

NCD WinCenter NIS Logon Utility Startup Guide

Copyright

Copyright © 2000 by Network Computing Devices, Inc. (NCD). The information contained in this document is subject to change without notice. Network Computing Devices, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material. This document contains information which is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of Network Computing Devices, Inc.

Trademarks

Network Computing Devices is a registered trademark of Network Computing Devices, Inc. ThinSTAR and ThinPATH are trademarks of Network Computing Devices, Inc. Explora, Explora Pro, ECX, HMX, HMXpro, HMXpro24, WinCenter, WinCenter Pro, WinCenter Connect, NCDnet, and NCDware are trademarks of Network Computing Devices, Inc. XRemote is a registered trademark of Network Computing Devices, Inc.

Other product and company names mentioned herein are the trademarks of their respective owners. All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. NCD cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Disclaimer

THE SOFTWARE PRODUCTS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NCD FURTHER DISCLAIMS ALL WARRANTIES, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE SOFTWARE PRODUCTS AND DOCUMENTATION REMAINS WITH THE END USER.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL NCD OR ITS SUPPLIERS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCTS OR DOCUMENTATION, EVEN IF NCD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Revision History

January, 2000. NCD WinCenter NIS Logon Utility Startup Guide. Document 9300898, Rev. A.

Contents

NCD WinCenter NIS Logon Utility	1
Features	1
Installing Software	2
Functionality	3
Implementation Options and Procedures	6
Starting the NCD WinCenter NIS Logon Utility	9
NIS Domains	9
NIS Databases	11
User Properties	13
Logons	17
Groups	20
Windows NT Domain Access	23
Configuring Windows NT Domain Data	24
Testing User Accounts	25
Event Log	26
Index	27

NCD WinCenter NIS Logon Utility

NCD WinCenter NIS Logon Utility is an administrative tool that lets Windows NT use logon data from a UNIX network. The utility, referred to as the NIS Logon Utility, makes it easier to introduce a Windows NT server into a UNIX network.

As an administrator, you can configure the NIS Logon Utility to use UNIX NIS data to validate users who want to log on to a Windows NT server. You do not have to create user accounts on the Windows NT server manually.

Features

The NIS Logon Utility offers the following features:

- Access management
 - Validating user accounts using the NIS password database
 - Regulating logons to multi-user sessions and the console by account type (sessions are identified as WinStations in the user interface)
 - Managing NIS users' properties
- Automatic data creation and mapping
 - Using UNIX NIS database information to create accounts on the Windows NT server
 - Mapping NIS groups to Windows NT groups (supported for NIS, and NIS+ running in YP compatibility mode)
 - Accessing an NIS user's home directory automatically when an automount database is identified and NFS or other UNIX host access software is installed
- Optionally, using NIS+ to authenticate users via shadowed passwords

Installing Software

The software setup includes installation files for the following platforms and installs files as appropriate for the operating system being used:

- NCD WinCenter 3.1
- Citrix WinFrame 1.6, 1.7, and 1.8
- WinDD 3.5
- Microsoft Windows NT 3.51 and Windows NT 4.0 (including Terminal Server)
- Microsoft Windows 2000

To install software on the server, you need:

- Local administrative rights to install or configure the software
- Domain administrator rights, if the Windows NT server is a member of a domain

To install the utility:

1. Log on to the server as the administrator and insert the CD.
2. Run **Setup** and select the **Install** or **Update** option, then click **Next**.
3. Enter licensing information, then click **Next**.

New installation. The license key is on a label on the CD case. Type the 22-character key, including the dashes (-), in the **License installation**.

Upgrade. The existing license key is displayed.

4. Configure settings, then click **Next** to complete the installation.
The new installation takes effect when you restart your computer.

To upgrade a license key:

1. Log on to the server as the administrator.
2. Select **Start > Programs > NCD Software > NCD License Manager**. (For Windows NT 3.51, go to the group the software was installed in. By default, this is NCD Software.)
3. Enter the new license keys. These replace the current keys.

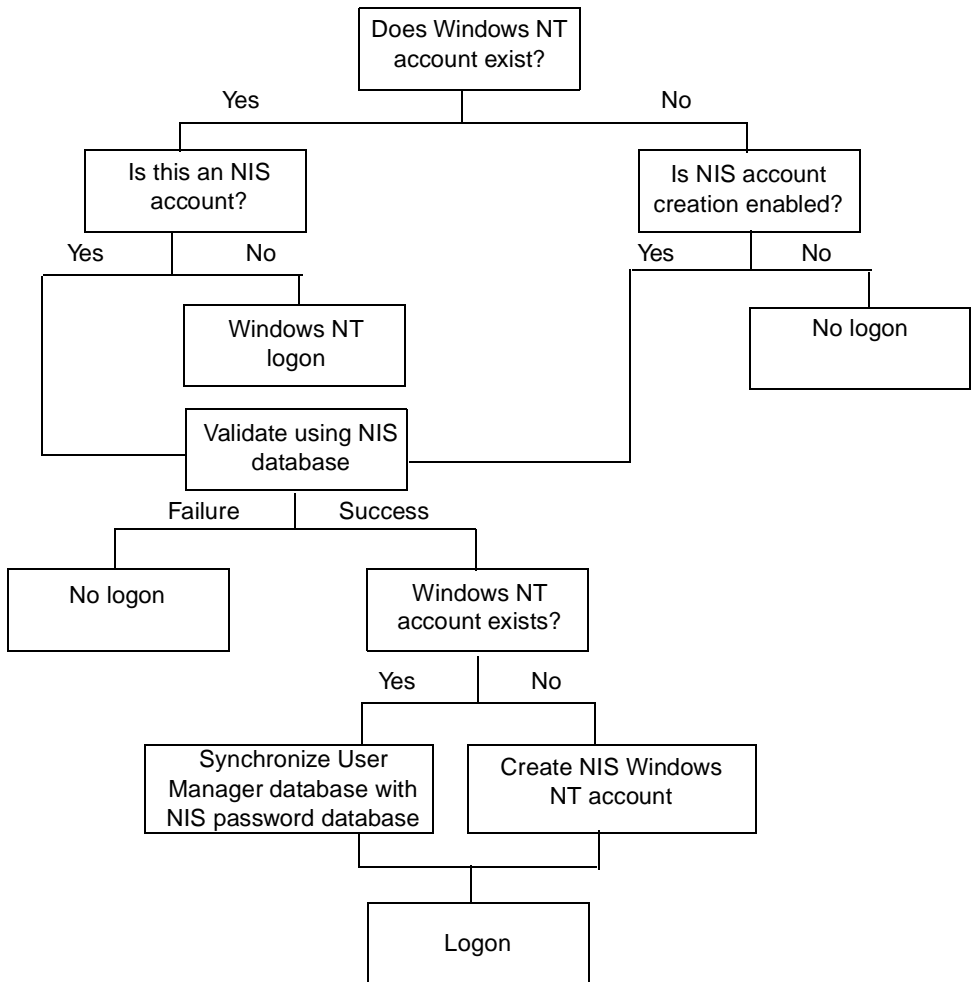
Functionality

This section describes functionality, including features, user validation, and the relationship between NIS accounts and Windows NT accounts.

Note Some UNIX servers use NIS to authenticate users; others use NIS+. This document uses NIS for both unless a distinction is necessary.

User Validation

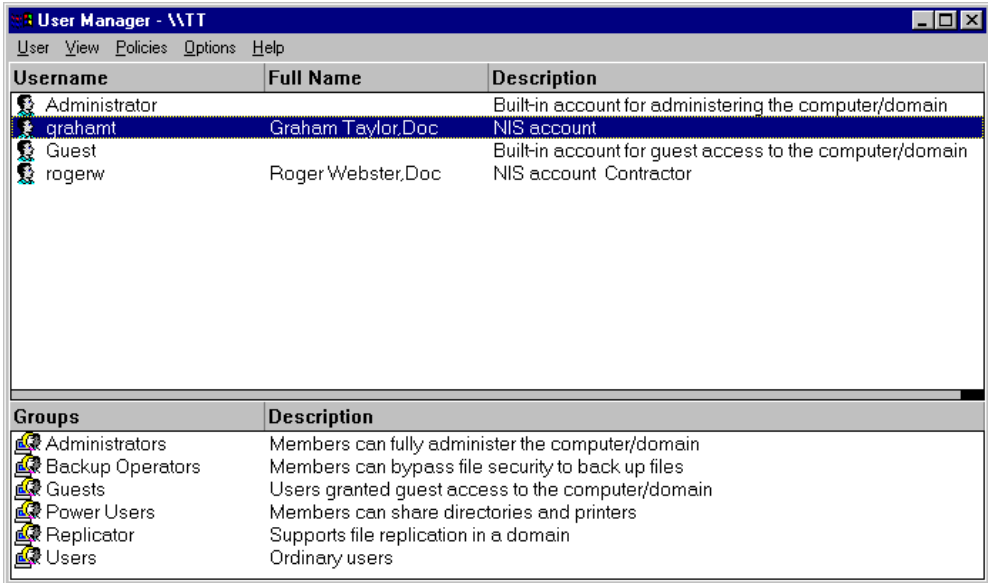
The logon process is as follows when the NIS Logon Utility is enabled.



NIS Accounts and Windows NT Accounts

UNIX systems keep user logon data for domains in NIS databases. Windows NT needs the same kinds of data for its logons.

The Windows NT User Manager has the following user properties:



The NIS Logon Utility extracts information from the existing NIS data so that you do not have to enter it manually.

Data for the **Username** and **Full Name** fields comes from the NIS password database.

You can convert an existing Windows NT account to an NIS account by inserting **NIS account** in the **Description** field of the Windows NT User Manager account. The **NIS account** text must be at the beginning of the field. If you need to include descriptive text, put a space before any additional text.

During each NIS logon, the Windows NT User Manager database is synchronized with the NIS database. The NIS Logon Utility uses data from the NIS database to update the **Full name** and **Password** fields in User Properties.

Note If you press **Ctrl+Alt+Delete** in Windows NT (or select **Program Manager > File > WinFrame Security** with Citrix WinFrame 1.6, 1.7, or 1.8) and change the user's password in Windows NT, it also changes in the NIS password database. If you change it using any other mechanism, the NIS password database does not change. Changing NIS passwords is supported for NIS and NIS+ running in YP compatibility mode. Changes made through Windows NT may not be reflected until the NIS domain is synchronized.

If NIS groups are enabled, the NIS account is added to the mapped Windows NT group.

Implementation Options and Procedures

The NCD WinCenter NIS Logon Utility gives you options for replicating NIS accounts for Windows NT. These options become available when you enable NIS authentication on the **NIS** tab. The following table summarizes implementation options.

Implementation Options		
Task	Feature	How to Do It
Create Windows NT user accounts from the NIS domain automatically	Automatic account creation and configuration	<p>On the NIS tab, identify which NIS domain and server authenticate logons. Correct information about the default NIS databases on the Database tab if necessary. On the User Properties tab, enter user information.</p> <p>Logging on to:</p> <ul style="list-style-type: none"> ■ A Windows NT domain results in an NT account being created in the Windows NT domain, if the NT Domain tab has name and password information for a domain administrator account. <p>This allows someone with domain administrator rights to add or change Windows NT user account information on the domain.</p> <ul style="list-style-type: none"> ■ The local system results in a local Windows NT account. <p>To prevent users from logging on to the local machine, select Restrict access to domain logons only on the NT Domains tab.</p>

Implementation Options (<i>continued</i>)		
Task	Feature	How to Do It
Change passwords	Windows NT or UNIX change password functions (NOT the Windows NT User Manager)	<p>You can change a password administratively only in the UNIX domain. Password changes made through the Windows NT User Manager are not sent to the UNIX NIS domain.</p> <p>Using the Change Password option from the Windows NT Security dialog changes the user's password on both the NIS domain and Windows NT. If a user changes a password only on the NIS domain using yppasswd, the new password is set in the user's Windows NT account information at the next logon.</p>
Automount home directories	User properties; for connect to, use password database	<p>On the User Properties tab, select a drive letter and then check the Use Password Database option. This enables automounting, which parses and sets the UNIX home directory. Automounting must be fully configured on the UNIX NIS domain. Also, UNIX host access software needs to be installed—for example, a Windows NT NFS client or SAMBA on the needed UNIX host(s).</p>
Run logon scripts or set a profile location other than the default when users validated by NIS log on	User properties	<p>If you set a logon script file name, the file needs to be located in the usual Windows NT location: <code>%SYSTEMROOT%\system32\Repl\Import\Scripts</code> and it needs to have the .bat or .cmd suffix.</p> <p>Profile location paths can use the <code>%username%</code> variable to configure profile locations for each user. Use the Set Paths at Every Login option to check and update these settings at each logon.</p>

Implementation Options (<i>continued</i>)		
Task	Feature	How to Do It
Use UNIX configured groups for Windows NT access permissions	Groups	Enable group mapping on the Groups tab. Map at least one NIS group to an existing Windows NT group. The rest of the NIS groups will be created in Windows NT. Use those groups to assign permissions for the new Windows NT NIS users for resources located in the Windows domain or server.
Restrict access for a group of users to a Windows NT system running the NIS Logon Utility	Groups or logons	<p>You can restrict access by:</p> <ul style="list-style-type: none"> ■ Assigning people to groups, then using the Groups tab to define which groups can log on to the Windows NT system. ■ Selecting options on the Logon tab to specify which types of accounts can log on to Windows NT from the console or a WinStation. ■ Letting approved users log on, but selecting the Don't Automatically Create Accounts option on the Login tab to disable creating additional automatic accounts on the server. ■ Selecting the option on the NT Domains tab that restricts access to domain logons only; users are not granted access to accounts on the local server.
Automatically replicate user account changes to all accounts	Set at every login	<p>When making changes, usually to the User Properties tab, you have two options:</p> <ul style="list-style-type: none"> ■ Set at NT Account Creation Time Only. This sets the user account information only when the Windows NT account is created. After that, it synchronizes only the NIS password from the NIS database. ■ Set at Every Login. This synchronizes the user's Windows NT account information with NIS account information at every logon.

Starting the NCD WinCenter NIS Logon Utility

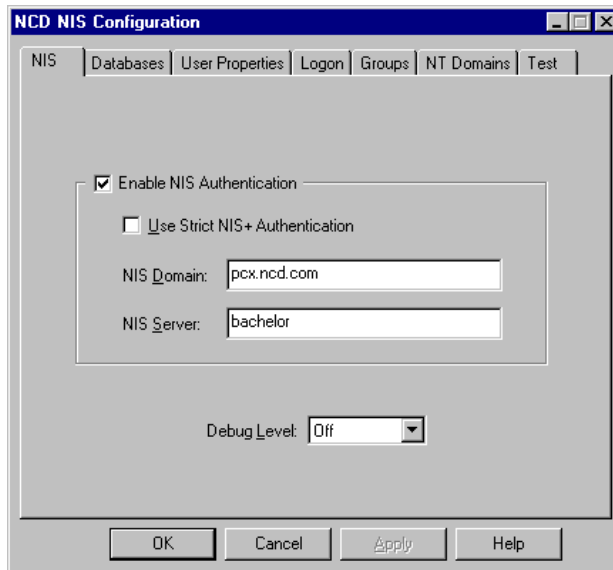
To start the NIS Logon Utility on Windows NT 4.0 or Windows 2000, select **Start > Programs > NCD Software > NIS Logon Utility**.

To start the NIS Logon Utility on Windows NT 3.51, open the installation group (NCD Software, by default), then double click on **NIS Logon Utility**.

Note NCD recommends that you reboot the server after applying any changes to the NCD WinCenter NIS Logon Utility.

NIS Domains

The **NIS** tab identifies the NIS domain and server whose data is used to validate NIS users who log on to a Windows NT server.



To select an NIS domain and server:

1. Start the NCD WinCenter NIS Logon Utility.
 - On Windows NT 4.0 or Windows 2000, select **Start > Programs > NCD Software > NIS Logon Utility**.
 - On Windows NT 3.51, open the installation group (NCD Software, by default), then double click on **NIS Logon Utility**.

2. Select the **NIS** tab and enter the following information, then click **OK**.

— **Enable NIS**

You can set NIS configuration values after enabling NIS, then edit them when your environment changes. If you do not use the NIS Logon Utility, standard Windows NT processes validate users.

— **Use Strict NIS+**

Check this if your NIS+ server is running strict NIS+ (that is, it is an NIS+ server **not** running in YP compatibility mode).

Note To validate shadowed passwords when using NIS+, give the **nobody** class permission to read the **passwd** table on the NIS+ server. Without read permission, user authentication fails and the string *NP* (for “No Permissions”) is returned instead of encrypted passwords.

— **NIS Domain**

The NIS domain name is not related to the Windows NT domain name. Often, though not always, the NIS domain name and the DNS domain name are the same and the UNIX system administrator can provide the name. If your server is running NIS+, end the domain name with a period (.), for example:

pcx.ncd.com.

— **NIS Server**

Enter **broadcast** to broadcast on the local subnet for an NIS server for the specified NIS domain or enter the server name.

Under NIS+, the server name is required; “broadcast” is invalid.

— **Debug level**

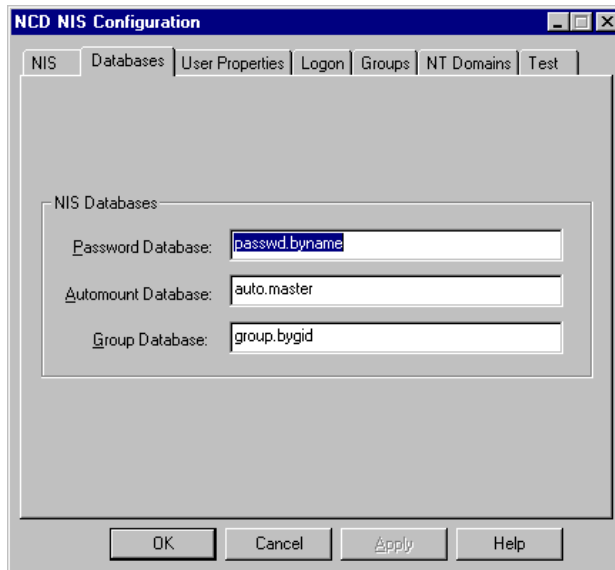
The Event Log, described on page 26, keeps a record of events. Here, choose the level of information for the log.

Off	No debug logging occurs.
Errors	Logs errors.
Warnings	Logs warnings and errors.
Information	Logs information, warnings, and errors.

NIS Databases

The NIS Logon Utility uses information in NIS databases (also called maps or tables) to manage NIS user accounts. The three NIS databases are the password database, the automount database, and the group database.

You specify these databases on the **Database** tab, as in the following example.



To select NIS databases:

1. Start the NCD WinCenter NIS Logon Utility.
 - On Windows NT 4.0 or Windows 2000, select **Start > Programs > NCD Software > NIS Logon Utility**.
 - On Windows NT 3.51, open the installation group (NCD Software, by default), then double click on **NIS Logon Utility**.

2. Select the **Database** tab and make selections for the NIS server specified on the **NIS** tab.

- **Password Database**

Contains password information.

For NIS+, the default is **passwd.org_dir**. For NIS, the default is **passwd.byname**.

- **Automount Database**

Contains information for mounting user home directories.

If you have automounting fully configured on the UNIX NIS domain and an NFS client is on the Windows NT server or an SMB server is on the required UNIX host, you can automatically mount a user's home directory.

For NIS, the default table is **auto.master**. For NIS+, the default table is **auto_master**. The database may be in Sun or AMD format.

The automount database is only used if **Use password database** is selected on the **User Properties** tab.

- **Group Database**

Contains group information. For NIS, the default table is **group.bygid**. For NIS+, the default table is **group.org_dir**. Group information is only supported by NIS+ running in YP compatibility mode.

If **NIS Groups** is enabled on the **Groups** tab, you can enable groups by setting **Group Database** to the name of the file on your NIS or NIS+ server.

User Properties

The **User Properties** tab has user information for the Windows NT User Manager.

Configuring user properties involves:

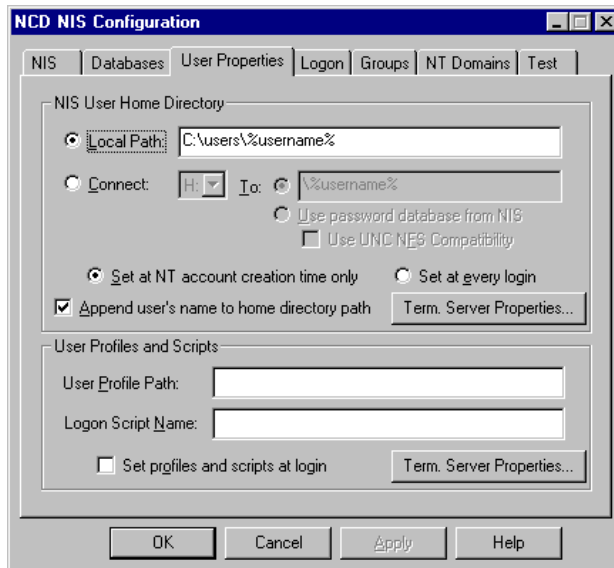
- Identifying a user's home directory
- Specifying when to set up the directory

You have two choices:

- Set the home directory at Windows NT account creation time only, then maintain the records through the Windows NT User Manager for Domains.
- Reapply the NCD configuration values each time a user logs on.

- Completing user profiles

You configure user properties on the following tab.



If you select **Set at every login**, the NIS Logon Utility reapplies the values on this tab each time an NIS user logs on. This overwrites any information that is contained within the Windows NT User Manager.

To configure user properties:

1. Start the NCD WinCenter NIS Logon Utility.
 - On Windows NT 4.0 or Windows 2000, select **Start > Programs > NCD Software > NIS Logon Utility**.
 - On Windows NT 3.51, open the installation group (NCD Software, by default), then double click on **NIS Logon Utility**.
2. Select the **User Properties** tab and provide information about home directories for the user's profile in the Windows NT User Manager. You can specify a local path or connect to a network server.

— **Local Path**

You can enter a path on a local machine. If you select **Append user's name to home directory path**, the NIS user's name (*%username%*) is appended to the path at logon. Otherwise, the explicit path is the home directory for all users.

— **Connect/To**

This maps home directories of all NIS users to a network path using the specified drive letter. You can enter a network path or resolve home directories automatically, as long as automounting is fully configured in UNIX.

If connecting to a network path, enter the pathname. If **Append user's name to home directory path** is checked, *%username%* is appended. *%username%* is a variable that will be replaced by the NIS user's name. If the name is not appended, the named path is the home directory for all users.

Commands such as Samba's HOME keyword resolve the home directory automatically. To allow this, use the keyword in the network path field (for example, "**Samba_Server\HOME**"). Do not check **Append user's name to home directory path**.

— **Use password database from NIS**

Select this to automatically mount the user's home directory as specified in the **Database > Automount Database** file. An NFS client must be installed on the Windows NT server or an SMB server must be installed on the required UNIX host.

— **Use UNC NFS Compatibility**

By default, the format for the automount directory is `\\server\home\directory`. If you select this option, the mixed slash format is used (`\\server\/home\directory`).

— **Set at NT account creation only**

Sets home directory information only when the account is created. If **Append User** is checked, the actual username replaces the `%username%` variable at logon.

Select **Set at NT account creation time only** if you want to update Windows NT with information about users' home directories only when the Windows NT account is created.

— **Set at every login**

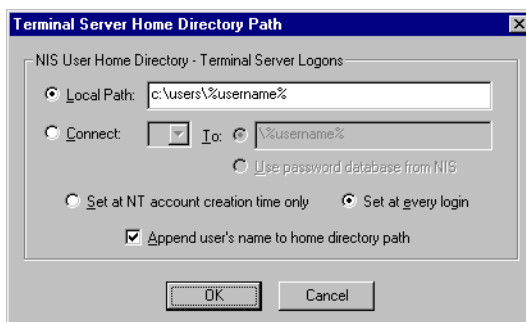
Sets or updates home directory information when the Windows NT account is automatically created and every time the NIS user logs on to this Windows NT server.

— **Append user's name to home directory path**

If checked, the actual username replaces the `%username%` variable at logon.

— **Terminal Server Properties**

This button—available only on Windows NT servers running Terminal Services—lets you configure home directory settings specific to Terminal Servers. Examples of Windows NT servers running Terminal Services are NT Server 4.0, Terminal Server Edition and Windows 2000 Server with Terminal Services installed.



3. Complete information about the user profile.

— **User Profile Path**

This is the pathname of a user profile kept somewhere other than the default location.

— **Logon Script Name**

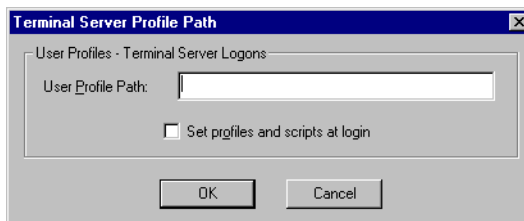
Logon scripts are **.bat** or **.cmd** files, kept in the standard location, which is `%SYSTEMROOT%\system32\Repl\Import\Scripts`.

— **Set Profiles and Scripts At Logon**

Check to apply the user profile path and logon script to the NIS user's account at each logon. Uncheck to apply profiles only when a new Windows NT account, validated by NIS, is created.

— **Terminal Server Properties**

This button—available only on Windows NT Servers running Terminal Services—lets you configure profile settings specific to Terminal Servers. Examples of Windows NT servers running Terminal Services are NT Server 4.0, Terminal Server Edition and Windows 2000 Server with Terminal Services installed.



Logons

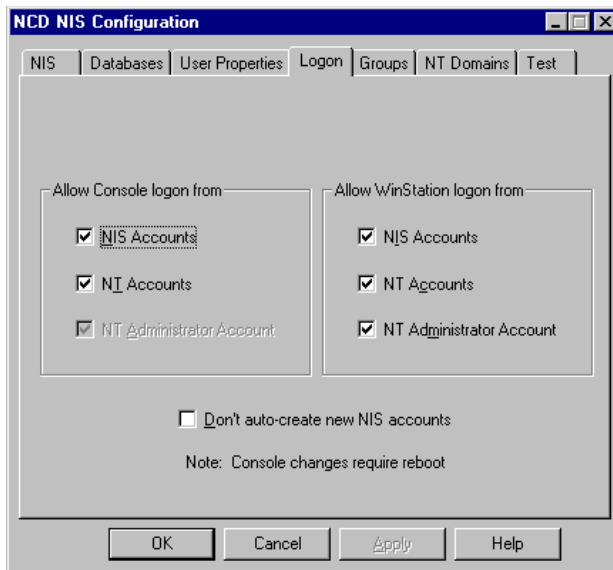
Logon options for Windows NT logons validated by NIS include:

- Whether different types of accounts (NIS, Windows NT, or Windows NT Administrator) can log on from the console or a WinStation
- Whether an account is created automatically when an NIS user logs on to the Windows NT server the first time

Configuring Logons by Account Type

On the **Logon** tab, you can specify whether NIS accounts, Windows NT accounts, or Windows NT Administrator accounts can log on from the console or a WinStation. The following examples show how the information differs for multi-user Windows NT systems and standard Windows NT systems.

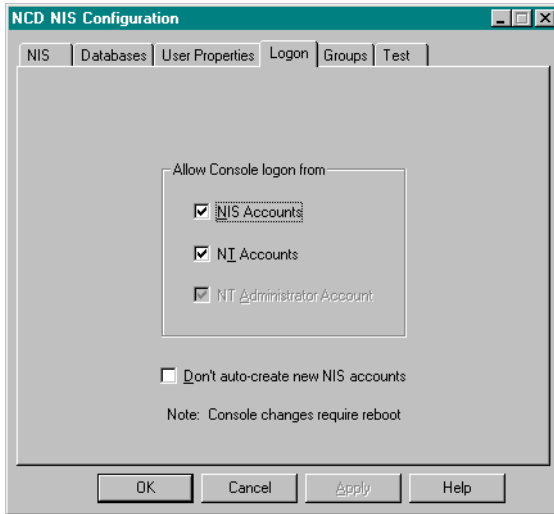
The following example is from a multi-user Windows NT system.



The Windows NT administrator can always log on from the console.

If all account types are blank, no one can log on from a WinStation, and only the Windows NT administrator can log on from the console. This is because the NT Administrator Account is always selected; it cannot be deselected.

The following example is from a standard Windows NT system.



To allow or deny logons from the console or from WinStations:

1. Start the NCD WinCenter NIS Logon Utility.
 - On Windows NT 4.0 or Windows 2000, select **Start > Programs > NCD Software > NIS Logon Utility**.
 - On Windows NT 3.51, open the installation group (NCD Software, by default), then double click on **NIS Logon Utility**.
2. Select the **Logon** tab and check which types of logons are allowed for the console and for WinStations.
 - **NIS Accounts**
Windows NT accounts either created by the NIS Logon Utility or manually edited to place **NIS account** in the **Description** field.
 - **NT Accounts**
User accounts created normally using the Windows NT User Manager for Domains.
 - **NT Administrator Account**
The account with the username Administrator, not just an account in the Administrator group.

3. Choose whether to create accounts for NIS users who are logging on to the Windows NT server for the first time.

— **Don't create new NIS accounts**

If you want to have Windows NT accounts created automatically for NIS users who log on to the specified Windows NT server for the first time, leave this unchecked (the default).

If you do not want to have Windows NT accounts created automatically for users who log on for the first time, check this.

Note If you want to create accounts manually for individual NIS users who do not yet have accounts on the Windows NT server, you can use **Administrative Tools > User Manager for Domains** and change the account's **Description** field to **NIS account**. If you want the NIS Logon Utility to manage an existing Windows NT user's account, "NIS account" must be given as the description.

4. Click **OK** to save information.

Groups

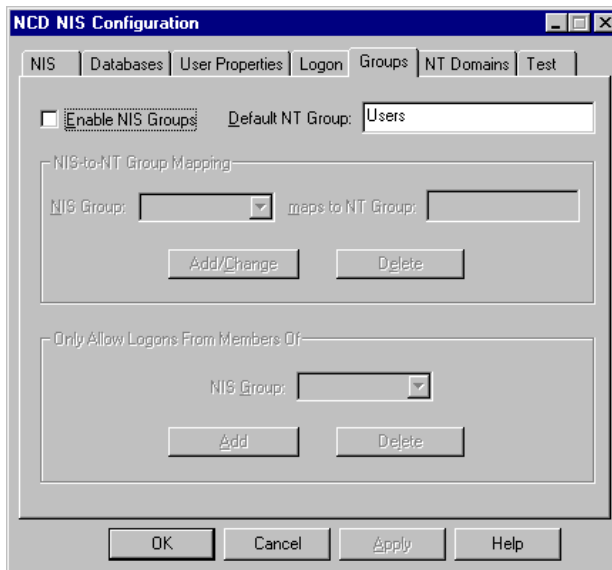
You have two basic choices for configuring groups for NIS users:

- Automatically assign all NIS users to a specified default Windows NT group (such as Users)
- Map NIS groups to Windows NT groups

If you map groups, you have the following mapping options:

- Map NIS groups to specific Windows NT groups, ignoring NIS groups as desired
- Restrict group logons

You make group choices by providing information on the **Groups** tab.



Selecting a Default Windows NT Group

You can assign NIS users to the default Windows NT group when they first log on to a Windows NT server.

To assign users to the default Windows NT group:

1. Start the NCD WinCenter NIS Logon Utility.
 - On Windows NT 4.0 or Windows 2000, select **Start > Programs > NCD Software > NIS Logon Utility**.
 - On Windows NT 3.51, open the installation group (NCD Software, by default), then double click on **NIS Logon Utility**.
2. Select the **Groups** tab.
3. Disable NIS groups by unchecking **Enable NIS Groups**, then specify the default Windows NT group, and click **OK**.

Mapping NIS Groups to Windows NT Groups

You can map NIS groups to Windows NT groups. After configuring a mapping, you can restrict logons to members of specific NIS groups.

When an NIS user logs on, the NIS domain is queried and password and group information is returned from the sources identified on the **Database** tab (see page 11).

If groups are enabled and the user is in a group that Windows NT lacks, the group is created and the user is added to it. The group is considered an NIS group and in the User Manager, “NIS group” is its description.

If an NIS group is mapped to an existing Windows NT group, the user becomes a member of that group automatically; the NIS group is not duplicated on the Windows NT system.

To map an NIS group:

1. Start the NCD WinCenter NIS Logon Utility.
 - On Windows NT 4.0 or Windows 2000, select **Start > Programs > NCD Software > NIS Logon Utility**.
 - On Windows NT 3.51, open the installation group (NCD Software, by default), then double click on **NIS Logon Utility**.

2. Select the **Groups** tab and enter the following information.
 - **Enable NIS Groups**

Check this.
 - **NIS Group/maps to NT Group**

To map to specific groups, select an NIS group and enter the desired Windows NT group, then click **Add/Change**.

For security, we recommend that you do not map to Administrator groups (to avoid assigning users to the Administrator group by mistake).

To remove an NIS group map, select the NIS group from the **NIS Group** list and click **Delete**.
3. Click **Apply** to save the information.

Limiting Group Logons

By default, any NIS user who is successfully validated against the NIS password database can log on to the Windows NT server. However, you can choose which NIS groups can log on.

To limit NIS logons by group:

1. Start the NCD WinCenter NIS Logon Utility.
 - On Windows NT 4.0 or Windows 2000, select **Start > Programs > NCD Software > NIS Logon Utility**.
 - On Windows NT 3.51, open the installation group (NCD Software, by default), then double click on **NIS Logon Utility**.
2. Select the **Groups** tab.
3. In **Only Allow Logons From Members Of**, select specific groups and click **Add** to allow logons or **Delete** to deny logons.

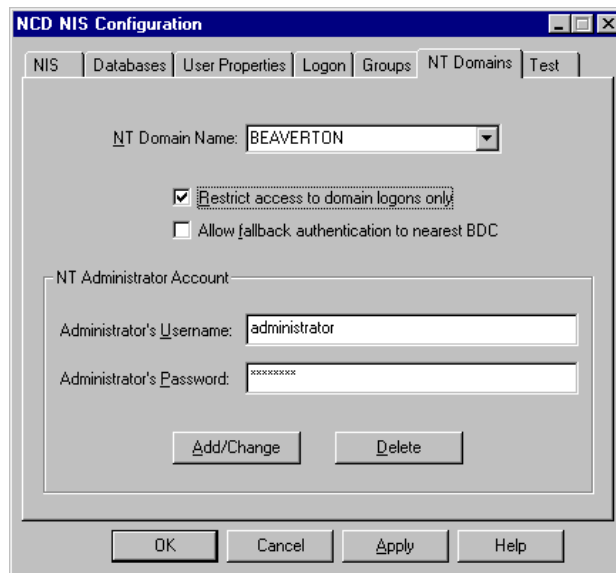
To allow NIS logons from all NIS groups, delete all NIS groups from the list.

Windows NT Domain Access

You must provide Windows NT domain administrator access if you want the NIS Logon Utility to automatically create and synchronize Windows NT domain accounts when NIS-authenticated users log on.

When the NIS Logon Utility has the domain administrator's username and password, it can write user information to the Primary Domain Controller in the Windows NT domain.

You provide the domain information on the **NT Domains** tab.



You can see this tab if you are running the NIS Logon Utility on a computer that is a member of a Windows NT domain and NIS is enabled on the **NIS** tab.

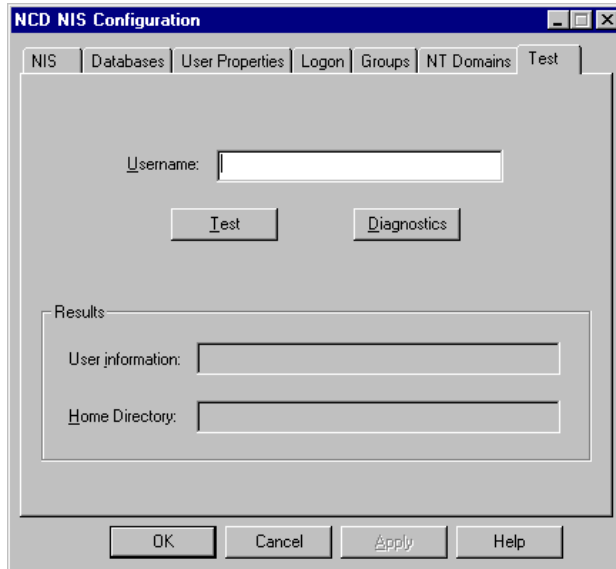
Configuring Windows NT Domain Data

To configure Windows NT domain data:

1. Start the NCD WinCenter NIS Logon Utility.
 - On Windows NT 4.0 or Windows 2000, select **Start > Programs > NCD Software > NIS Logon Utility**.
 - On Windows NT 3.51, open the installation group (NCD Software, by default), then double click on **NIS Logon Utility**.
2. Select the **NT Domains** tab, then select the Windows NT domain name. You may enter a new name here.
3. Modify domain information as follows, then click **Add/Change** or **Delete**.
 - **Administrator's Username**
A Windows NT domain administrator's username.
 - **Administrator's Password**
The Windows NT domain administrator's password.
4. If you want to restrict validated logons to a Windows NT domain instead of the local server, check the **Restrict access to domain logons only** option.
5. If a domain's Primary Domain Controller is offline or otherwise unavailable at logon, domain user information cannot be modified. Check the **Allow fallback authentication to nearest BDC** option to allow users who are authenticated by NIS to log on using information from a backup domain controller. User account information is not updated until the user logs on again when the Primary Domain Controller is available.
6. Click **Apply** to save the information.

Testing User Accounts

If a user has problems when trying to log on, you can test the user account. This procedure is useful for checking communication with an NIS domain.



To test user accounts:

1. Start the NCD WinCenter NIS Logon Utility.
 - On Windows NT 4.0 or Windows 2000, select **Start > Programs > NCD Software > NIS Logon Utility**.
 - On Windows NT 3.51, open the installation group (NCD Software, by default), then double click on **NIS Logon Utility**.
2. Select the **Test** tab.
3. Enter the username.
4. Click **Test** to see the user's NIS password information and home directory in the **Results** group.
5. If you see a problem, you can click **Diagnostics** to view diagnostic information.

Event Log

The Windows NT Event Log contains NIS startup and logon information. The amount of information logged depends on the debug level, as described in “NIS Domains” on page 9.

To view information:

1. In Windows NT Administrative Tools, select the Event Viewer, then select **Log > Application**.

Date	Time	Source	Category	Event	User	Computer
12/13/99	3:33:24 PM	NCD NIS	None	2	N/A	TEN_C
12/13/99	3:33:24 PM	NCD NIS	None	2	N/A	TEN_C
12/13/99	3:33:23 PM	NCD NIS	None	2	N/A	TEN_C
12/13/99	3:33:23 PM	NCD NIS	None	2	N/A	TEN_C
12/13/99	3:33:23 PM	NCD NIS	None	2	N/A	TEN_C
12/13/99	3:33:23 PM	NCD NIS	None	2	N/A	TEN_C
12/13/99	3:33:22 PM	NCD NIS	None	2	N/A	TEN_C
12/13/99	3:33:21 PM	NCD NIS	None	2	N/A	TEN_C
12/13/99	3:33:21 PM	NCD NIS	None	2	N/A	TEN_C
12/13/99	3:33:09 PM	NCD NIS	None	2	N/A	TEN_C
12/13/99	3:33:09 PM	NCD NIS	None	2	N/A	TEN_C
12/13/99	3:33:09 PM	NCD NIS	None	2	N/A	TEN_C
12/13/99	3:33:09 PM	NCD NIS	None	2	N/A	TEN_C
12/13/99	3:33:09 PM	NCD NIS	None	2	N/A	TEN_C
12/13/99	3:33:09 PM	NCD NIS	None	2	N/A	TEN_C

2. To see detail, double click an item. All events generated by the NIS Logon Utility have “NCD NIS” as the source.

Event Detail

Date: 12/13/99 Event ID: 2
Time: 3:33:24 PM Source: NCD NIS
User: N/A Type: Information
Computer: TEN_C Category: None

Description:
NCD NIS Information: joes matched
joes:65acUQ7xZAPik:330:100:Joe
Sand.Doc.8498.BV.Writer.,/home/joes:/bin/csh

Detail: Bytes Words

Close Previous Next Help

Index

A

- access
 - Windows NT domain 23
- account
 - NIS 4
 - options
 - don't create new NIS accounts 19
 - type 1
 - logon by 17
 - user 19
 - testing 25
 - Windows NT 4
- Administrator group 22
- Administrator's Password field 24
- Administrator's Username field 24
- Append User option 14
- Auto_Master table 12
- automount
 - database 11, 12

B

- broadcasting for an NIS server 10

D

- Database tab 11
- database(s)
 - NIS 11
 - NIS automount 11, 12
 - NIS group 11, 12
 - NIS password 1, 5, 11, 22

- synchronized 5
- Windows NT User Manager 5
- debug level 10, 26
- diagnostic information 25
- DNS domain 10
- domain
 - DNS 10
 - NIS 9, 10
 - tab 23
 - Windows NT 10, 23

E

- Enable NIS Groups
 - option 22
- event
 - startup 26
- Event Log 10, 26
- Event Viewer 26

G

- group(s)
 - Administrator 22
 - configuring 20
 - database 11, 12
 - default 21
 - enabling 12
 - mapping 20
 - mapping to Windows NT group 21
 - NIS 5
 - restricted logon 22
 - Windows NT 21

- group.bygid file 12
- Groups tab 12, 20

H

- home directory
 - mounting 12
 - specifying when created 15

L

- Local Path option 14
- logon
 - by account type 17
 - process 3
 - restricted 22
 - script 16
- Logon Script Name field 16
- Logon tab 17

M

- map 11
 - group 20
- mounting home directories 12

N

- NFS client 12, 14
- NIS
 - account 4
 - account conversion 4
 - database 11
 - databases 11

- domain
 - configuring 9
 - name 10
- features 1
- groups 5
- logon 5
 - limiting 22
- maps 11
- password database 1, 4
- server 10
- tab 9, 23
- NIS Group/Maps to NT
 - Group option 22
- NIS+ 1, 3, 5, 10, 12
 - server 10, 12
 - strict 10
- nobody class 10
- NT Domains tab 23
- O**
- Only Allow Logons From Members Of field 22
- P**
- passwd.byname table 12
- passwd.org_dir table 12
- password
 - database option 12
 - NIS database 1, 4, 11, 22
 - NIS 5
 - shadowed 1, 10
 - table 10
- profile path 16
- S**
- Set at every login option 15
- Set at NT account creation only option 15
- Set Profiles and Scripts At Logon option 16
- shadowed password 1, 10
- SMB server 12, 14
- startup events 26
- strict NIS+ 10
- T**
- Terminal Server
 - properties 16
- Test tab 25
- testing user accounts 25
- U**
- Use password database option 12
- Use Strict NIS+ option 10
- user
 - account 19
 - testing 25
 - properties 1
 - configuring 13
 - validation 3, 10
- User Profile Path field 16
- User Properties tab 12, 13
- V**
- validation
 - shadowed password 10
 - user 3, 10
- W**
- Windows NT
 - account 4
 - domain
 - access 23
 - name 10
 - group 21
 - default 20, 21
- Windows NT User Manager database 5
- Y**
- YP compatibility mode 1, 5, 10, 12