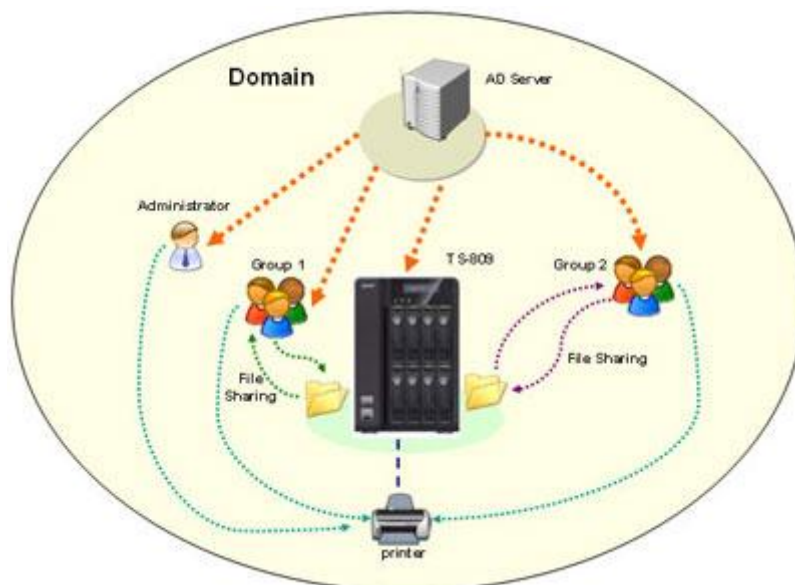
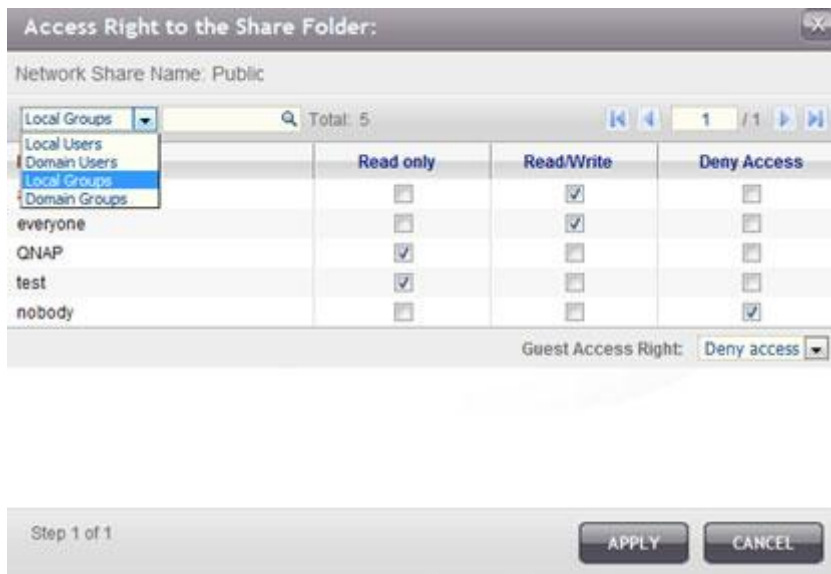


## How to Join QNAP NAS to Microsoft Active Directory (AD)

### What is Active Directory?

Active Directory® is a Microsoft directory used in Windows environments to centrally store, share, and manage the information and resources on your network. It is a hierarchical data centre which centrally holds the information of the users, user groups, and the computers for secure access management. Advantages of joining the QNAP NAS to Active Directory:

- **Convenient account setup:** By joining the NAS to the Active Directory, all the user accounts of the AD server will be imported to the NAS automatically. The AD users can use the same set of user name and password to login the NAS. This saves the time and effort of the server manager to create the user accounts one by one on the NAS.
- **Efficient access control:** The NAS allows the server manager to configure the access rights (read only, read/write, or deny access) to the network share folders for the local/ domain users and local/ domain groups individually.

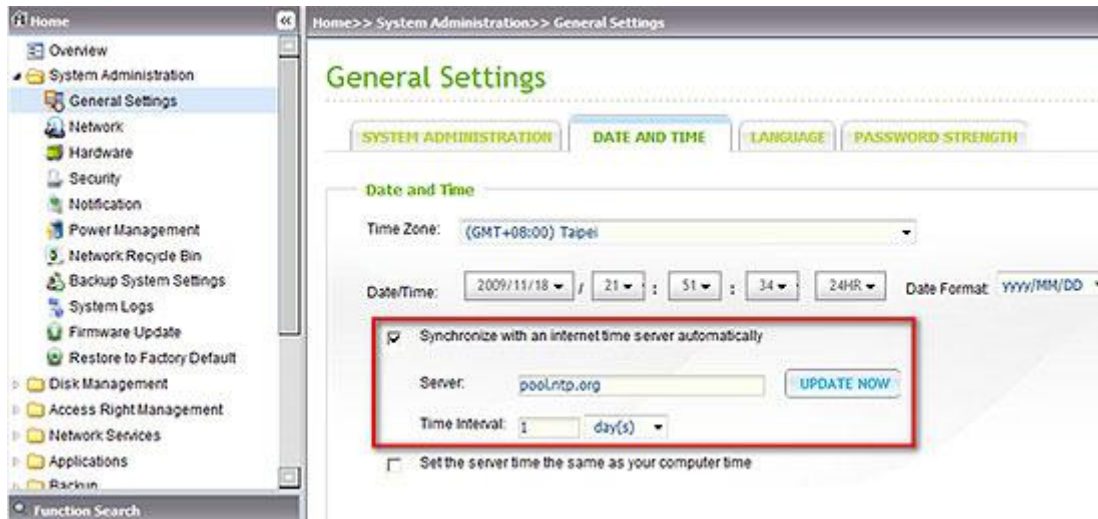


## Prerequisites

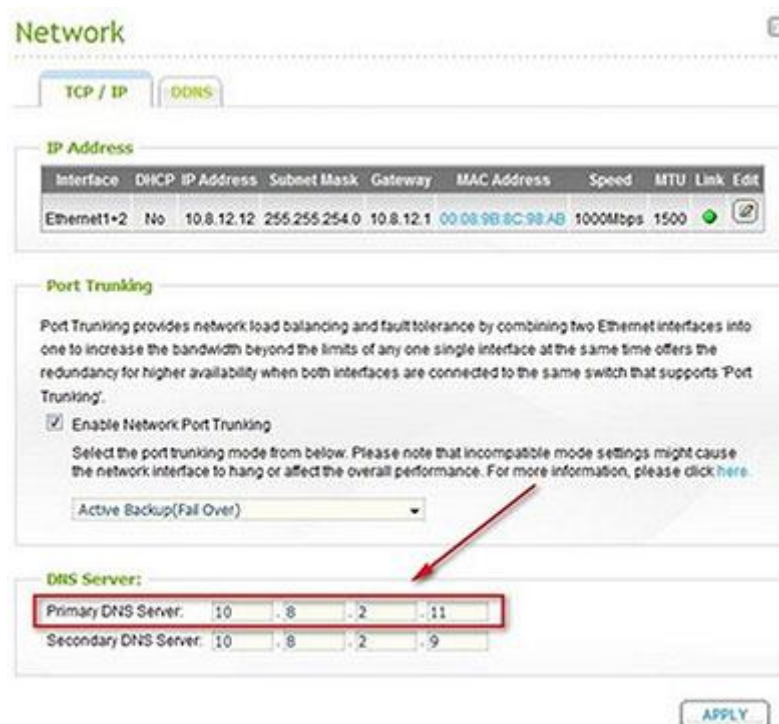
To join the Turbo NAS to an Active Directory with Windows Server 2008 R2, you must update the NAS firmware to V3.2.0 or above. Follow the steps below to join the Turbo NAS to the Active Directory (Windows Server 2008).

### Step 1: Set up the time and DNS information

Login the NAS as an administrator. Go to "System Administration" > "General Settings" > "Date and Time". Set the date and time of the NAS, which must be consistent with the time of the AD server. The maximum time difference allowed is 5 minutes.

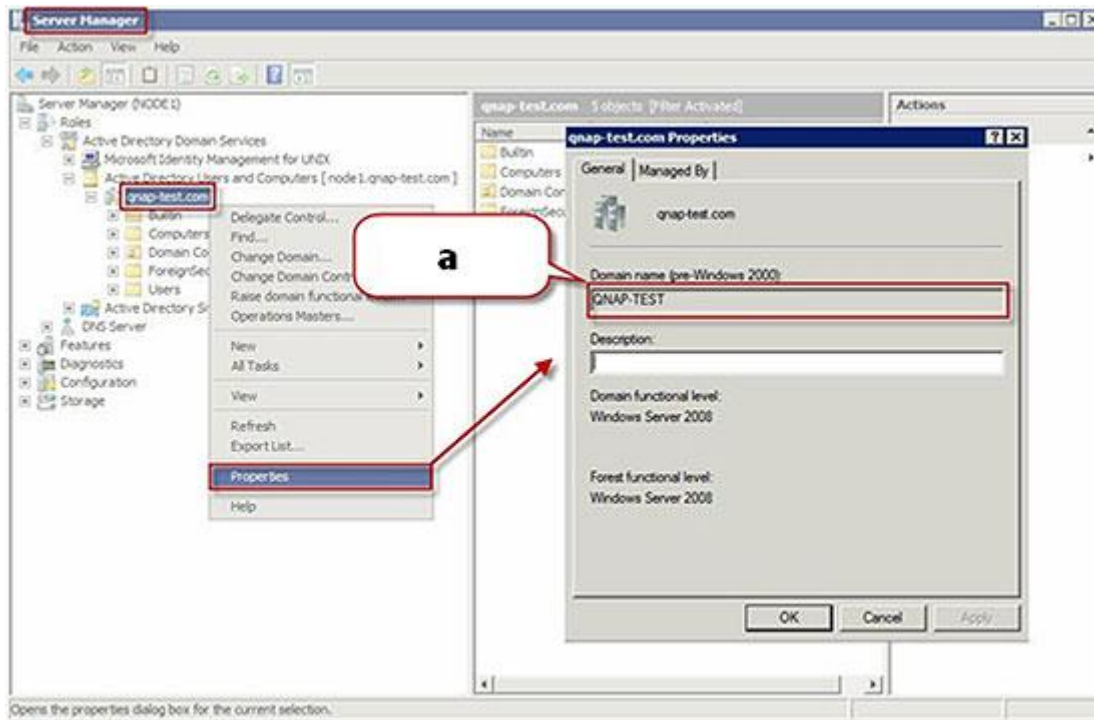


Next, set the IP of the primary DNS server as the IP of the Active Directory server that contains the DNS service. It MUST be the IP of the DNS server that is used for your Active Directory. If you use an external DNS server, you will not be able to join the domain.

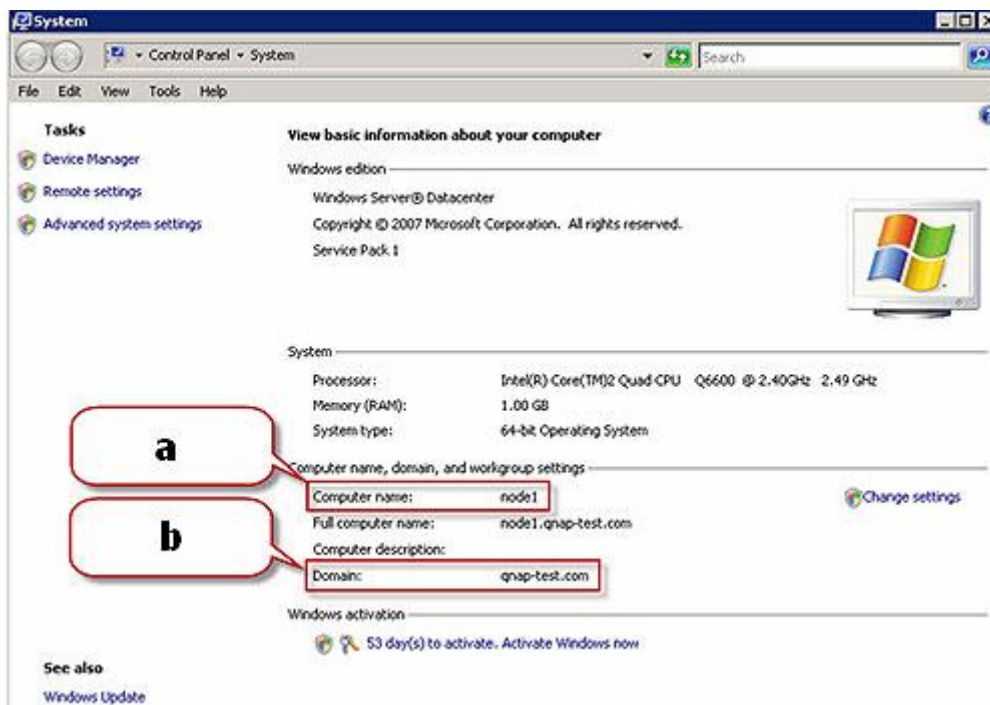


## Step 2:

Check the AD server name and the domain name.



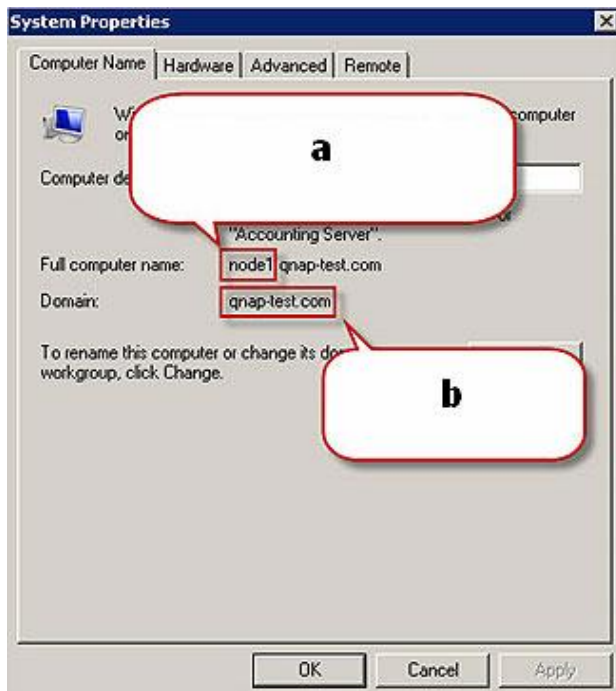
a. Domain NetBIOS Name



a. This is your 'AD Server Name'

b. This is your 'Domain Name'

\*Please note that the above example is based on Windows Server 2008. For Windows Server 2003, please see the image below to check the "AD Server Name".



a. In Windows 2003 Servers, the AD server name is 'node1' NOT 'node1.qnap-test.com'

b. The 'Domain name' remains the same.

### Step 3: Join the Active Directory

Go to "Network Services" > "Microsoft Networking". Enter the information of the AD domain.

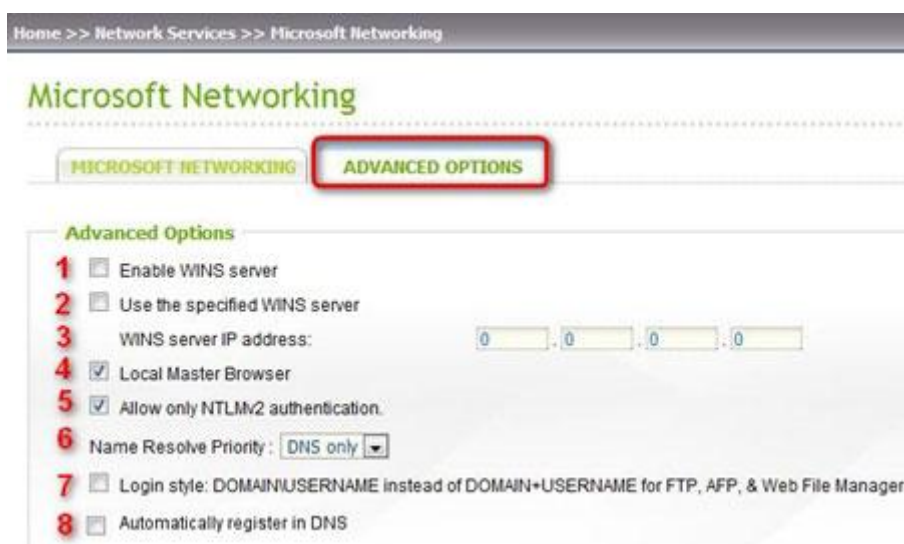


Note:

If you failed to join the AD domain, please review step 1:

- Check the time difference between your NAS and your domain controller.
- Check that the DNS server of your NAS is the same as your Domain Controller DNS. It MUST be your domain DNS server. If you use an external DNS server, you will not be able to join the domain

## Advanced Options tab



WINS Support:

Note that in most cases, it is not necessary to enter WINS server setting. In an Active Directory environment, it is suggested to use a pure DNS name resolution.

1. **Enable WINS server:** This option has to be activated only if you do not have a WINS server on your network, and that some of your computers are on a different subnet. In such case you will have to set up all your computers to use this WINS server. Note that there must be only one WINS server on the network. All the clients have to be configured to use the same WINS server. If you are not sure about the setting, do not enable it.
2. **Use the specified WINS server:** This option should be activated only if you have a WINS server on your network and your NAS should be a WINS client. Enter the IP address of your WINS server
3. If you are not sure about the setting, do not enable it.
4. **Local Master Browser:** This option allows the NAS to be a Local Master Browser which is responsible for maintaining the list of the computers on your network for its workgroup. The name of the NAS workgroup must be the same as that of your computer's workgroup (often called "workgroup"). The setting is enabled by default. If you disable it, the NAS will not maintain the computer list, and the job will be done by another computer on the network. The default setting is enabled.
5. **Allow only NTLMv2 authentication:** This option allows only NTLMv2 authentication and refuses LM and NTLM. If you are not sure about the setting, do not check this option. If you check this option, make sure all the computers on your network can use NTLMv2.
6. **Name Resolution Priority:** This refers to the name resolution on the Windows network. If you enable WINS (option (1) or (2)), you will be able to choose the priority of the name resolution. The default setting is "DNS only" when all WINS settings are disabled. When WINS is enabled, the default setting is "WINS first, then DNS". If you do not have any problems, keep the default values.
7. **Login Style:**  
By default in an Active Directory environment, the username formats for domain users are:
  - \* Windows Shares Access: domain\username
  - \* FTP: domain+username
  - \* Web File Manager: domain+username
  - \* AFP: domain+username

For example, to access a share folder by Web File Manager with a domain user account, you have to authenticate with domain+username if the option is not turned on.

If this option is turned on, all services will use the same username format:

- \* Windows Shares: domain\username

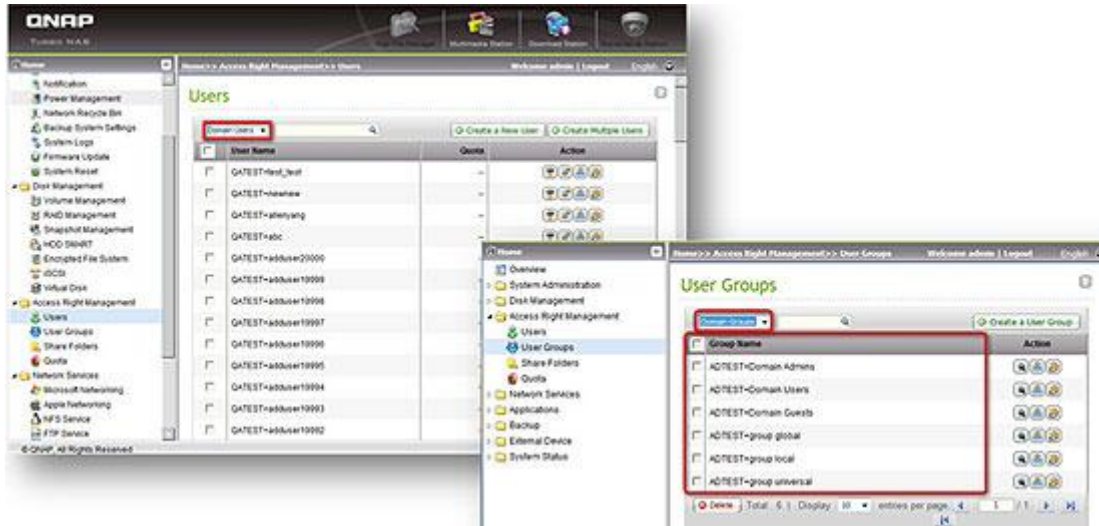
- \* FTP: domain\username
- \* Web File Manager: domain\username
- \* AFP: domain\username

For example, to access a share folder by Web File Manager with a domain user account, you have to authenticate with domain\username if the option is turned on.


- Automatically register in DNS: If this option is turned on, when the NAS is joined in Active Directory, the NAS will register itself automatically in the domain DNS server. This will create a DNS host entry for the NAS in the DNS server. If the NAS IP is changed, the NAS will automatically update the IP with the DNS server.

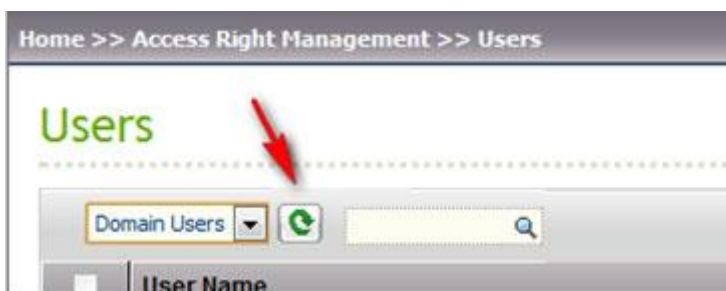
### Verify the settings

To verify that the NAS has been joined to the Active Directory successfully, go to "Access Right Management" > "Users". A list of users and groups will be shown on the "Domain Users" and "Domain Groups" lists respectively.



### Refresh the domain user and user group lists on web interface

If you have created new users or user groups in the domain, you can click the "reload" button (  ) next to "Domain Users" drop-down menu in "Access Right Management" > "Users" or "Domain Groups" drop-down menu in "Access Right Management" > "User Groups" (firmware 3.3 or above). This will reload the user and user group lists from the Active Directory to the NAS. The process is done only for the web interface user list. The user permission settings will be synchronized in real time with the domain controller.



### Notes:

- After joining the NAS to the Active Directory, the local NAS users who have access right to the AD server should use "**NAS\_name\username**" to login; the AD users should use their own user names to login the AD server (Domain\username).
- The local NAS users and the AD users (using domain name and username) are allowed to access the NAS via AFP, FTP and Web File Manager with firmware 3.2.0 and above. However, with firmware prior to 3.2.0, only local NAS users are allowed to access Web File Manager.
- To login the NAS by Windows Explorer, use "Domain\Username" as the login name.

- To login the AFP, FTP and Web File Manager services, use "Domain+Username" as the login name.
- WebDAV can be accessed by local users and groups only.
- For TS-109/209/409/509 series, if the AD Server is based on Windows 2008, the NAS firmware must be updated to v2.1.2 or later.
- To login the NAS by AFP, FTP, and Web File Manager services, use "Domain+Username" as the login name. To be able to use a standard Windows login format (DOMAIN\USERNAME), you have to enable the option "Login style" in the "Advanced Options" tab in "Microsoft Networking" (see above).

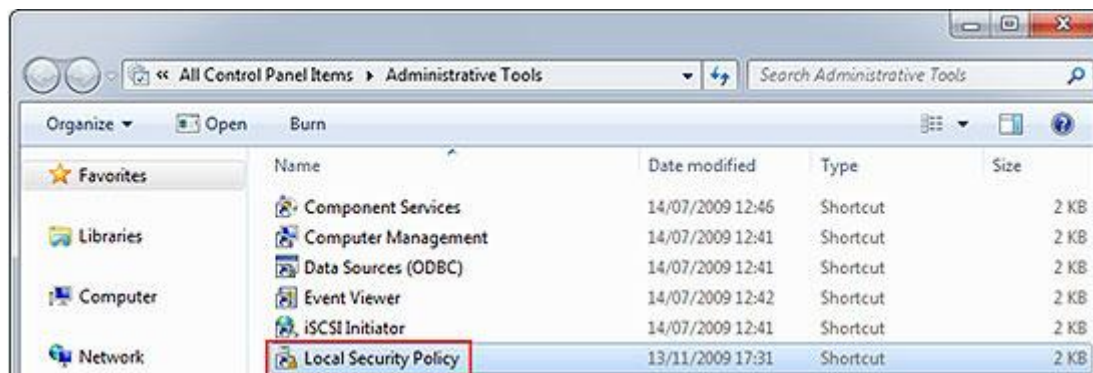
### Note about Windows 7

If you are using a Windows 7 PC which does not belong to an Active Directory, to access a NAS with firmware prior to V3.2.0 and is also an AD domain member, please change the security settings of the client PC as below.

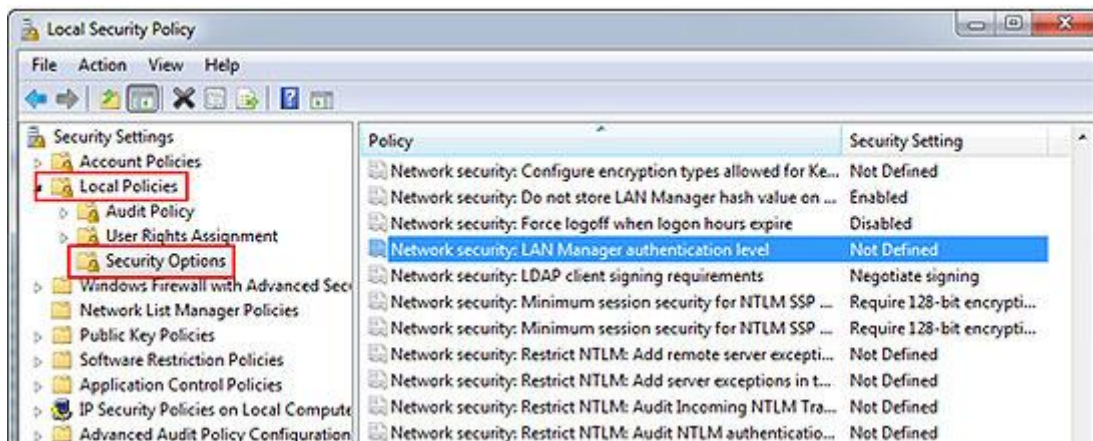
1. On Windows 7, go to "Control Panel" > "All Control Panel Items", and select "Administrative Tools".



2. Select "Local Security Policy".



3. Go to "Local Policies" > "Security Options". Then select "Network security: LAN Manager authentication level".



4. Select the "Local Security Setting" tab, and select "Send LM & NTLMv2 – use NTLMv2 session security if negotiated" from the list. Then click "OK".

