Report Number: C4-005R-01

Guide to Securing Windows NT/9x Clients in a Windows 2000 Network

Network Security Evaluations and Tools Division of the Systems and Network Attack Center (SNAC)

Authors:
Melanie Cook
Heather Eikenberry

Updated: March 6, 2002
Version 1.0.3

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

W2KGuides@nsa.gov

Change Control

Version	Date	Details
1.0.3	6 March, 2002	Added this change control section to track version modifications. On pp. 11, removed reference to a NSA guideline to be released covering migration. Replaced the statement with a reference to Microsoft's white paper, "Planning Migration from Windows NT to Windows 2000". On pp. 11 and 13, added a hyperlink to Microsoft's white paper, "Planning Migration from Windows NT to Windows 2000".

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- This document is current as of March 2002. See Microsoft's web page http://www.microsoft.com/ for the latest changes or modifications to the Windows 2000 operating system.

This Page Intentionally Left Blank

Acknowledgements

The author would like to acknowledge the authors of the "*Guide to Implementing Windows NT in Secure Network Environments*" and the *"Guide to Securing Microsoft Windows NT Networks"* versions 2.0, 2.1, 3.0, 4.0, and 4.1.

The author would like to acknowledge Julie Haney, Paul Bartock, and LT. William Billings for their help reviewing the document.

Some parts of this document were drawn from Microsoft copyright materials with their permission.

Trademark Information

Table of Contents

Table of Figures

Table of Tables

This Page Intentionally Left Blank

Introduction

The purpose of this guide is to inform the reader about Active Directory Client Extensions and recommend security configurations for Windows NT, Windows 98, and Windows 95 clients in a Windows 2000 domain. This guide is not intended to cover migration from a Windows NT network to a Windows 2000 network. For information regarding migration issues, refer to Microsoft's white paper, "Planning Migration from Windows NT to Windows 2000" at http://www.microsoft.com/windows2000/techinfo/planning/activedirectory/plandommig.asp.

The following essential assumptions have been made to limit the scope of this document:

- The network consists of Windows 2000 Domain Controllers and a combination of Windows 2000, Windows NT and Windows 9x clients.
- The latest service packs and hotfixes have been installed on domain controllers, member servers, and workstations.
- All network machines are Intel-based architecture.
- Applications are Windows 2000 compatible.
- Users of this guide have a working knowledge of Windows 2000 and Windows NT installation and basic system administration skills.

Getting the Most from this Guide

The following list contains suggestions to successfully secure the non-Windows 2000 client configurations according to this guide:

WARNING: This list does not address site-specific issues and every setting in this guide should be tested on a non-operational network.

- ❑ Read the guide in its entirety. Omitting or deleting steps can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.
- ❑ Perform a complete backup of your system before implementing any of the recommendations in this guide
- ❑ Follow the security settings that are appropriate for your environment.

About the Guide to Non-Windows 2000 Client Configuration

This document consists of the following chapters:

Chapter 1, "Active Directory Client Extensions and Window 9x and NT 4.0" contains a list of features and capabilities of Active Directory Client Extensions.

Chapter 2, "Securing Windows NT and Windows 9x Clients" contains directions on how to secure Windows NT/9x clients.

Appendix A, "References," contains a list of resources cited.

This Page Intentionally Left Blank

Chapter

1

Active Directory Client Extensions and Windows 9x and NT 4.0

Windows 2000 is designed to support mixed networks with full interoperability. A Windows 2000 network comprising of both 2000 and NT domain controllers operates in mixed mode. Whereas a Windows 2000 network with only 2000 domain controllers can operate in native mode. (Note that the move to native mode cannot be reversed.) A network administrator does not have to upgrade all machines in a domain to take advantage of some of the Windows 2000 features. Through the use of Active Directory Client Extensions, Windows 2000 Server can support Windows NT 4.0, Windows 98, and Windows 95 clients.

Without the client extensions, Windows 2000 servers provide Active Directory transitive trusts, which enable Windows NT and 9x clients to access resources in the Active Directory forest. If clients do not upgrade with the extension, the environment will basically be the same as with a Windows NT server. If a client wants to have increased Active Directory functionality, then the administrator needs to install the Active Directory client extension or upgrade to Windows 2000 Professional.

NOTE: This guide assumes a network made up of Windows 2000 domain controllers, Windows 2000, NT, and 9x clients, and NT member servers.

Active Directory Features Available to Windows NT and 9x Clients

Windows 9x and NT 4.0 clients lack many of the features of Windows 2000 Professional that are related to the Active Directory service. The Active Directory client extension is an upgrade or patch for Windows 9x and NT 4.0, which enables the following Active Directory features:

- **Site Awareness**
  - Capability to log on to the DC that is closest to the client in the network (reduces network traffic).
  - Ability to change password on any Windows 2000 DC, instead of the PDC.
- **Active Directory Services Interfaces (ADSI)**
  - Allows scripting to Active Directory.
  - Provides a common programming API to Active Directory programmers.
- **Default File System (DFS) Fault Tolerance Client**

  - Provides access to Windows 2000 distributed file system fault tolerant and fail-over file shares specified in the Active Directory.
- **Active Directory Windows Address Book (WAB) Property Pages**
  - Allows only the users who have permission to change properties on user objects (e.g., phone number and address) via the user object pages. User object pages can be accessed by clicking the **Start** menu, and then pointing to **Search** and **For People**.
  - Supports display specifiers that allow rendering of new schema elements stored on the user object in Active Directory.
- **NT LAN Manager version 2 Authentication**
  - Takes advantage of the improved authentication features available in NT LAN Manager version 2. Although NTLM2 improves on the features of NT Lan Manager, this authentication protocol is not as strong as Kerberos.

Active Directory Features Unavailable to Windows NT and 9x Clients

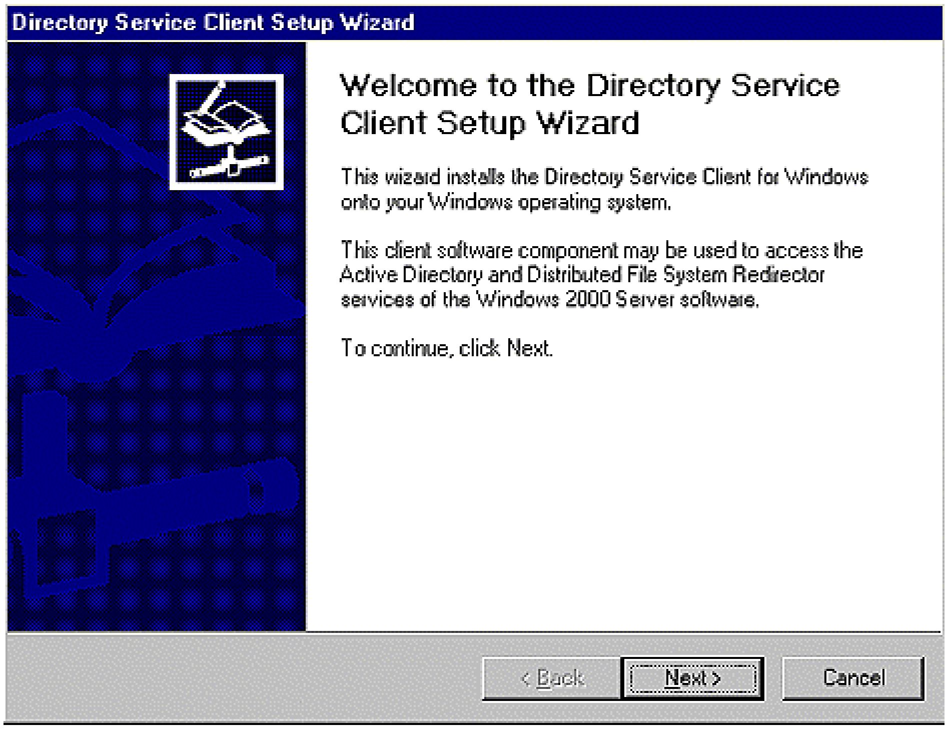
While the client extension will provide added Active Directory features, the following functions will not be added unless there is a compete upgrade to Windows 2000 Professional:

- **No Kerberos Support**
  - The Active Directory client extension does not deliver Kerberos support to Windows 9x and NT 4.0 based clients.
- **No Group Policy or Intellimirror Support**
  - The Active Directory client extension does not deliver Intellimirror™ management technologies or Windows 2000 Group Policy functionality. (This allows the administrator to quickly set up machines according to a predefined template and allows users to access their desktop and applications from any machine in the network.)
- **No IPSEC or L2TP Support**
  - The Active Directory client extension does not deliver advanced Virtual Private Networking (VPN) protocols.
- **No Service Principal Name (SPN) or Mutual Authentication**
  - The Active Directory client extension does not deliver SPN or mutual authentication.

Implementing the Active Directory Client Extensions

The Active Directory client extension can be found on any of the Windows 2000 Server installation CD-ROMs in the \Clients\Win9x folder. Double-click on the DSCLIENT.EXE file to start the setup program. The setup program is guided by a wizard and is easy to navigate. However, Internet Explorer 4.0 or higher must be installed on the client for the Active Directory client extension to install properly.

As shown in **Figure 1**, the first screen is a Welcome screen containing a brief description of the Directory Service Client. Click **Next** to advance through the wizard. Setup will copy some files to the client's hard drive. Restart the computer to complete the installation.



Welcome to the Directory Service Client Setup Wizard

This wizard installs the Directory Service Client for Windows onto your Windows operating system.

This client software component may be used to access the Active Directory and Distributed File System Redirector services of the Windows 2000 Server software.

To continue, click Next.

Figure 1 Directory Service Client Setup Wizard Welcome Screen

Thoughts on Active Directory Client Extension

The Active Directory Client Extension is less invasive than upgrading to Windows 2000 Professional. Unlike an upgrade, which cannot be reversed, the Directory Service Client can be uninstalled. The Add/Remove Programs applet in Control Panel lists Directory Service Client for Windows 9x.

Note that even with the Active Directory client extension, the client is still not a fully functioning member of the Active Directory domain. While the Directory Service Client is useful, it is not as beneficial as upgrading clients to Windows 2000 Professional. Significant architectural advancements have been made in the Windows 2000 Professional client platform. A client extension for Windows 9x and Windows NT 4.0 clients can provide the means to access some of the Active Directory functionality. However, the only way to take full advantage of all the Active Directory features is to upgrade to Windows 2000 Professional.

This Page Intentionally Left Blank

Chapter

2

Securing Windows NT 4.0 and Windows 9x Clients

Windows 2000 networks can operate in either mixed or native mode with Windows NT workstations, member servers, and Windows 9x. Although the backward-compatibility features of Windows 2000 support Windows NT 4.0 and Windows 9x clients, it is recommended to have all Windows 2000 clients. A network of all Windows 2000 clients can take advantage of the enhanced security features of Windows 2000 such as sole authentication using Kerberos version 5, IPSEC, L2TP, and Mutual Authentication. Additionally, the Group Policy Editor tool does not support non-Windows 2000 machines.

However, situations may arise that necessitate the use of legacy operating system clients. Administrative templates and the System Policy Editor (poledit.exe) tools provide policy support to Windows NT 4.0 and Windows 9x clients within Windows 2000 networks. This chapter discusses ways to secure Windows NT 4.0 and Windows 9x clients.

Windows NT 4.0 Workstations

The *Guide to Securing Microsoft Windows NT Networks and Applications*, version 4.1 by the System and Network Attack Center of NSA provides the foundation for securing Windows NT 4.0 clients and will be referenced in this chapter. This guide can be obtained by calling 1-800-688-6115.

Recommendations for securing Windows NT 4.0 workstations include:

- Apply the most current service pack and hotfixes.
- Run the **Workstation.inf** Security Configuration File that is included with the “Guide to Securing Microsoft Windows NT Networks,” version 4.1.
- Follow manual setting recommendations that are also included in the “Guide to Securing Microsoft Windows NT Networks,” version 4.1.
- Install the Active Directory Client Extensions included on the Windows Server CD (Refer to Chapter 1 of this guide.)
- Apply system policy using the System Policy Editor.

More detailed instructions on how to secure Windows NT 4 workstations can be found in the *Guide to Securing Microsoft Windows NT Networks* version 4.1.

NOTE: Native mode does not support Windows NT domain controllers. However, if all domain controllers are Windows 2000, native mode does support Windows NT workstations and Windows NT member servers.

NOTE: The DNS server must be specified before NT clients can be successfully added to the Windows 2000 domain.

Authentication

NTLM version 2 authentication has been available for Windows NT since Service Pack 4 and is supported by Windows 2000 natively. NTLM 2 improves on the authentication and session security mechanisms of LAN Manager and NTLM version 1. In a Windows 2000 domain, the domain controller that is acting as the PDC emulator acts as the master browser for NT clients and provides NTLM authentication services. The following registry setting will force NT clients to use only NTLM 2 for authentication.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Control\LSA
Name:	LMCompatibilitylevel
Type:	REG_DWORD
Value:	5

WARNING: Setting this value higher than 1 will prevent connection to systems that support only LM authentication (Windows 95/98 that do not have Directory Services Client installed).

WARNING: Setting this value higher than 2 wlll prevent connection to Windows NT 4.0 systems with Service Pack 5 or lower since NTLM version 2 is a Service Pack 6a feature.

Table 1 shows the available authentication options.

NTLM Setting	Clients	Domain Controllers
Level 0 Send LM and NTLM response; never use NTLM 2 session security.	Use LM and NTLM authentication, and never use NTLM 2 session security.	Accept LM, NTLM and NTLM 2 authentication.
Level 1 Use NTLM 2 session security if negotiated.	Use LM and NTLM authentication; use NTLM 2 session security if the server supports it.	Accept LM, NTLM, and NTLM 2 authentication.
Level 2 Send NTLM response only.	Use only NTLM authentication, and use NTLM 2 session security if the server supports it.	Accept LM, NTLM, and NTLM 2 authentication.
Level 3 Send NTLM 2 response only.	Use NTLM 2 authentication and NTLM 2 session security if the server supports it.	Accept LM, NTLM, and NTLM 2 authentication.
Level 4 Domain Controllers refuse LM responses.	Use NTLM 2 authentication, and use NTLM 2 session security if the server supports it.	Accept NTLM and NTLM 2; refuse LM authentication.
Level 5 Domain Controllers refuse LM and NTLM responses.	Use NTLM 2 authentication, and use NTLM 2 session security if the server supports it.	Accept only NTLM 2; refuse LM and NTLM authentication.

Table 1 – LMCompatibilityLevel Settings

Windows 95 and Windows 98 Clients

Because of the inherent non-secure nature of Windows 9x clients, it not recommended to use Windows 9x. At a minimum, use Windows NT 4.0 workstations. Ultimately, it is recommended to have only Windows 2000 workstations and operate in native mode. However, if Windows 9x clients exist on the network, configure these machines to restrict network access. The following recommendations describe how to secure Windows 9x clients during system boot and network authentication. In addition, System Policy settings are recommended.

Because Windows 9x use the FAT file system rather than NTFS, access to directories and files cannot be protected with access control lists (ACLs). Therefore, Windows 9x clients should be located in a secure location with controlled physical access. It is also recommended that all current security patches be applied to Windows 9x clients. Patches can be downloaded from www.microsoft.com/downloads/search.asp

Authentication

With the introduction of the Active Directory Service Client, NTLM 2 support can be extended to Windows 95/98 clients. Dsclient.exe installs the following system files that support NTLM 2:

- Secur32.dll
- Msnp32.dll
- Vredir.vxd
- Vnetsup.vxd

If Dsclient is uninstalled, the NTLM 2 system files are not removed because they provide security-related fixes.

NTLM 2 session security encryption is restricted to a maximum key length of 56-bits by default. The optional 128-bit key length is automatically installed if the system satisfies United States export regulations.

❑ Install Internet Explorer 4.x or 5 and upgrade to 128-bit secure connection before installing the Directory Services Client.

❑ Verify the installation version by locating the Secur32.dll file, clicking Properties and the Version tab. The description for the 56-bit version is “Microsoft Win32 Security Services (Export Version)”. The description for the 128-bit version is “Microsoft Win32 Security Services (US and Canada Only).”

To enable NTLM 2 authentication on Windows 95/98 clients modify the following registry key (create the LSA key if it is not present):

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Control\LSA
Name:	LMCompatibility
Type:	REG_DWORD
Value:	3

Table 2 shows the available LMCompatibility settings.

NTLM Setting	Clients	Domain Controllers
Level 0 Send LM and NTLM response; never use NTLM 2 session security.	Use LM and NTLM authentication, and never use NTLM 2 session security.	Accept LM, NTLM and NTLM 2 authentication.
Level 3 Send NTML 2 response only.	Use NTLM 2 authentication; use NTLM 2 session security if the server supports it.	Accept LM, NTLM, and NTLM 2 authentication.

Table 2 – LMCompatibility Settings

NOTE: The valid range is 0,3. This value specifies the mode authentication and session security to be used for network logons. It does not affect interactive logons.

For information on enabling NTLMv2 on Windows clients, see How to Enable NTLM 2 Authentication for Windows 95/98 Clients, KB Q239869.

NOTE: If Windows 95/98 clients must authenticate on the network, Directory Services Client must be installed on Windows 95/98 clients in order to support NTLMv2. See Appendix A of “The Guide to Securing Microsoft Windows NT Networks and Applications” version 4.1 for more information on this topic.

Group Policy

Group Policy in Windows 2000 does not support non-Windows 2000 clients. Policy support for Windows NT and Windows 9x clients is provided via the use of administrative templates (.adm files) and the System Policy Editor (poledit.exe). The administrative templates (Common.adm, Windows.adm, and Winnt.adm) are for setting policy for Windows NT and 9x clients. They are used with the System Policy Editor and should not be loaded into Group Policy. Windows NT clients need to have the Ntconfig.pol file (config.pol for Windows 9x) created on the client machine. The .pol file is then copied to the domain’s netlogon share (%systemroot%\SYSVOL\sysvol\<*domain name*>\SCRIPTS).

There are several benefits to Group Policy over System Policy. Group Policy refreshes whenever the policy changes and it is possible to disable unused parts of the Group Policy Object to speed the logon process. When upgrading computer accounts to Windows 2000, be aware of persistent registry settings from the System Policy. For example, the logon banner is handled differently in Windows 2000 and Windows NT. The logon banner in NT is part of the administrative template whereas the logon banner is one of the security settings in Windows 2000. To avoid any such problems associated with persistent registry settings, it is recommended to give clients a fresh install of the Windows 2000 operating system.

NOTE: If both system policy and group policy are enabled on the Windows 2000 network, system policies will overwrite the Windows 2000 Group Policies. Ensure that both the system policy and group policy match.

System Policy Editor

The System Policy editor is available for Windows NT 4.0 and Windows 95/98. It provides the administrator with a graphical interface that can be used to enforce system policies.

Settings can be applied at a User or Computer level. The **Enable User Profiles** setting must be enabled in the System Policy Editor. In Windows 95 this setting is located in **Local Computer→System→Enable User Profiles**. In Windows 98 this setting is located in **Default Computer→System→Enable User Profiles**.

The System Policy Editor (Poledit.exe) must be installed on Windows 9x before it can be used. It is available in the **Admin\Apptools\Poledit** folder on the Windows 95 CD-ROM. The System Policy Editor for Windows 98 is in the **Tools\Reskit\Netadmin\Poledit** folder on the Windows 98 CD-ROM. Use the Add/Remove Programs tool in Control Panel to install the System Policy Editor.

NOTE: The System Policy Editor should be removed after it is used to configure the system policy for a client.

Hotfix

"Directory Service Client may not be Installed on Windows NT 4.0 SP6a with Certain Hotfixes"

Installing directory service client (Dsclient.exe) on Windows NT with SP6a applied may not be successful due to previously installed hotfixes. The setup error that may be generated follows:

Setup cannot detect the Windows NT4 with SP6a or higher operating system which is required to install the Directory Service Client. The installation will terminate.

A fix is available from Microsoft. More information is available in Microsoft article, Q293322.
http://support.Microsoft.com/support/kb/articles/Q293/3/22asp

This Page Intentionally Left Blank

Appendix

A

References

"Active Directory Client Extensions for Windows 95, Windows 98 and Windows NT 4 Workstation," Microsoft technical paper, 2000.

Ahmad, Zubair, "Mixed Mode vs. Native Mode", Windows 2000 Magazine, August 30, 1999.

Bartock, Paul, et. al., *Guide to Securing Microsoft Windows NT Networks version 4.1*, National Security Agency, September 2000

"How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT," Microsoft Knowledge Base Article Q239869, http://support.microsoft.com/support/kb/articles/Q239/8/69.asp, 2001.

Kling, Judy. "Supporting Clients in your Windows 2000 Environment," Exploring Windows NT, ZD Inc., December 15, 1999.

"Planning Migration from Windows NT to Windows 2000", Microsoft white paper, http://www.microsoft.com/windows2000/techinfo/planning/activedirectory/plandommig.asp, 2000.

Ricadela, Aaron. "Microsoft Prepping Client Extensions for Windows 2000." Information Week, 24 Nov 1999.

Windows 2000 Resource Kit documentation, Microsoft, 2000.