Integrating LANGuardian with Active Directory

01 February 2012

This document describes how to integrate LANGuardian with Microsoft Windows Server and Active Directory.

Overview

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

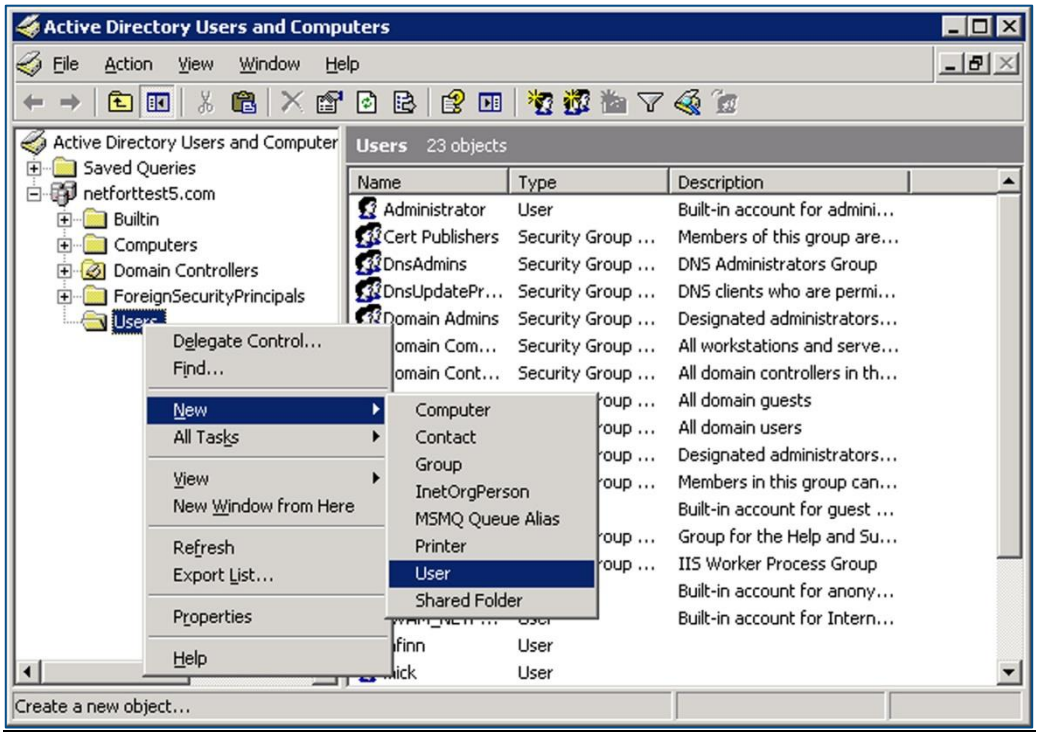
To configure your Windows server to work with LANGuardian, you must create a LANGuardian-specific account on the Windows domain, give the account the required permissions, and enable event log auditing.

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

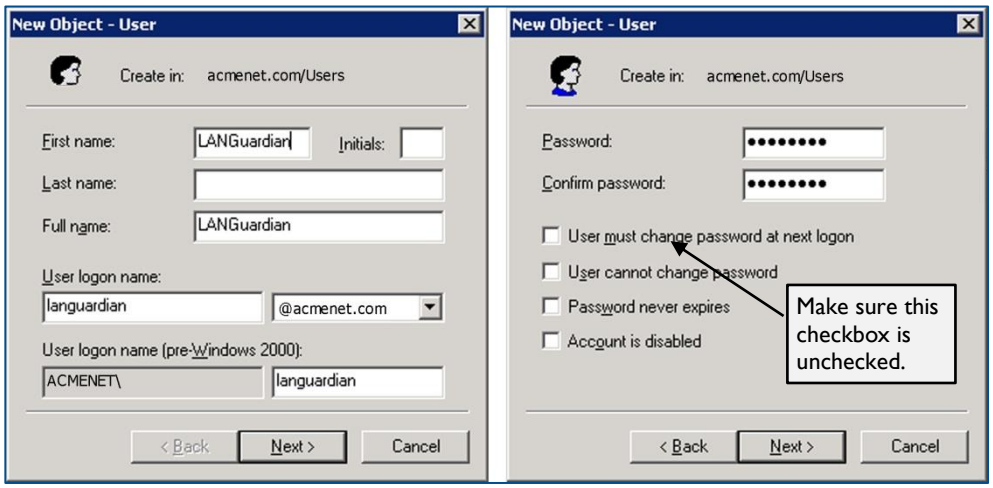
Create a LANGuardian account

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.

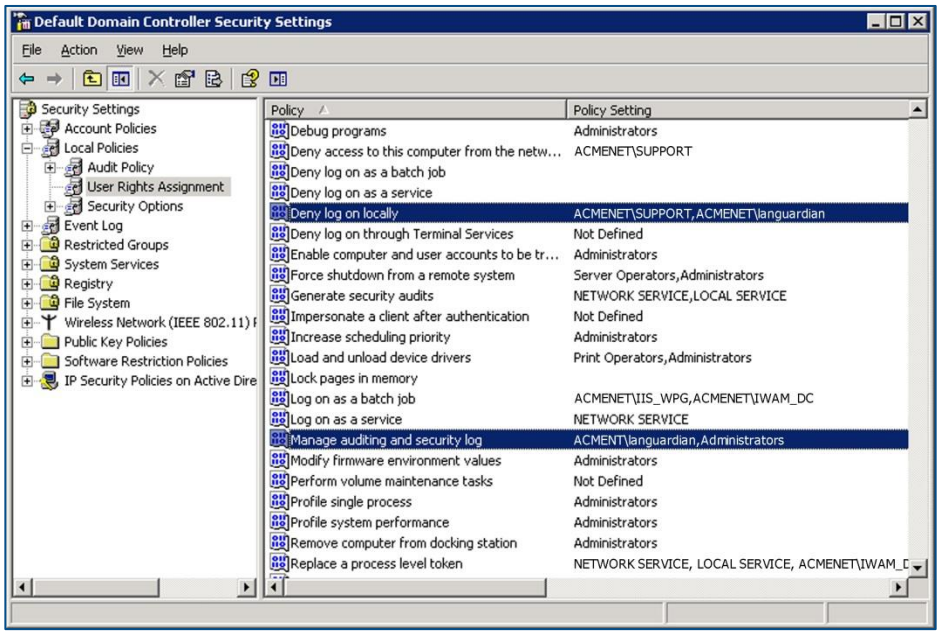
Configure the account security attributes

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

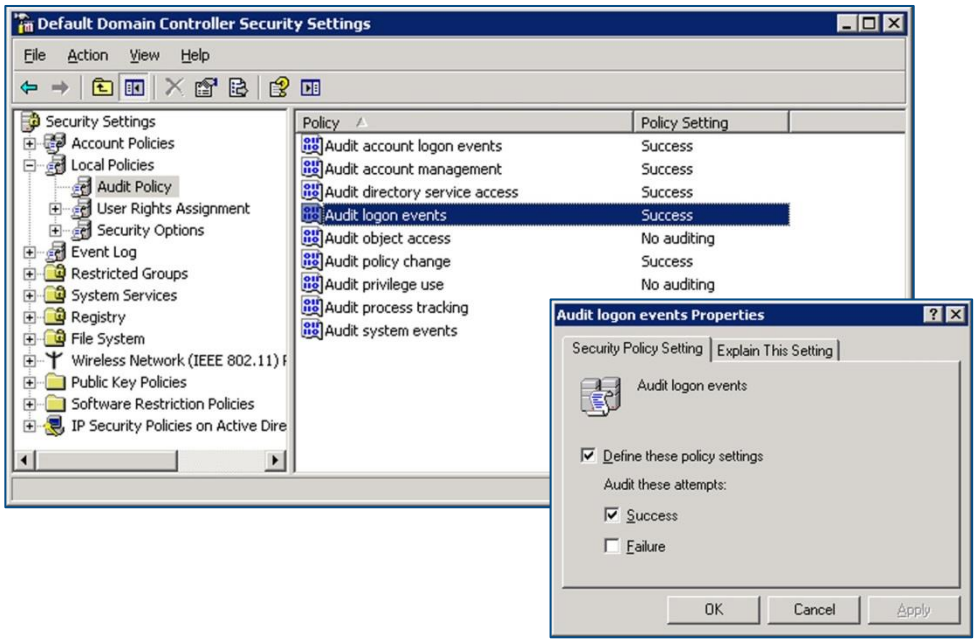
In a Windows server, the event log records details of all system and user activity (events). There are many different types of event, and you can configure the Windows server to record only the events that are of interest. If you record logon events, LANGuardian can include details of user logons in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

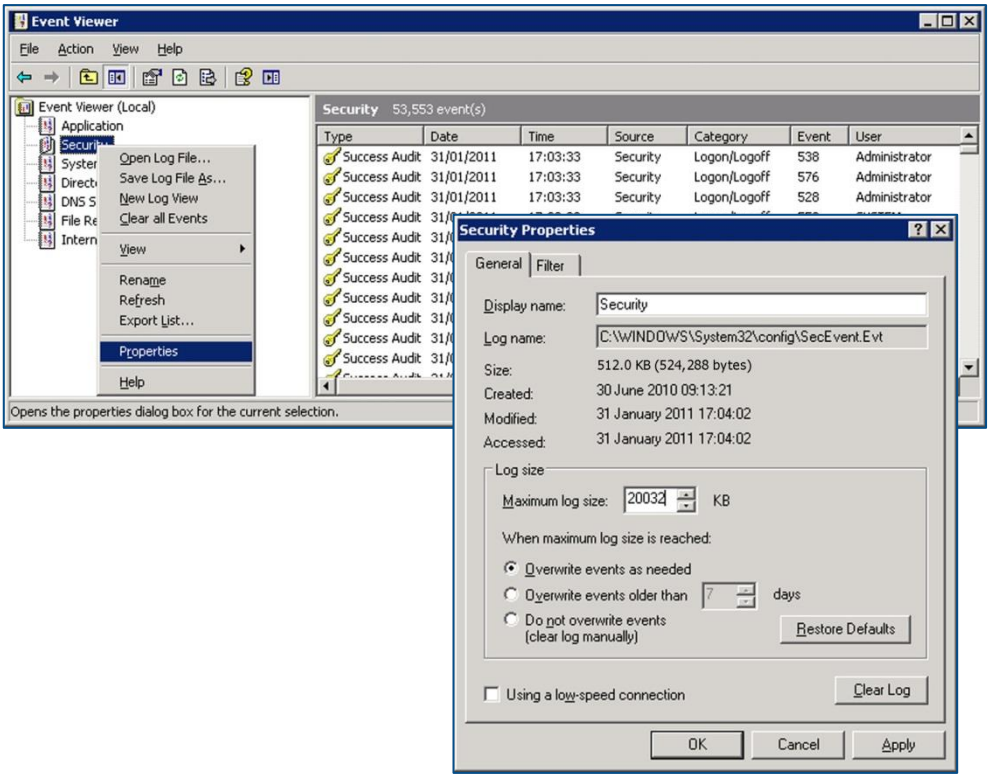
Follow these steps to set the maximum event log size:

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

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

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

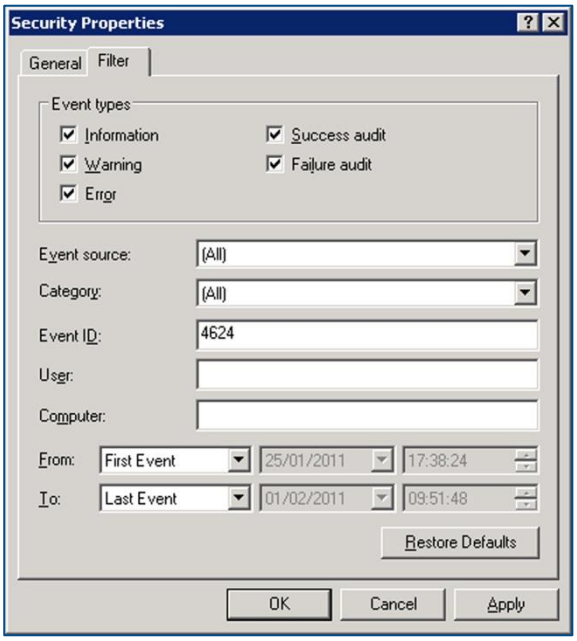
4. On the General tab, set the **Maximum log size** to 20032 MB.



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.

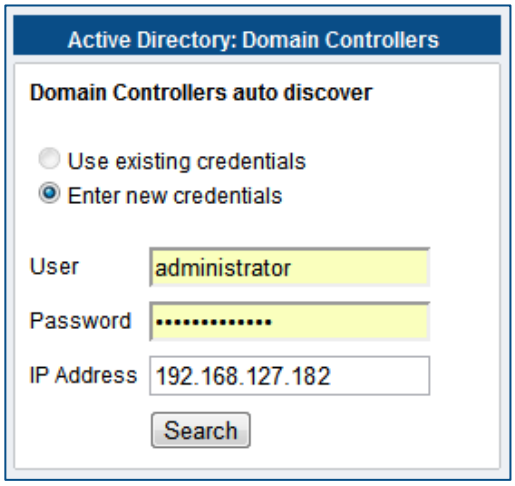
2. On the Configuration page, scroll down to the section on **Identity Configuration**.

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.**

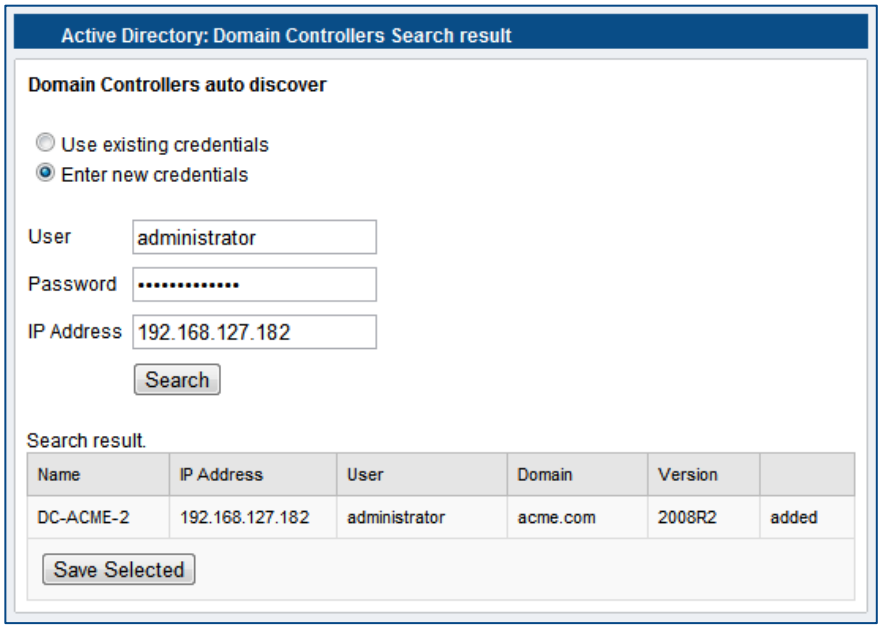


Enter the following details:

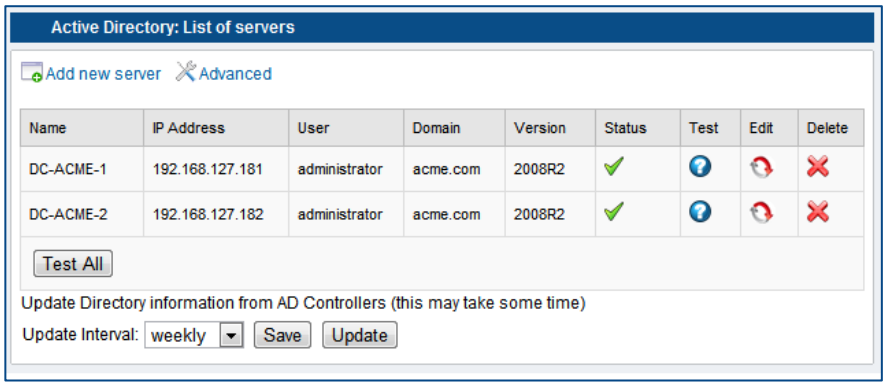
- **User:** the username of the domain account.
- **Password:** the password for the domain account.
- **IP Address:** the address of a domain controller.

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.**



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



Notes:

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

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.