

LANGuardian 8.4

Active Directory Configuration Guide

Version 2.1

11 May 2010

Contents

1	Introduction	3
2	Supported versions of Microsoft™ Active Directory.....	3
3	Requirements.....	4
3.1	Domain Account.....	4
3.2	Event Log Auditing	4
3.3	LANGuardian License	4
4	Configuration steps.....	5
4.1	Create and configure the Domain Account	6
4.1.1	Create an account in the Active Directory Domain	6
4.1.2	Configure the account Security attributes.....	7
4.2	Configure the Event Log Auditing	9
4.2.1	Check that the security event logs are set to a sufficient size.....	9
4.2.2	Determine which type of event is suitable for your version of Active Directory	10
4.2.3	Enable Auditing of Events	10
4.2.4	Verify that events are being logged on the Domain Controller.....	11
5	Configure the LANGuardian	12
6	Editing the Domain Controller configuration on LANGuardian	14
7	Testing the Configuration	15
8	Error Messages.....	16

1 Introduction

Microsoft™ Active Directory is one of the directory systems supported by the LANGuardian Identity Module. The LANGuardian Identity Module associates a username provided by the directory with every network event and traffic flow that is recorded by LANGuardian.

This guide describes how to configure your LANGuardian and Active Directory to successfully integrate the two products.

This guide is for LANGuardian Version 8.4.

For further information please contact support@netforttechnologies.com

2 Supported versions of Microsoft™ Active Directory

LANGuardian Version 8.4 supports:

- Windows Server 2008 R2
- Windows Server 2003 R2 (32 bit)
- Windows Server 2000

3 Requirements

3.1 Domain Account

The LANGuardian requires an Active Directory Domain account that has been granted sufficient privileges to read the Domain Controller Event Security Logs. The steps to configure the account are described in section 4.1 *Create and configure the Domain Account*.

If multiple Active Directory Domains are to be supported, then a separate account in each domain is required.

3.2 Event Log Auditing

The LANGuardian requires that auditing for successful network logons are enabled on each Domain Controller in the Domain. The steps to enable the auditing are described in section 4.2 *Configuring the Eventlog Auditing*.

3.3 LANGuardian License

The LANGuardian Identity Module is an optional module that must be enabled by loading an appropriate license. The evaluation versions of LANGuardian (if you downloaded the software) automatically support the Identity Module. Please contact support@netforttechnologies.com for further information.

4 Configuration steps

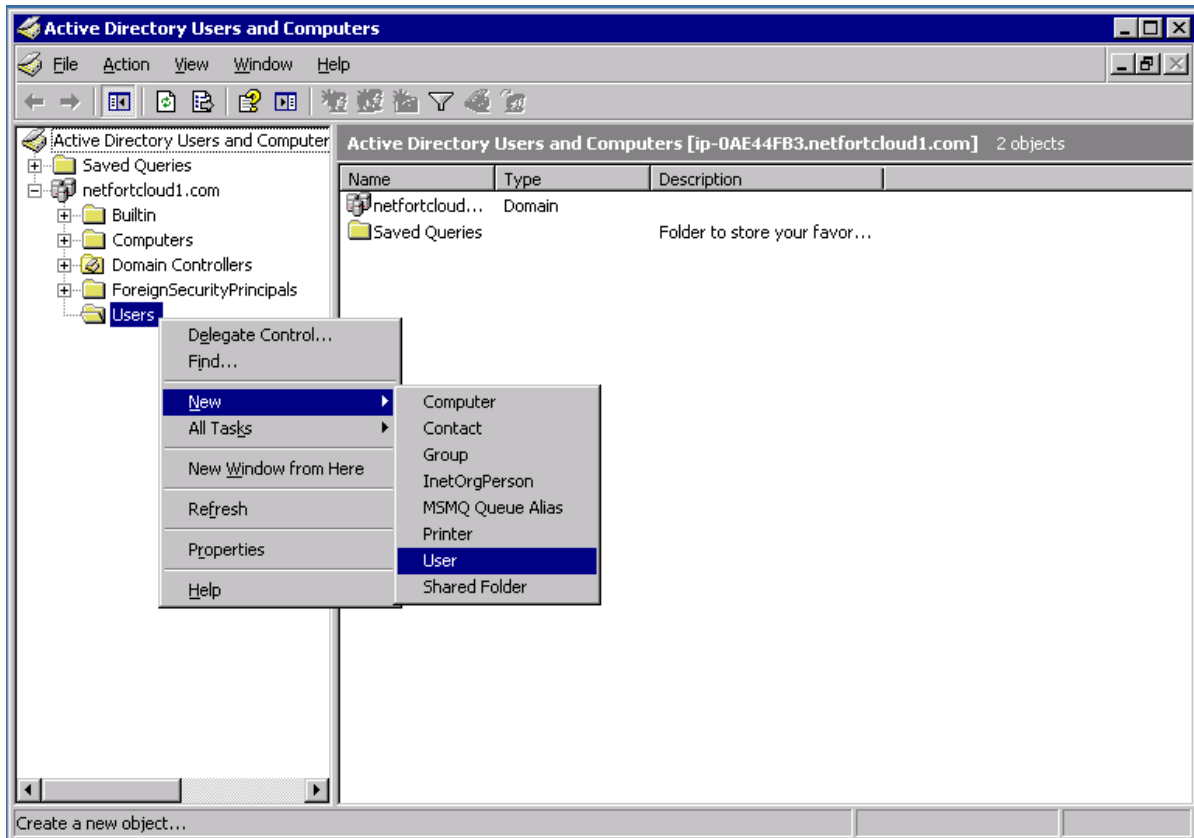
This guide describes the following steps which are required to enable Active Directory Support on LANGuardian.

- Create and configure the Domain Account
- Configure the Event Log Auditing
- Configure the LANGuardian

4.1 Create and configure the Domain Account

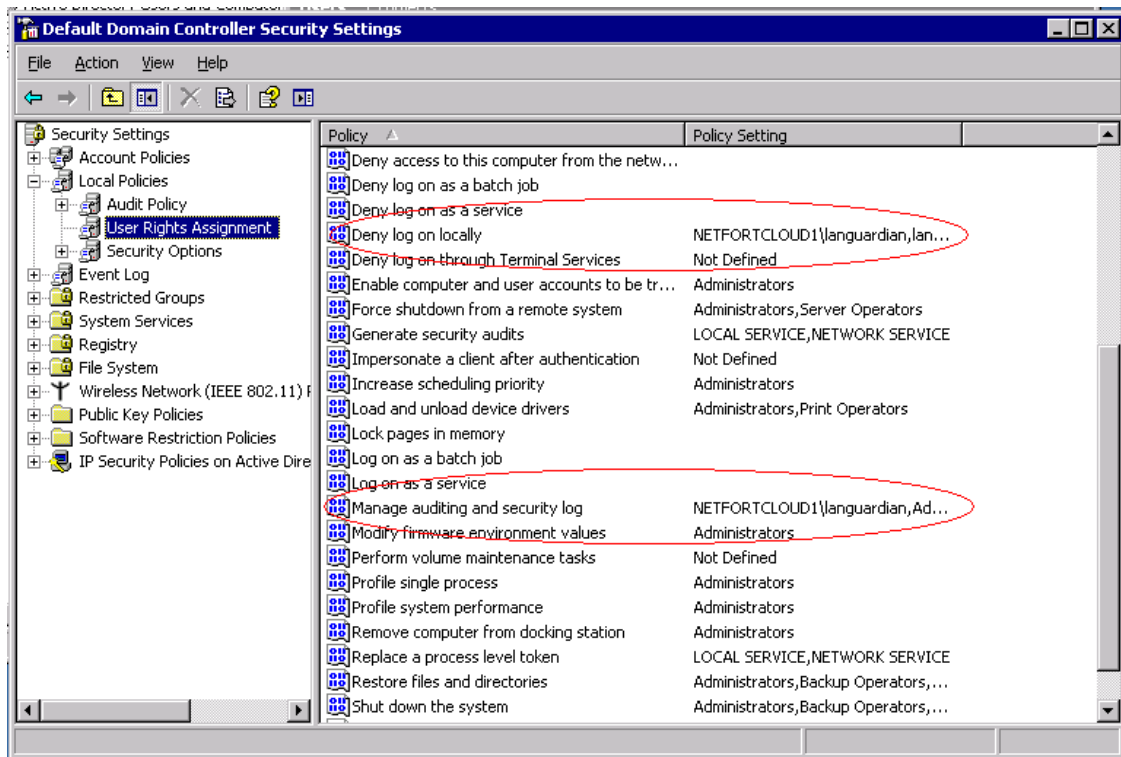
4.1.1 Create an account in the Active Directory Domain

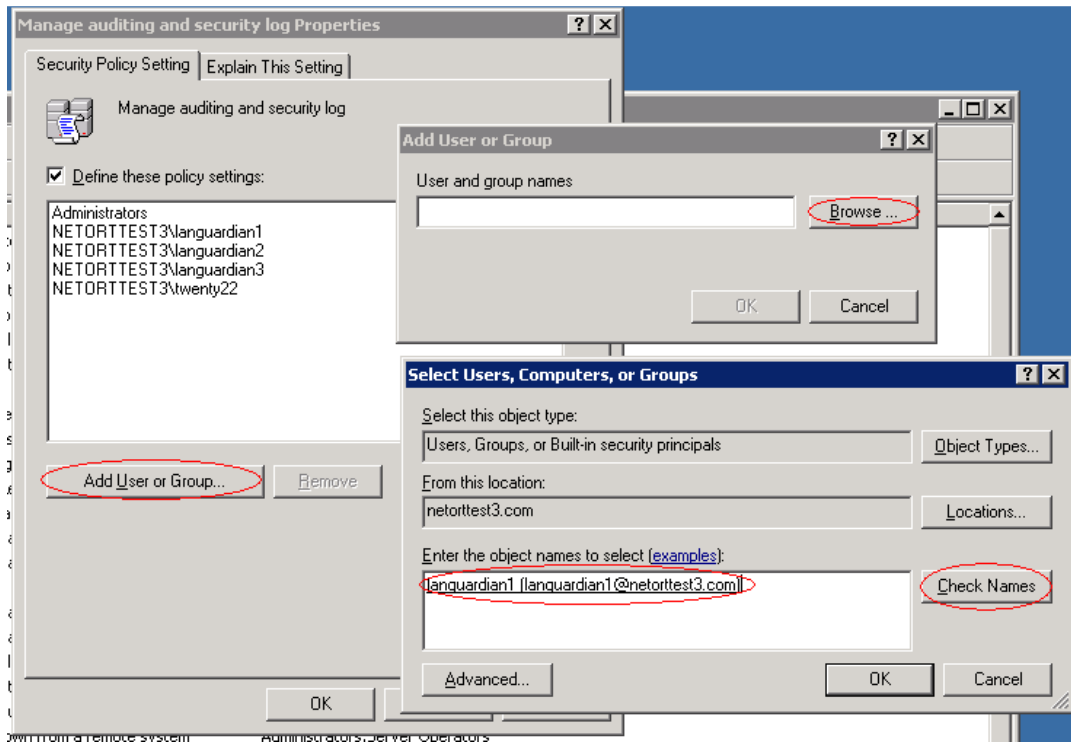
1. Logon to an Active Directory Domain Controller
2. Open Start -> Administration Tools -> Active Directory Users and Computers
3. Under the correct Domain, right click on Users and select New
4. Type in the user account details and click on next
5. Unselect the checkbox marked *User must change password at next logon*
6. Save the User Account



4.1.2 Configure the account Security attributes

1. Open Start -> Administration Tools -> Domain Controller Security Policy
2. Open Local Policies -> User Rights Assignments
3. Double click on *Manage auditing and security log* to open the *Manage auditing and security log Properties* dialog.
4. Click on *Add User or Group* to open the *Add User or Group* dialog
5. Click on *Browse* to open the *Select Users Computers or Groups* dialog
6. Type the name of the account that you created in the domain as described in section 4.1.1
7. Click on *Check Names* button to correctly identify the domain account
8. Click the successive *OK* buttons to save the change
9. OPTIONAL STEP. To follow a practice of granting minimum required privilege to newly created accounts, double click on *Deny log on locally* and repeat steps 4 to 8 above.



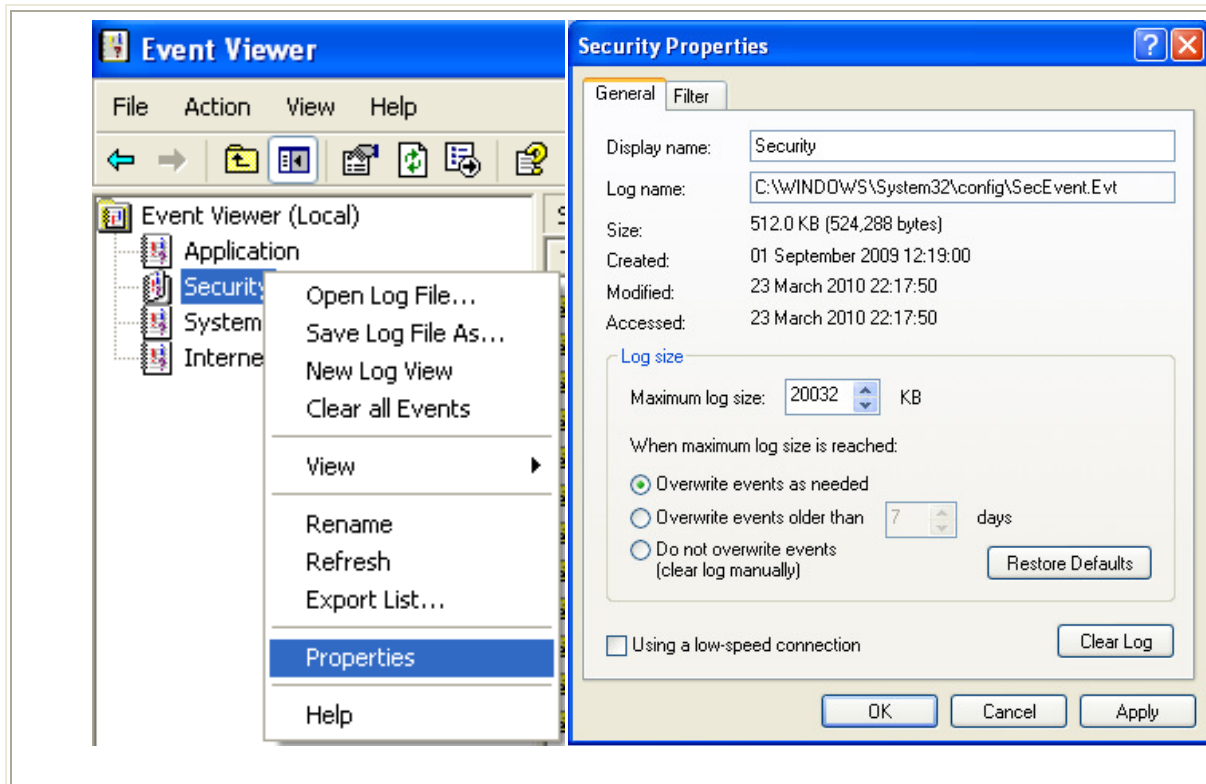


Screen shots of how to configure domain account Security Attributes on Windows Server 2003

4.2 Configure the Event Log Auditing

4.2.1 Check that the security event logs are set to a sufficient size

1. Open Start > Administrative Tools -> Event Viewer
2. Right click on the Security Log
3. Select Properties
4. Set the *Minimum Log size* to 20 MB (20032 KB) and *When Maximum log size is reached* to *Overwrite events as needed*.



4.2.2 Determine which type of event is suitable for your version of Active Directory

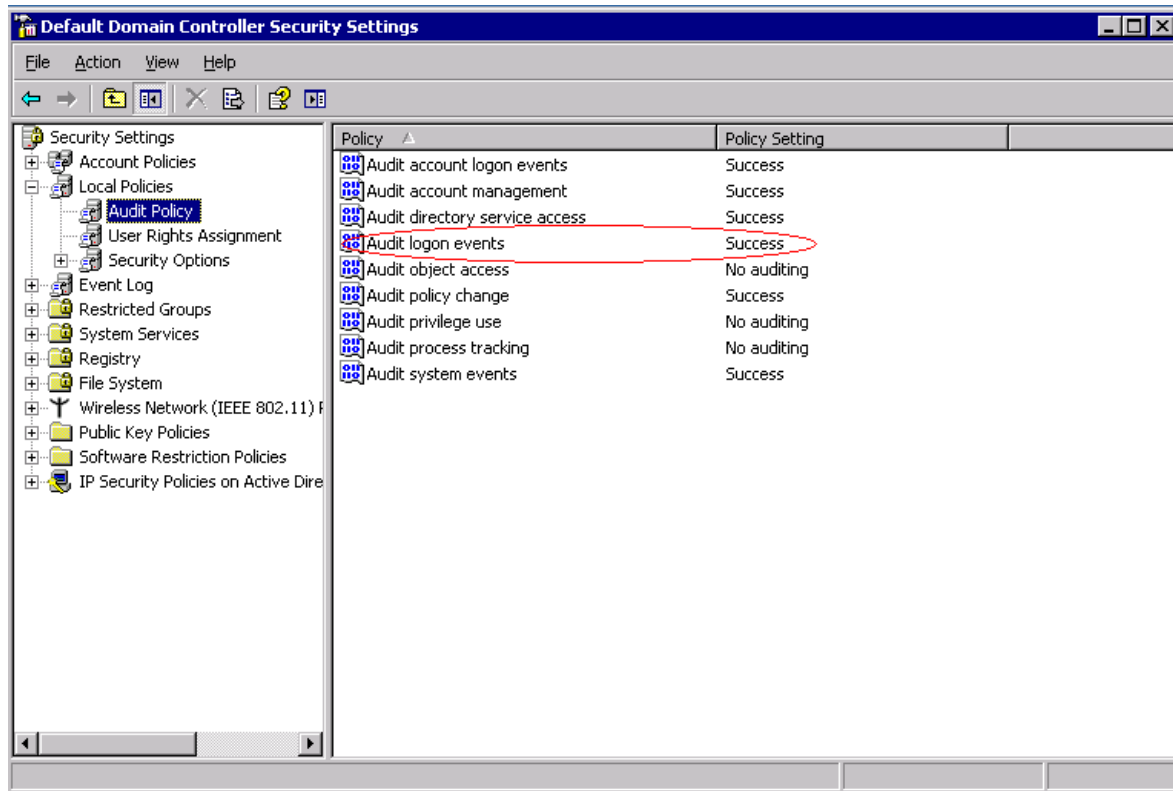
The following table shows the options available for selecting events for Auditing

Server Windows Server version	Event Description	Supported Event IDs
2008 R2	Logon Event	4624
2008	Logon Event	4624
2003	Logon Event or Account Logon Event	540 or 672
2000	Account Logon Event	672

Table 1 – Supported Event types

4.2.3 Enable Auditing of Events

1. Open start -> Administrative tools -> Domain Controller Security Policy
2. Click on Security Settings -> Local Policies -> Audit Policy
3. Enable Auditing for Success for your chosen Event ID (see Section 4.2.2)



4.2.4 Verify that events are being logged on the Domain Controller

1. Open the Start -> Administrative Tools -> Event Viewer
2. Right click on Security -> View -> Filter
3. Enter your chosen event ID in the event ID field (see Section 4.2.2)
4. Click OK
5. Verify that events are listed

5 Configure the LANGuardian

1. Open Configuration -> Configure support for Active Directory identity logging
2. Click on *Auto-Discover*
3. Select the *Enter new credentials* radio button
4. Type the password of the LANGuardian Domain Account in the *Password* field
5. Type the IP address of any Domain Controller in the Domain in the *IP Address* field
6. Click on the *Search* button

Active Directory: Domain Controllers

Domain Controllers auto discover

Use existing credentials
 Enter a new credentials

User

Password

IP Address

LANGuardian searches for all Domain Controllers in the Domain (even those that are not running) and displays the results.

Active Directory: Domain Controllers Search result

Domain Controllers auto discover

Use existing credentials
 Enter a new credentials

User

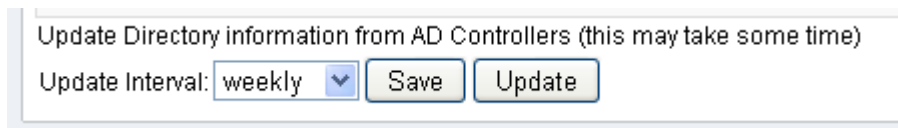
Password

IP Address

Search result.

Name	IP Address	User	Domain	Version	
test1	192.168.127.155	languardian	netforttest1.local	2003	<input type="checkbox"/>

7. Select those Domain Controllers that should be queried to obtain user logon information. As any Domain Controller on a Domain can authenticate users logging on to a Domain, Netfort advise that all Domain Controllers in a Domain should be added. However, the Administrator may elect to exclude some Domain Controllers that are known not to authenticate any users (for examples DC's on remote sites which may take a long time to query).
8. Click on Save
9. Determine a suitable interval for LANGuardian to check for updates and changes to the directory. This allows LANGuardian to detect when new users have been added to the directory, or other setting such as email addresses for user have changed.
10. Select the correct update interval from the *Update Directory information from AD Controllers* drop down list. Weekly is normally sufficient.



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

Update Interval: weekly

11. Click on *Save*
12. This completes the Active Directory configuration.

6 Editing the Domain Controller configuration on LANGuardian

After adding a Domain Controller to LANGuardian, you can review or edit the settings.

1. Open Configuration -> Configure support for Active Directory identity logging
2. Locate the Domain Controller in the table of known Domain Controllers
3. Click on the *Edit* button
4. Review the configuration or make changes as desired
5. Click on the *Save* button

Active Directory: List of servers

[Add new server](#) [Auto discover](#)

Name	IP Address	User	Domain	Version	Status	Test	Edit	Delete
NETFORT-7362AED	192.168.127.188	languardian1	netforttest3.com	2003				
VMN-ID46IOORJI6	192.168.127.189	languardian1	netforttest3.com	2008R2				

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

Update Interval:

Active Directory: Edit server "192.168.127.188"

Server IP:

User:

Password:

Domain:

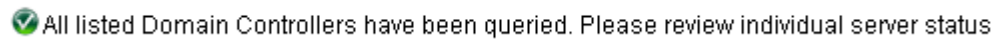


Event ID: Logon Event (ID 540)
 Account Logon Event (ID 672)
 2008 Logon Event (ID 4624)

Screenshot of editing Domain Controller configuration on LANGuardian

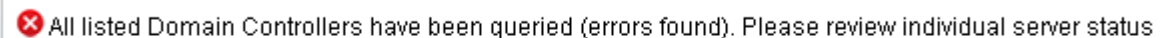


7 Testing the Configuration

The LANGuardian Active Directory Configuration page helps test and troubleshoot the Active Directory Configuration settings.

1. Open Configuration -> Configure support for Active Directory identity logging
2. Click on the Test All button
3. Review the result.
4. If the result looks the following, then the configuration has been completed successfully.

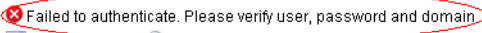



 









5. If the result looks like the following, then there is an error in the configuration, move on to step 6.

6. Identify servers that are reporting errors and click on the test button for each
7. Review the informational messages and actions in Section 8

Active Directory: List of servers

Name	IP Address	User	Domain	Version	Status	Test	Edit	Delete
NETFORT-7362AED	192.168.127.188	languardian1	netortest3.com	2003				
WIN-I046I00RJI6	192.168.127.189	languardian1	netortest3.com	2008R2				

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

Screenshot showing server 192.168.127.189 reporting an error and the informational message generated by clicking on the test button.

8 Error Messages

The following errors messages are displayed.

Message	Description	Action
Server authenticated OK	The server was contacted, the event log is readable and there are logon events present.	No user action required. If you still have problems with the integration, please contact support@netforttechnologies.com
Failed to connect to the server	The selected server cannot be contacted	<p>Check IP address of the Domain Controller is specified correctly.</p> <p>Check the Domain Controller is running.</p> <p>Check there is no ACL blocking access to the Domain Controller.</p> <p>Check the default router is correctly set on LANGuardian</p>
Failed to authenticate. Please verify user, password and domain	An LDAP connection and query to the Domain Controller was refused	<p>Verify the Domain Account exists (see section 4.1.1)</p> <p>Verify the Domain Account and Password are correctly entered on LANGuardian</p> <p>Verify the Domain specified on LANGuardian exists</p>
Failed to read Event Security Log. Please verify the domain account has sufficient rights	The specified Domain Account does not have sufficient permissions to read the Event Security Log on the Domain Controllers.	Verify the specified Domain Account has rights to 'Manage auditing and Security Logs' in the Default Domain Controllers Security Policy. See Section 4.1.2
'Windows 2000 Server must be configured to use Account Logon Event only	LANGuardian is attempting to read an unsupported event type from a Windows Server 2000 Domain Controller.	Edit the LANGuardian configuration to specify Account Logon Event for all Windows Server 2000 Domain Controllers. See Section 4.2.2.

'Failed to find a recent Logon Event (ID 540) in the Security Event log	LANGuardian connected to the Domain Controller and accessed the Event Security Log, but could not find an Logon Event logged there during the past 1 hour.	Verify the Domain Controller is recoding Logon Events (ID 540) by checking in the Event Viewer. See sections 4.2.4, 4.2.2 and 4.2.3
Failed to find a recent Account Logon Event (ID 672) in the Security Event log	LANGuardian connected to the Domain Controller and accessed the Event Security Log, but could not find an Account Logon Event logged there during the past 1 hour.	Verify the Domain Controller is recoding Account Logon Events (ID 672) by checking in the Event Viewer. See sections 4.2.4, 4.2.2 and 4.2.3
Windows 2008 Server must be configured to use 2008 Logon Event only	LANGuardian is attempting to read an unsupported event type from a Windows Server 2008 or Windows 2008 R2 Domain Controller.	Edit the LANGuardian configuration to specify Account Logon Event for all Windows Server 2000 Domain Controllers. See section 4.2.2.
Failed to find a recent 2008 Logon Event (ID 4624) in the Security Event log	LANGuardian connected to the Domain Controller and accessed the Event Security Log, but could not find an Account Logon Event logged there during the past 1 hour.	Verify the Domain Controller is recoding Logon Events (ID 4626) by checking in the Event Viewer. See sections 4.2.4, 4.2.2 and 4.2.3
An unknown error has occurred		Please contact support@netforttechnologies.com

Table 2. Error messages and actions