



Installing the LANGuardian VMware appliance

01 February 2012

This document describes how to install the LANGuardian VMware appliance that is available for download from the NetFort website:

www.netfort.com/software-download

Note: The LANGuardian VMware appliance requires VMware ESX server 4.0. It is not suitable for installation on VMware ESXi or VMware ESX 3.5. However, you can still install LANGuardian in these environments using the ISO image.

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.

The virtualized version of LANGuardian is provided as a pre-configured VMware .OVA file that you can install with the VMware vSphere client.

The virtual appliance is pre-configured to use the following resources:

- One CPU
- 800 MB RAM
- 16 GB disk space

You can adjust these CPU and memory values after the LANGuardian installation has finished. If you need to capture large amounts of traffic, please install and configure LANGuardian using the ISO image because then you will be able to specify a suitable disk size.

Installation of the LANGuardian VMware appliance is a three-part process:

1. First, you deploy the virtual machine on your VMware ESX infrastructure.
2. Then, you configure LANGuardian for local ESX Server monitoring and external monitoring.
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.

Deploying the virtual machine

Follow these steps to deploy the LANGuardian image:

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 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 image and install it in the ESX server.

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

Initializing LANGuardian

Follow these steps to initialize your newly installed LANGuardian virtual machine.

1. Open the vSphere client, select your virtual machine and power it on.
2. Click the **Console** tab and wait for the virtual machine to boot. Verify that the virtual machine boots correctly.

3. The command-line interface main menu has options for basic administration of the virtual machine. The option that is relevant to initial configuration is **option 6** (Configure network device). Select option 6 from the list. Specify the IP address, subnet mask, and default gateway address.
4. Visit the home page 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 access the LANGuardian user interface, it will display 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.

Setting up local ESX Server monitoring

If you want to monitor internal traffic on an ESX Server virtual switch, you must allow promiscuous-mode connections to it. The steps are as follows:

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

LANGuardian will immediately begin monitoring all traffic flowing through the vSwitch.

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 on the **Edit Settings** tab.
2. Click on 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 **Sensors** on the **Administration** menu.
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.

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, and associate them with a physical adapter that will be connected 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 on 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 on **Finish**.

Follow these steps to create a new virtual adapter:

1. Open the settings for the LANGuardian appliance and click on 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 **Sensors** on the **Administration** menu.
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**.

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

1. Open the host settings for the ESX Server and click on the **Configuration** tab.
2. Click **Properties...** to view the properties for the virtual switch.
3. Edit the properties, then click on the **Security** tab.

4. Click **Accept** from the **Promiscuous Mode** drop-down list, then click on **OK**.

Configure 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 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.

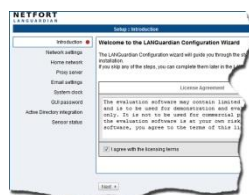
Using the Configuration Wizard

When your LANGuardian VMware appliance starts, 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:

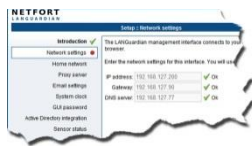
The steps are as follows:

- I. Accept the license agreement



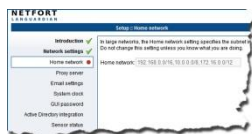
You must accept the license agreement to complete the configuration

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



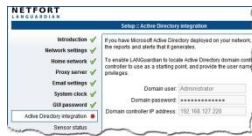
You can set the LANGuardian system clock manually or you can synchronize it automatically with a reference clock on the Internet.

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.

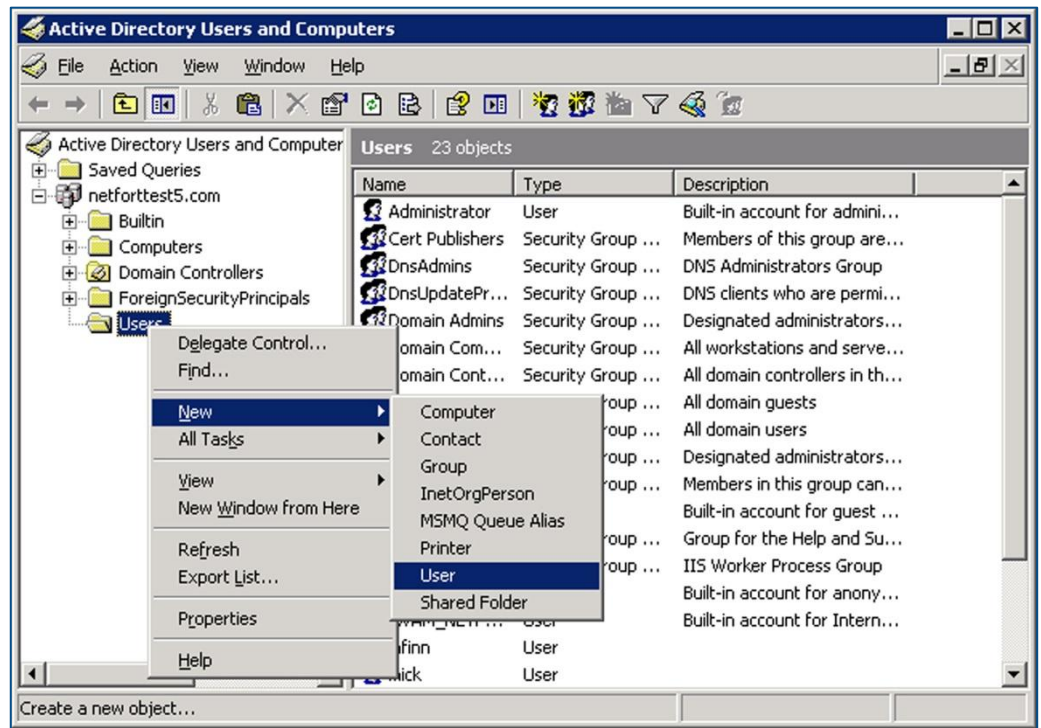
Configuring your Windows server

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.

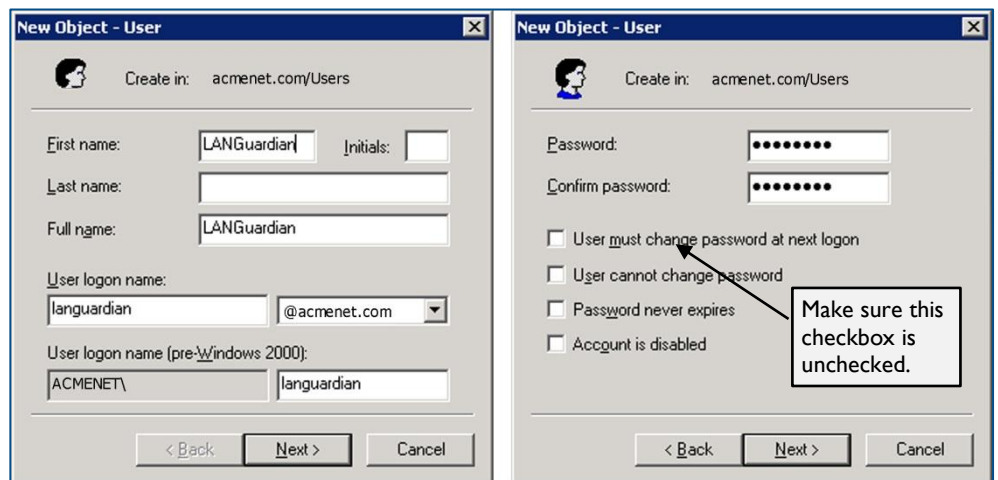
Create a LANGuardian account

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.



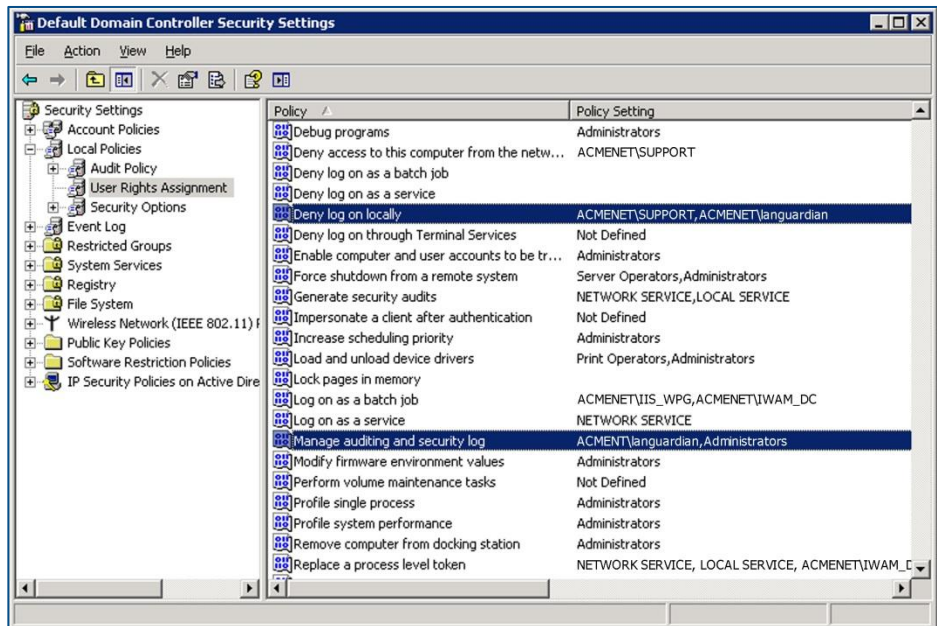
Make sure the **User must change password at next logon** checkbox is left unchecked.

Configure the account security attributes

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

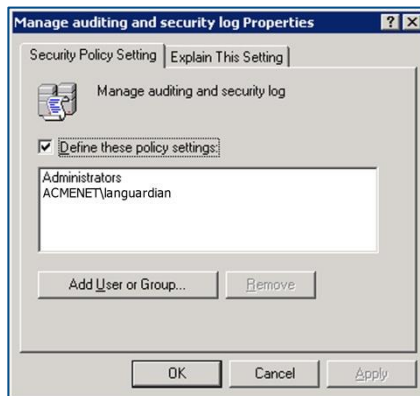
1. Click **Start** → **Administrative Tools** → **Domain Controller Security Policy**.
2. Click **Local Policies** → **User Rights Assignment**.

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.



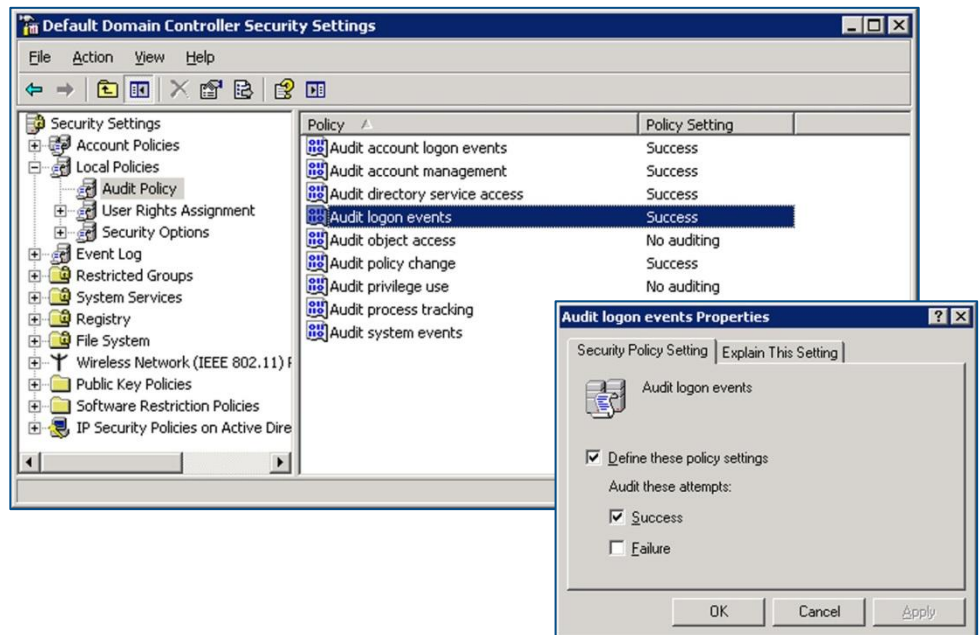
Configure event log auditing

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**.

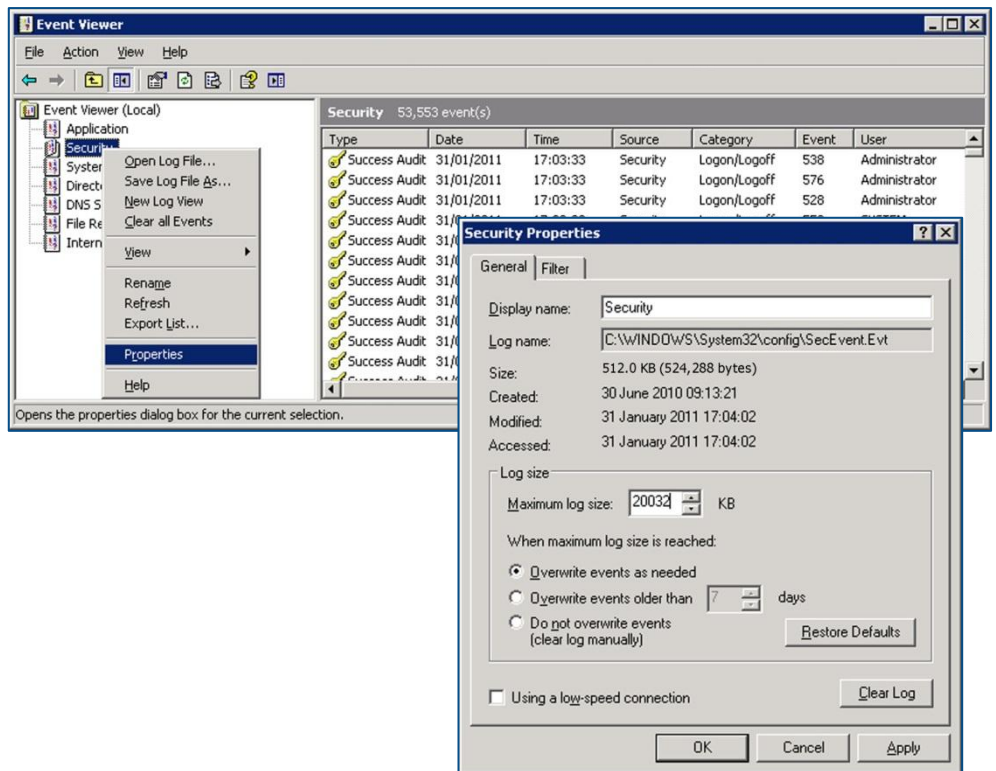


4. Check the **Success** checkbox to audit successful logon attempts in the event log.

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.

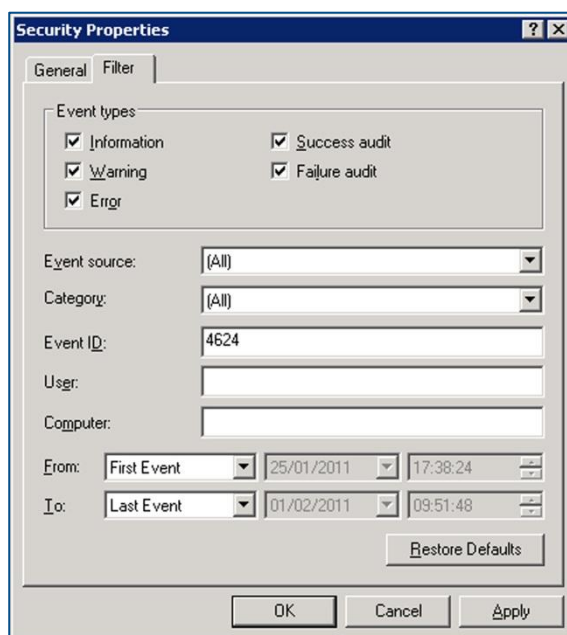
Follow these steps to set the maximum event log size:

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.

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 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.