

# Installing the LANGuardian ISO image

#### 03 October 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:

- I. 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.

# **Running the LANGuardian Setup utility**

The LANGuardian Setup utility runs when you boot the LANGuardian CD. There are six 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.



Enter YES to continue with the installation.

## Step 1: Select the installation disk

LANGuard:	ian Setup	
Step 1 o:	f 6: Select the installation disk	
The follo	owing list shows the existing disks on this computer.	
Disk ID	Description	Size
1 2 3 4	Western Digital WD5000B Maxtor Hitachi SD160002 Seagate HD Barracuda 7200 RPM	100 GB 400 GB 260 GB 500 GB
Please so Enter the	elect the disk on which you want to install LANGuardian. e 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 di	sk:
Disk ID Description	Size
2 Maxtor	400 GB
If you proceed with the installation, all data on Type YES to continue with the installation. Type Y without installing LANGuardian.	this disk will be erased. NO to quit the setup utility
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

LANGUARC	lian Setup	
Step 3 c	of 6: Select a network device for the LANGuardian user	interface
LANGuard be assig other NI	lian requires at least two network interface cards (NI gned to the browser-based user interface. LANGuardian CS to capture network traffic data.	Cs). One NIC will will use the
The foll	owing NICs are available on your computer:	
NIC ID	Description	Status
1	Intel PRO/1000 Network Connection	Connected
2	Intel PRO/1000 Network Connection	Connected
	Tatal DDO/1000 National Campactica	a , ,
3	Intel PRO/1000 Network Connection	Connected
3 4	Marvell Yukon 88E805 PCI-E Gigabit Ethernet	Not connected
3 4 Please s	Marvell Yukon 88E805 PCI-E Gigabit Ethernet	Connected Not connected
3 4 Please s If you w reconnec	Marvell Yukon 88E805 PCI-E Gigabit Ethernet select a NIC to assign to the user interface. want to be sure of the ID of each NIC, disconnect all so t them one at a time, pressing the R key after you co	Not connected Not connected network cables and nnect each one.

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 int	erface network device	
You have chosen to assign this devi	ce to the LANGuardian	user interface:
NIC ID Description		Status
3 Intel PRO/1000 Network Co	onnection	Connected
Please enter the following network	settings:	
LANGuardian computer IP address: LANGuardian computer network mask: Default gateway IP address: DNS server IP address:	192.168.127.200 255.255.255.0 192.168.127.1 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

Scep 5 of		
LANGuardı	an Setup will now complete the installation using the	ese 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 without i	to continue with the installation. Type NO to quit th nstalling LANGuardian.	ne setup program
without i	nstalling LANGUArdian.	

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, make a note of the LANGuardian URL, then remove the LANGuardian CD or USB flash drive and restart the system.



After the system restarts, you can visit the URL shown in step 6 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 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:



I. Accept the license agreement.

Satap :: Introduction		
Introduction	Welcome to the LANGuardian Configuration Wizard	
Network Settings	The LANGuerdien Configuration witand will guide you through the try ou skip any of the steps, you can complete them later in the L LICENSE AGREEMENT	
Prany Server		
Email Settings		
System Clock		
GUI Paseword	THE EVALUATION SOFTWARE MAY CONTAIN LIMITED FUN	
Active Directory Integration	FOR DEMONSTRATION AND EVALUATION PURPOSES ONLY COMMITICAL RUREONES, UNE OF THE EVALUATION FOR	
Sensor Status	BY USING THIS SOFTWARE, YOU AGREE TO THE TERMS OF	
	F Lagree with the licensing terms	

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.

Setup :: Network Settings			
Introduction 🎸	The LANGuardian management interface connects to your network		
Network Settings 😐	Enter the network settings for this interface. You will use the IP add		
Proxy Server Ernall Settings System Clock GUI Password Ictive Directory Integration Sensor Status	IP address 192.168.52.5 Gatewys 192.168.52.2 DNS server 8.8.8.8		

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.

	Setup :: Proxy Server
Introduction 🖌	LANGuardian connects to the Internet to keep itself up to date by di
Network Settings 🖌	if your nativosh provides access to the internet through a proxy sam
Proxy Server 🌒	if your nativosh provides direct access to the Internet, Isave the field
Email Settings	Specify the prexy server using the following ferent choolsance part
System Clock	If the prexy server requires authentication, specify a username and
GUI Password	HTTP prexy:
Active Directory Integration	HTTP prexy user.
Sensor Status	HTTP prexy password:

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.

	Setup ::	Email Settings
Introduction 🖌 Notwork Settings 🖌 Proxy Server 🖌	LANGuardian v Enter the addre Tha From Addr	ses e mail to send scheduled reports to users and to ss of the SMTP server that LANGuardien will use to sss is the e-mail address that will appear as the send
Email Settings 😐	SMTP server d	omain; many e-mail servers will not send e-mail usle
System Clock	To address:	alerts@netforttechnologies.com
GUI Password	From address:	alerts@netfortlechnologies.com
Active Directory Integration	SMTP server.	159.134.198.135
Sensor Status		

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.

	Setup :: System Clock
Introduction 🖌	The can set the UMGaurdine system clock namely or you
Rotwork Settings 🖌	UMGaurdine sease and to seet a clock namely or you
Proxy Server 🖌	Content close and free 26.03.2912 13.51
Email Settings 🚽	C Set manual
System Circk •	Date: Use State With
GUI Password	Time: Use State
Active Directory Integration	Phase years: Decoding long
Senser Status	Secondary serve: [pcc/clop.up]

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.

Setup :: GUI Password		
letroduction ✓ Network Settings ✓ Proxy Server ✓ Email Settings ✓ System Clock ✓ GUI Password ●	Set a password for the LANDuardian Administrator account. After Type a new password: Type a new password again to confirm: Note: the password must be at least 7 characters long.	
tive Directory Integration Sensor Status		

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

7. Specify the Active Directory details.



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

8. Review the sensor status.

	Sela	: Sensor st	ales	
Introduction 🖌	The final ste network.	p in configuri	ing your LA	VSuardian system k
Home network 🖌	Link up indi	also that the	sensor is	connected to a netw
Proxy server 🧹	SPAN treffs	indicates the	al Tre sero	or is capturing neter
Email settings 🖌	Last undate	Ine 142.20	011 11:29	
System clock 🧹	Service	Interface	Linkup	SPANINATE
System clock 🗹 Gill password 🖋 the Directory integration 🖌	Senar 1	ovi1	Lêksp V	Shih bafte

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

- 9. Click **Finish** to complete the configuration. LANGuardian displays the login page.
- 10. Type Administrator as the username, type the password that you set in Step 7, and click Log In. LANGuardian displays the main menu 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. For information on using LANGuardian, see the LANGuardian Administration and User Guide at:

http://www.netfort.com/downloads/documentation

# **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 readonly. 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:

- I. 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  $\rightarrow$  New  $\rightarrow$  User.



🐗 Active Directory Users and Compu	uters			_ 🗆 ×
Gile Action View Window He	lp			_ <del>8</del> ×
← → 🗈 📧 🐰 🛍 🗙 📽	🖸 🗟 😫 🖬	🛛 😿 🖉 🎽 🖓	🤹 🙍	
Active Directory Users and Computer Active Directory Users and Computer Active Directory Users and Computer Active Directory Users and Computers Builtin Computers Domain Controllers ForeignSecurityPrincipals Delegate Control Find New All Tasks View New Window from Here Refresh Export List	<ul> <li>Users 23 objects</li> <li>Name</li> <li>Administrator</li> <li>Cert Publishers</li> <li>DnsAdmins</li> <li>DnsUpdatePr</li> <li>Domain Admins omain Com</li> <li>omain Cont</li> <li>Computer</li> <li>Contact</li> <li>Group</li> <li>InetOrgPers</li> <li>MSMQ Queu</li> <li>Printer</li> <li>User</li> </ul>	Type         User         Security Group         Security Group	Description Built-in account for admini Members of this group are DNS Administrators Group DNS clients who are permi Designated administrators All workstations and serve All domain controllers in th All domain guests All domain users Designated administrators Members in this group can Built-in account for guest Group for the Help and Su IIS Worker Process Group Built-in account for apopy.	
P <u>r</u> operties Help		User	Built-in account for Intern	
Create a new object	i 🖘 Mick	User		<u> </u>

5. Enter the user account details and password.

ew Object - User	New Object - User
Create in: acmenet.com/Users	Create in: acmenet.com/Users
Eirst name:	Password:
Full name: LANGuardian	User must change password at next logon
languardian @acmenet.com	Password never expires Make sure this
User logon name (pre- <u>W</u> indows 2000): ACMENET\ languardian	Checkbox is unchecked.
< <u>B</u> ack <u>N</u> ext > Cancel	< <u>B</u> ack <u>N</u> ext > Cancel

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:

- Click Start → Administrative Tools → Domain Controller Security Policy.
- 2. Click Local Policies  $\rightarrow$  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.

Manage auditing and security log Properties 🛛 🔋 🗙
Security Policy Setting Explain This Setting
Manage auditing and security log
Define these policy settings:
Administrators ACMENET\languardian
Add User or Group
OK Cancel Apply

#### 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:

- Click Start → Administrative Tools → Domain Controller Security Policy.
- 2. Click Local Policies  $\rightarrow$  Audit Policy.



3. Double-click the policy Audit logon events.

🚡 Default Domain Controller Securi	ty Settings		
Eile Action View Help			
⇐ ⇒ 🗈 🖪 🗙 🗳 😫	<b>N</b>		
Security Settings     Count Policies     Local Policies     Local Policies     Local Policies     Security Options     Security Options     Registry     System Services     Registry     System Setwork (IEEE 802.11) F     Public Key Policies     Software Restriction Policies     IP Security Policies on Active Dire	Policy Pol	Policy Setting         Success         Success         Success         Success         No auditing         Success         No auditing         Success         No auditing         Security Policy Setting         Explain This         Image: Comparison of the security Policy Setting         Audit logon events         Image: Comparison of the security Policy settings         Audit these attempts:         Image: Comparison of the security Policy settings         Audit these attempts:         Image: Comparison of the security Policy Settings         Audit these attempts:         Image: Comparison of the security Policy Settings         Audit these attempts:         Image: Comparison of the security Policy Settings         Audit these attempts:         Image: Comparison of the security Policy Settings         Audit these attempts:         Image: Comparison of the security Policy Settings         Success         Image: Comparison of the security Policy Settings         Success         Image: Comparison of the security Policy Settings         Success         Image: Comparison of the security Policy Settings         Success	2 Setting
		ОК	Cancel Apply

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:

- I. Click Start  $\rightarrow$  Administrative Tools  $\rightarrow$  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.



Event Viewer								
Image: Second	Security 53,57 Type Success Audit Success Audit	53 event(s)  Date  31/01/2011  31/01/2011  31/01/2011  31/0  Security 31/0  Gener 31/0  Size: Creat Modil Acce Log M W G C C	Time           17:03:33           17:03:33           17:03:33           17:03:33           Properties           al           Filter           ay name:           ay name:           ay name:           gize           aximum log siz           aximum log siz           'hen maximum           Qverwrite ev           Ovgerwrite ev           Do pot over           sing a log-spe	Source Security Security Security Security Security C:\V/INDOV 512.0 KB (52 30 June 2010 31 January 20 31 January	Category Logon/Logoff Logon/Logoff Logon/Logoff (S\System32\con 4,288 bytes) 103:13:21 111 17:04:02 111 17:04:04:04:04:04:04:04:04:04:04:04:04:04:	Event. 538 576 528 	User Administrator Administrator 2 > 2 > ent.E vt : Defaults Clear Log	

- 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)



General Filter	?
Event types I Information Warning Error	I⊽ <u>S</u> uccess audit I⊽ Failure audit
Event source:	(All)
Category:	(All)
Event I <u>D</u> :	4624
Us <u>e</u> r:	
Computer:	
Erom: First Event	25/01/2011 🔽 17:38:24 🚆
Io: Last Event	▼ 01/02/2011 ▼ 09:51:48 🗧
	<u>R</u> estore Defaults
	OK Cancel Apply

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:

- I. 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 I	Directory: Domain Controllers
Domain Co	ntrollers auto discover
<ul> <li>○ Use exi</li> <li>● Enter ne</li> </ul>	sting credentials ew credentials
User	administrator
Password	•••••
IP Address	192.168.127.182
	Search

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 D	lirec	tory: Domain Contr	ollers Search resul	t		
Domain Cor	itroll	ers auto discover				
Use exis	sting	credentials				
Enter ne	w cr	edentials				
User	adn	ninistrator				
Password	••••	•••••				
IP Address	192	.168.127.182				
	Se	arch				
Search resu	lt.					
Name		IP Address	User	Domain	Version	
DC-ACME-2		192.168.127.182	administrator	acme.com	2008R2	added
Save Se	lecte	ed				

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

Active Dire	ectory: List of serve	rs						
Add new se	rver 🔀 Advanced							
Name	IP Address	User	Domain	Version	Status	Test	Edit	Delete
DC-ACME-1	192.168.127.181	administrator	acme.com	2008R2	<b>V</b>	0	0	×
DC-ACME-2	192.168.127.182	administrator	acme.com	2008R2	<b>√</b>	0	3	×
Test All Update Directo Update Interva	ry information from A I: weekly 💌 Sa	AD Controllers ( ave Update	this may take	some time)	)			

#### 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 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.



# Appendix A: Creating a bootable CD

To create a bootable CD, download the LANGuardian ISO image and use ImgBurn to copy the image to a USB stick (ImgBurn is free but you can also use commercial alternatives such as Nero, Roxio Toast, and PowerISO).

The steps to create a bootable CD are as follows:

I. Download the LANGuardian ISO image from the Downloads page on the NetFort website:

http://www.netfort.com/software-download

The ISO image will have a filename such as Ig-10.0.iso.

2. Download ImgBurn from:

http://www.imgburn.com

The download is a Windows installer – after downloading, double-click the installer file to install ImgBurn on your computer.

- 3. Insert a blank CD in the optical drive of your computer, then launch ImgBurn from the Windows Start menu.
- 4. In the main ImgBurn window, click the icon for Write image file to disc.



5. ImgBurn will display its **Write** window. In the **Source** area, select the LANGuardian image you downloaded from the NetFort website. Then, click the Write icon at the bottom of the window.



Label: Imp ID: File Sys:	CDROM Unknown ISO9660 (Bootable), Joliet		
Sectors:	25,049 (MODE1/2048)		
Size:	51,300,352 bytes	-	0
Time:	05:35:74 (MM:SS:FF)	C	6
Destinati	on		
[2:0:	UJ HL-D1-ST BD-RE BH10LS38 (E:)	_	
🎯 🗖	Test Mode 🛛 📝 Verify		9

ImgBurn will burn the LANGuardian image onto the CD and display a status message when the CD is ready.

You now have a bootable LANGuardian CD.