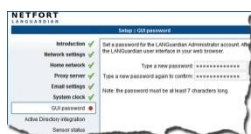
LANGuardian uses email to send scheduled reports to users and issue alerts when specified incidents occur or thresholds are breached. Enter the address of the SMTP server that LANGuardian uses to send email.

6. 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.

7. Set the GUI password



Set the password that you will use to the log on to the LANGuardian user interface.

8. Specify Active Directory details



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

9. Review sensor status



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

Click **Finish** to complete the configuration. LANGuardian will display the main dashboard page.

After you complete the wizard steps, LANGuardian will display the home page. It 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.

Integration with Active Directory

With the optional Identity module enabled, LANGuardian integrates with a Microsoft Windows environment to access additional information that it incorporates into reports, trends, and dashboards. The Identity 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, trends, 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.

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.

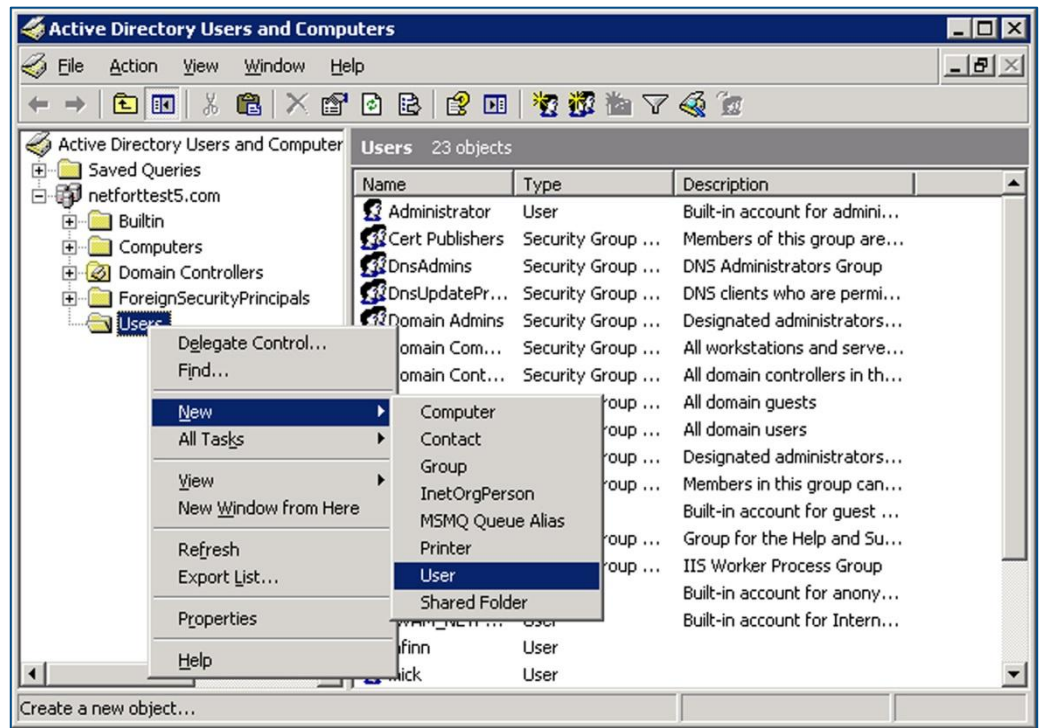
Configuring your Windows server

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.

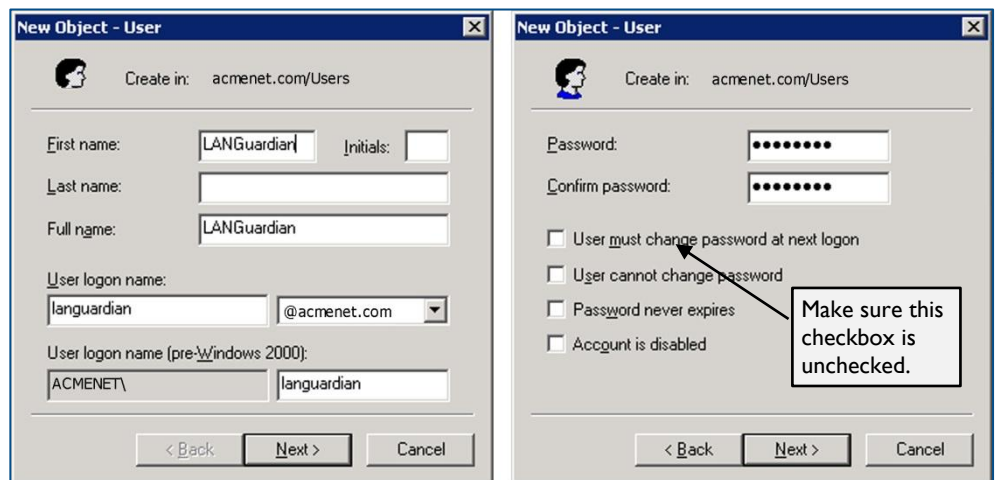
Create a LANGuardian account

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.



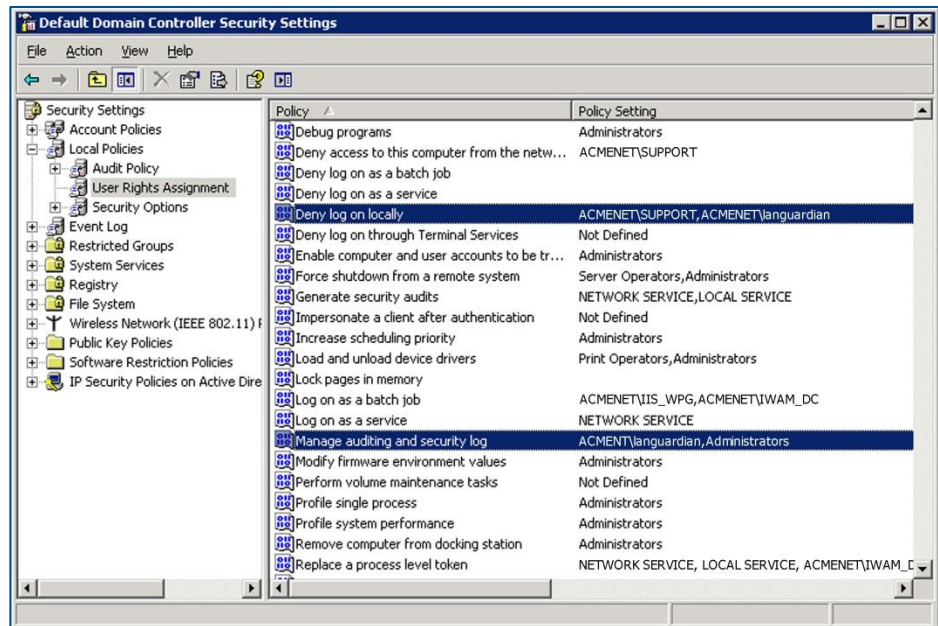
Make sure the **User must change password at next logon** checkbox is left unchecked.

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.



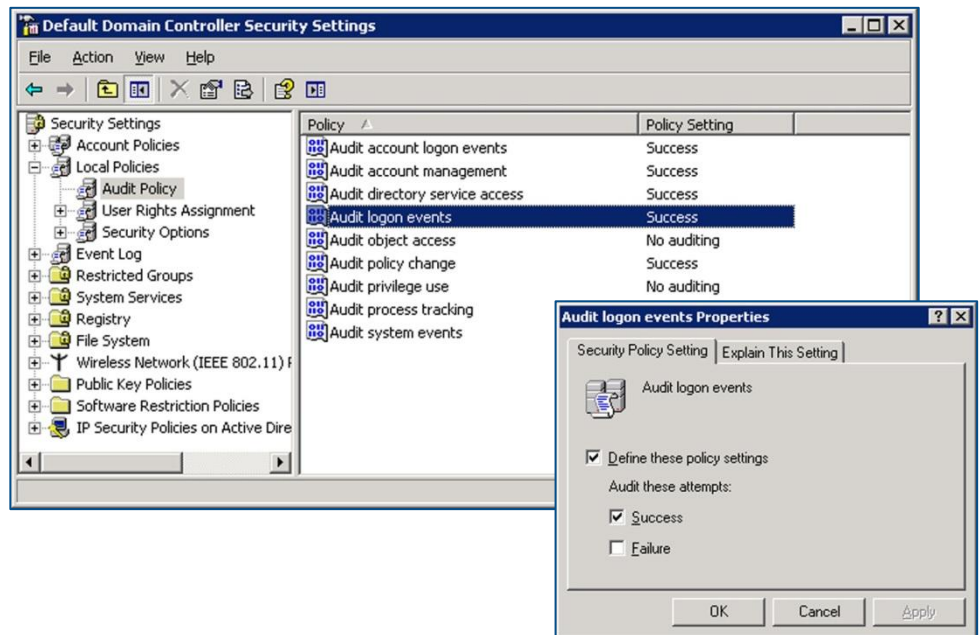
Configure event log auditing

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**.

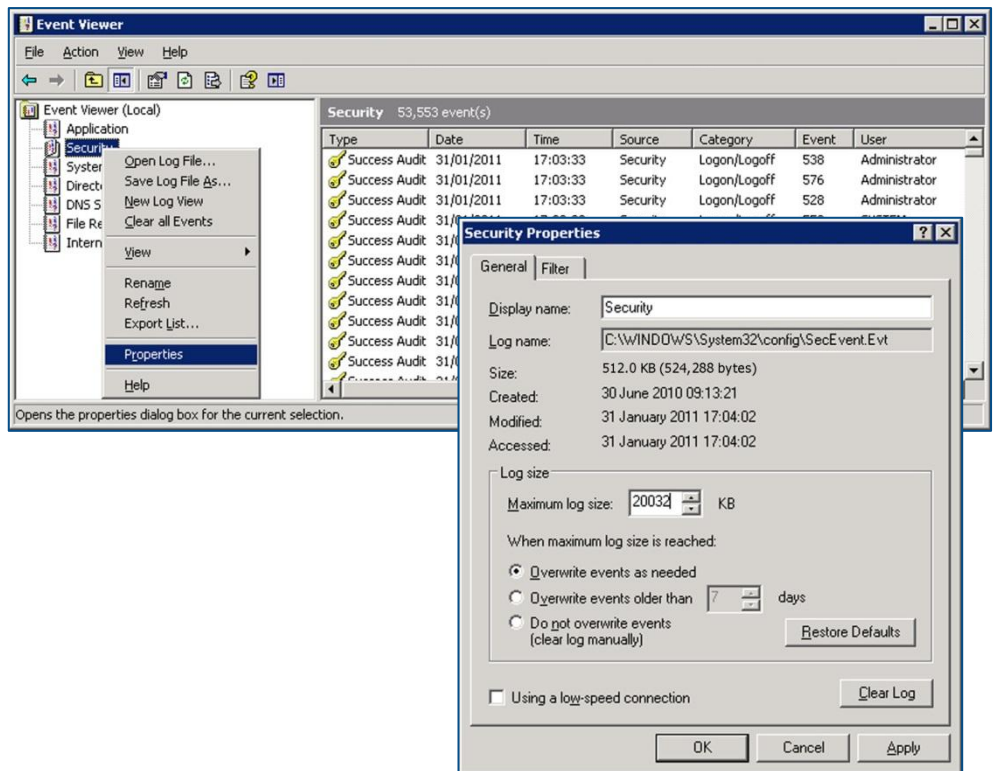


4. Check the **Success** checkbox to audit successful logon attempts in the event log.

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.

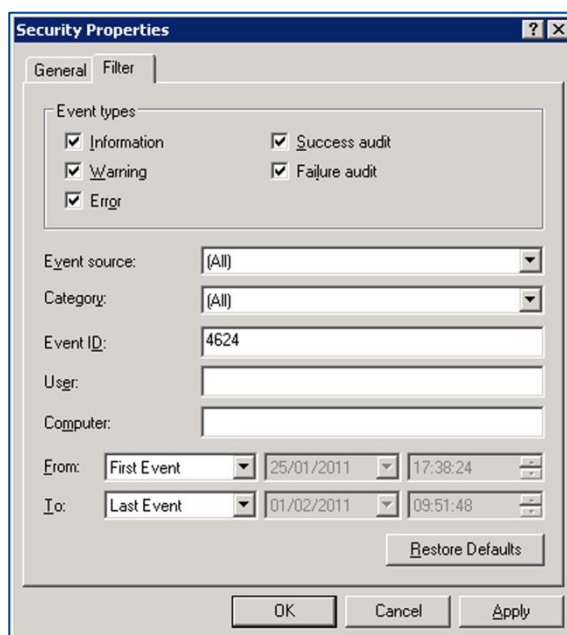
Follow these steps to set the maximum event log size:

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.

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.

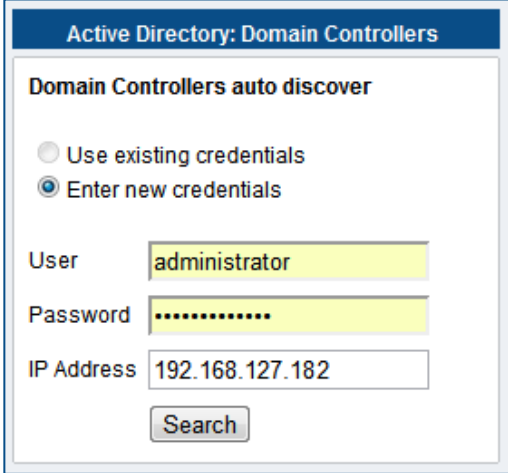
LANGuardian has an auto-discover facility that identifies every domain controller (DC) in a domain. To enumerate the DCs, it directs an LDAP query to a seed server, which returns a list of all DCs in the domain. LANGuardian then queries each DC to request its version.

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 **Configuration** on the **Administration** menu.
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.



Active Directory: Domain Controllers

Domain Controllers auto discover

Use existing credentials

Enter new credentials

User

Password

IP Address

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**.

Active Directory: Domain Controllers Search result

Domain Controllers auto discover

Use existing credentials
 Enter new credentials

User:

Password:

IP Address:

Search result.

Name	IP Address	User	Domain	Version	
DC-ACME-2	192.168.127.182	administrator	acme.com	2008R2	added

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

Active Directory: List of servers

Name	IP Address	User	Domain	Version	Status	Test	Edit	Delete
DC-ACME-1	192.168.127.181	administrator	acme.com	2008R2	✓	?	?	✗
DC-ACME-2	192.168.127.182	administrator	acme.com	2008R2	✓	?	?	✗

Update Directory information from AD Controllers (this may take some time)

Update Interval:

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.

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.

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 off of a client machine.

Need help?

Please contact us if you need help installing or configuring NetFort LANGuardian. You can avail of free no-obligation technical support by contacting our helpdesk on **support@netfort.com**. See also the NetFort discussion forum – <http://forum.netfort.com> – for technical tips and usage information.