New User

Creates one or more new user accounts.

See Also

Creating a New User Account

New Global Group

Creates a new global group.

Note

- **New Global Group** is unavailable when **Low Speed Connection** is selected or when you administer a computer running Windows NT Workstation or Windows NT Server that is not a domain controller (a member server).

See Also

Creating a New Global Group

Using Low Speed Connection

New Local Group

Creates a new local group.

See Also

Creating a New Local Group

Copy

Creates one or more new user accounts or a new group, copying existing user accounts or a group that you have selected in User Manager for Domains.

See Also

Copying a User Account

Copying a Global Group

Copying a Local Group

Using Low Speed Connection

Delete

Deletes a local group or one or more user accounts that you have selected in User Manager for Domains. User accounts and groups created with User Manager for Domains can be deleted, but the built-in user accounts and groups cannot be deleted.

Note

- Be certain you want to delete a group or user account before you do so because they cannot be recovered.

See Also

Disabling and Enabling User Accounts

Deleting User Accounts

Deleting a Global Group

Deleting a Local Group

Using Low Speed Connection

Rename

Renames a selected user account.

See Also

Renaming User Accounts
Using Low Speed Connection

Properties

Modifies a group or one or more user accounts that you have selected in User Manager for Domains.

See Also

Managing Properties for One User Account
Managing Properties for Multiple User Accounts
Managing Global Group Properties
Managing Local Group Properties
Using Low Speed Connection

Select Users

Displays a dialog box from which you can select a group and then quickly select or deselect all the user accounts that are members of that group.

After the user accounts are selected, you can modify the properties of those accounts in the same way, delete all of them, or create a new group containing those accounts.

Select Users is unavailable when **Low Speed Connection** is selected**.**

See Also

Selecting User Accounts

Using Low Speed Connection

Select Domain

When User Manager for Domains starts, it displays the domain in which your user account is defined. Use **Select Domain** to display a different domain.

Optionally, use **Select Domain** to display an individual computer. However, you can display only a computer that maintains its own directory database, such as a computer running Windows NT Workstation or Windows NT Server that is not a domain controller (a member server) or a Microsoft LAN Manager server.

See Also

Selecting a Domain

Using Low Speed Connection

Exit

Quits User Manager for Domains.

Sort by Full Name

Sorts the displayed user accounts by the full names. When **Sort by Full Name** is enabled, a check mark appears on the menu to the left of the command.

This command is unavailable when **Low Speed Connection** is selected.

See Also

Sorting the User Account List

Sort by Username

Sorts the displayed user accounts by the user names. A check mark appears next to the command when it is enabled.

This command is unavailable when **Low Speed Connection** is selected.

See Also

Sorting the User Account List

Refresh

Updates the display with current information.

This command is unavailable when **Low Speed Connection** is selected.

See Also

Refreshing the View

Using Low Speed Connection

Account

The **Account** policy controls how passwords must be used by all user accounts. It defines things such as the maximum password age, minimum password age, minimum password length, whether a password history is maintained, and whether users must log on before changing their passwords.

It also determines lockouts. If locking out is enabled, then a user account cannot log on after a number of failed attempts to log on to that account within a specified time limit. A locked account remains locked until an administrator unlocks it or a specified amount of time passes.

The **Account** policy also determines whether or not a remote user is forcibly disconnected from a domain when that user's logon hours expire.

Notes

- Windows NT version 3.1 and LAN Manager version 2.x do not use the lockout feature.
- Failed password attempts against workstations or member servers that have been locked using Ctrl+Alt+Delete or password-protected screen savers do not count against account-lockout settings entered in User Manager for Domains.

See Also

Managing the Account Policy

User Rights

The **User Rights** policy manages the rights granted to groups and user accounts.

A right authorizes a user to perform certain actions on the system. A user who logs on to an account to which the appropriate rights have been granted can carry out the corresponding actions. When a user does not have appropriate rights, attempts to carry out those actions are blocked by the system. Rights apply to the system as a whole and are different from permissions, which apply to specific objects.

The rights granted to a group are provided to the members of that group. In most situations, the easiest way to provide rights to a user is to add that user's account to one of the built-in groups that already possesses the needed rights, rather than by administering the **User Rights** policy.

See Also

Managing the User Rights Policy

The User Rights

Audit

The **Audit** policy tracks selected user activities by auditing security events and storing the data in a security log. Your **Audit** policy specifies the types of security events to be logged.

These types can range from system-wide events (such as a user logging on) to specific ones, such as a user attempting to read a particular file. The types can include successful events, unsuccessful events, or both.

When you administer domains, the **Audit** policy affects the security logs of all domain controllers.

When you administer a computer that is not a domain controller, the **Audit** policy affects the security log of only that computer (running Windows NT Workstation or Windows NT Server).

You can use **Event Viewe**r to review events in a security log.

See Also

Managing the Audit Policy

Trust Relationships

A trust relationship is a link between two Windows NT Server domains.

Use the **Trust Relationships** policy to add and remove trusting domains (resource domains) and trusted domains (account domains).

- Trusting domains allow their resources to be used by accounts in other (trusted) domains.
- Trusted-domain users and global groups are allowed to hold user rights, resource permissions, and local group memberships on the trusting domain.

Trust relationships can allow a user to access resources on the entire network using a single user account and a single password. This moves the convenience of centralized administration from the domain level to the network level.

Note

- Trust relationships can be established only between Windows NT Server domains.

See Also

Adding a Trusting Domain

Adding a Trusted Domain

Low Speed Connection

When administering a domain or computer that communicates with your computer across a connection providing relatively low transmission rates, some User Manager for Domains functions can occur slowly. In this situation, you can reduce delays by clicking **Low Speed Connection** on the **Options** menu.

When you select a different domain or computer to be displayed by User Manager for Domains, you can also select or clear the **Low Speed Connection** check box in the **Select Domain** dialog box.

The system saves the **Low Speed Connection** setting for each of the last 20 domains or computers you have administered. After you specify a domain or computer name in the **Select Domain** dialog box, the previous state of this option will be initially set. You can accept or change this setting.

If you have not previously administered the specified domain or computer, and if you do not select the **Low Speed Connection** check box in the **Select Domain** dialog box, the system automatically determines the appropriate connection mode and accordingly selects or clears **Low Speed Connection** after you click **OK**. After connecting, you can still change the setting by clicking **Low Speed Connection** on the **Options** menu.

See Also

Using Low Speed Connection

Selecting a Domain

Confirmation

Causes a message to appear asking for confirmation after you click certain commands.

When **Confirmation** is enabled, a check mark appears on the menu, to the left of the command.

Save Settings on Exit

Saves these settings when you quit User Manager for Domains: Window size and position, sort order (by user name or full name), and the setting for **Confirmation** on the **Options** menu.

When **Save Settings** is enabled, a check mark appears to the left of the command on the **Options** menu.

Font

Enables you to change the font used for the list of users and groups in User Manager for Domains.

Contents

Lists Help topics for User Manager for Domains.

Search for Help On

Presents an index of keywords from Help for User Manager for Domains. Associated Help topics can be listed, selected, and opened.

How to Use Help

Provides introductory information about accessing and using the online Help system.

About User Manager

Provides the version number, serial number, copyright, licensing, and other information about User Manager for Domains.

What Is User Manager for Domains?

User Manager for Domains is a Windows NT 4.0 tool you can use to manage security for Windows NT 4.0 domains, member servers, and workstations. For Windows 2000 domains, member servers, and Windows 2000 Professional computers, use Active Directory and the other Windows 2000 administrative tools instead. With User Manager for Domains you can:

- Select the domain or computer to be administered.
- Create and manage user accounts.
- Create and manage groups.
- Manage the security policies.

See Also

The User Manager for Domains Window

The User Manager for Domains Window

In most cases, User Manager for Domains displays your logon domain when it first starts. The title bar shows the domain name, and the body of the User Manager for Domains window displays two lists. The upper list contains user accounts; the lower list contains group accounts. You can select one or more user accounts, or one group account, and manage them using commands on the **User** menu.

Click the following for more information about User Manager for Domains.

- Title bar
- Menu bar
- List of users
- User icon
- Username
- Full Name
- Description (of users)
- List of groups
- Group icon
- Groups
- Description (of groups)

See Also

Using Low Speed Connection

Title bar

The title bar names the domain or computer that is displayed for administration.

Menu bar

The menu bar contains five menus.

- **User**: Commands to create and manage user accounts and groups, and to select the domain or computer to be administered.
- **View**: Commands to sort the user account list either by user name or by full name, and to update User Manager with current information.
- **Policies**: Commands to manage the security policies.
- **Options**: Commands to select or clear **Low Speed Connection**, **Confirmation**, and **Save Settings on Exit**.
- **Help**: Commands to provide online Help.

List of user names

When you select a domain for administration, the upper half of the window lists the user accounts of the domain (the domain name appears in the title bar). The list contains both the built-in user accounts provided with the system, and any user accounts that have been added from User Manager for Domains.

When you administer a computer running Windows NT Workstation or Windows NT Server that is not a domain controller (a member server), the list contains the user accounts of that computer.

User icon

An icon graphically indicates the type of each listed user account.

 Global account: a normal user account in a user's home domain. Most accounts are global accounts. When trust relationships are established between domains, each network user needs only one global account in one domain to be granted access to any trusting domain.

 Local account. An account provided in this domain to accommodate a user whose global account is in a domain that is not trusted by this domain.

When you are administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller (a member server), the list contains only global accounts. Computers running Windows NT Workstation do not maintain local accounts.

Username

For each listed user account, this column contains a user name, which is used by the Windows NT operating system to identify the account. A user name is always unique, meaning it cannot be identical to any other user or group name of the domain or computer being administered.

The user names can appear in either the first or second column of the user account list. This sort order is controlled by commands on the **View** menu.

Full Name

For each listed user account, this column either contains the user's full name or is blank. (When a user account is created or modified, **Full Name** is an optional entry.)

The full names can appear in either the first or second column of the user account list. This sort order is controlled by commands on the **View** menu.

Description (of users)

For each listed user account, this column either contains descriptive text or is blank. (When a user account is created or modified, **Description** is an optional entry.)

List of groups

When a domain is being administered, the lower half of the window lists the groups of the domain (the domain name appears in the title bar). The list contains local and global groups, including both the built-in groups provided with the system, and any groups that have been added by using User Manager for Domains.

When you are administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller (a member server), the list contains only local groups. These computers do not maintain global groups.

Group icon

An icon graphically indicates the type of each listed group.

 Local group. Can be granted permissions and rights for only the domain controllers of its own domain. However, it can contain user accounts and global groups from its own domain and from trusted domains.

 Global group. Can be granted permissions and rights for the domain controllers of its own domain, for other workstations and member of its own domain, and for trusting domains. A global group can become a member of local groups in any of these domains. However, it can contain user accounts only from its own domain.

When you are administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller (a member server), the list contains only local groups. These computers do not maintain global groups.

Groups

This column contains a group name that identifies the group account. A group name is always unique, meaning it cannot be identical to any other group or user name of the domain or computer being administered.

Description (of groups)

This column either contains descriptive text or is blank. (**Description** is an optional entry.)

What Are the Security Policies?

Click the following for summary information about the security policies.

- Account policy
- User Rights policy
- Audit policy
- Trust Relationships

Account policy

The **Account** policy controls how passwords must be used by all user accounts. It defines things such as the maximum password age, minimum password age, minimum password length, whether a password history is maintained, and whether users must log on before changing their passwords.

It also determines lockouts. If locking out is enabled, then a user account cannot log on after a number of failed attempts to log on to that account within a specified time limit. Lockout can also occur when a user attempts to change the password using an incorrect password for the old password. A locked account remains locked until an administrator unlocks it or a specified amount of time passes.

The **Account** policy also determines whether or not a remote user is forcibly disconnected from a domain when that user's logon hours expire.

Note

- Failed password attempts against workstations or member servers that have been locked using Ctrl+Alt+Delete, or password protected screen savers, do not count against account lockout settings entered in User Manager for Domains.

User Rights policy

The **User Rights** policy manages the rights granted to groups and user accounts.

A right authorizes a user to perform certain actions on the system. A user who logs on to an account to which the appropriate rights have been granted can carry out the corresponding actions. When a user does not have appropriate rights, attempts to carry out those actions are blocked by the system. User rights apply to the system as a whole and are different from permissions, which apply to specific objects.

The rights granted to a group are provided to the members of that group. In most situations, the easiest way to provide rights to a user is to add that user's account to one of the built-in groups that already possesses the needed rights, rather than by administering the **User Rights** policy.

Audit policy

You can track selected user-activities by auditing security events and storing the data in a security log. Your **Audit** policy specifies the types of security events to be logged.

These types can range from system-wide events (such as a user logging on) to specific events (such as a user attempting to read a particular file). They can include successful events, unsuccessful events, or both.

When you administer domains, the **Audit** policy affects the security logs of all domain controllers.

When you administer a computer that is not a domain controller, the **Audit** policy affects the security log of only that computer (running Windows NT Workstation or Windows NT Server).

You can use Event Viewer to review events in a security log.

Trust Relationships

A trust relationship is a link between two Windows NT Server domains.

Use **Trust Relationships** to add and remove trusting domains (resource domains) and trusted domains (account domains).

- Trusting domains allow their resources to be used by accounts in other (trusted) domains.
- Trusted-domain users and global groups can hold user rights, resource permissions, and local group memberships on the trusting domain.

Trust relationships can allow a user to access resources on the entire network using a single user account and a single password. This moves the convenience of centralized administration from the domain level to the network level.

Note

- Trust relationships can be established only between Windows NT Server domains.

To change the displayed domain

1 On the **User** menu, click **Select Domain**.

2 Enter a domain name in **Select Domain**.

3 If the domain or computer you have specified communicates with your computer over a low-speed connection, select the **Low Speed Connection** check box.

Notes

- When it first starts, User Manager for Domains displays the domain in which your user account is defined. A different domain can be selected.
- The system saves the **Low Speed Connection** setting for each of the last 20 domains or computers you have administered. After you specify a domain or computer name, the previous setting is initially displayed here. If no previous setting is known, **Low Speed Connection** is initially cleared. You can accept or change the setting.

See Also

Using Low Speed Connection

To change the sort order

- On the **View** menu, click either **Sort By Full Name** or **Sort By Username**.

Note

When **Low Speed Connection** is enabled, **Sort By Full Name** and **Sort By Username** are unavailable.

To update the view with current information

- On the **View** menu, click **Refresh**.

Notes

- When User Manager for Domains first displays a domain or a computer, it obtains the information shown in the User Manager for Domains window. This information is automatically updated at fixed intervals. Use the **Refresh** command to display the most current information.
- When **Low Speed Connection** is enabled, **Refresh** is unavailable.

To select or clear Low Speed Connection

1 On the **User** menu, click **Select Domain**.

2 Select a domain or computer to administer.

3 In the **Select Domain** dialog box, click to select or clear **Low Speed Connection**.

Notes

- When starting User Manager for Domains from command prompt you can append parameters for connection speed:
- [**/l**] for **Low Speed Connection**.
- or [**/h**] for the normal (high speed) connection.

For example, to start User Manager for Domains and administer a domain named Shipping using **Low Speed Connection**, type **usrmgr shipping /l**.

- Using **Low Speed Connection** causes the following changes to User Manager for Domains:
- The list of user accounts does not appear in the User Manager for Domains window, and on the **User** menu **Select Users** is unavailable. To manage user accounts, you can use commands on the **User** menu.
- The list of groups does not appear in the User Manager for Domains window. To manage local groups, you can use commands on the **User** menu.
- Global groups cannot be created or copied, properties of existing global groups cannot be managed, and **New Global Group** on the **User** menu is unavailable. You can indirectly manage global group memberships by managing the group memberships of individual user accounts.
- The **View** menu commands are unavailable.

See Also

Selecting a Domain

To create a new user account

1. On the **User** menu, click **New User**.
2. Type appropriate information in the dialog box:
   - In **Username**, type a user name.
   - In **Full Name**, type the user's complete name.
   - In **Description**, type a description of the user or the user account.
   - In both **Password** and **Confirm Password**, type a password of up to 14 characters.
3. Select or clear the check boxes for **User Must Change Password at Next Logon**, **User Cannot Change Password**, **Password Never Expires**, and **Account Disabled**.
4. To administer a property associated with a button in the **New User** dialog box, click the button and complete the dialog box that appears; then click **OK**.
5. Click **Add**.

   To add another user account, repeat steps 2 through 5.

Notes

- A user name cannot be identical to any other user or group name of the domain or computer being administered. It can contain up to 20 uppercase or lowercase characters except for the following:

  `" / \ [ ] : ; | = , + * ? < >`

  A user name cannot consist solely of periods (.) and spaces.
- Which buttons appear in the **New User** dialog box depends on whether you are administering domains or workstations.
  - **Groups**, **Profile**, and **Dialin** always appear.
  - **Hours**, **Logon From**, and **Account** appear only when you administer domains.

See Also

Managing Group Memberships for One User Account

Managing Terminal Server User Configuration

Managing the User Environment

Managing Dialin Permissions

Managing Logon Hours

Managing Logon Workstations

Managing Account Information

Using Low Speed Connection

To copy a user account

1. On the **User** menu, click **Copy**.
2. Type appropriate information in the dialog box:
   - In **Username**, type a user name.
   - In **Full Name**, type the user's complete name.
   - In **Description**, type a description of the user or the user account (optional).
   - In both **Password** and **Confirm Password**, type a password of up to 14 characters.
3. Select or clear the check boxes for **User Must Change Password at Next Logon**, **User Cannot Change Password**, **Password Never Expires**, and **Account Disabled**.
4. To administer a property associated with a button in the **Copy Of** dialog box, click the button and complete the dialog box that appears; then click **OK**.
5. Click **Add**.

Notes

- A user name cannot be identical to any other user or group name of the domain or computer being administered. It can contain up to 20 uppercase or lowercase characters except for the following:

  `" / \ [ ] : ; | = , + * ? < >`

  A user name cannot consist solely of periods (.) and spaces.
- When you copy a user account, group memberships of the original account are copied to the new account.
- Which buttons appear in the **Copy Of** dialog box depends on whether you are administering domains or workstations.
  - **Groups**, **Profile**, and **Dialin** always appear.
  - **Hours**, **Logon From**, and **Account** appear only when you administer domains.

See Also

Managing Group Memberships for One User Account

Managing Terminal Server User Configuration

Managing the User Environment

Managing Dialin Permissions

Managing Logon Hours

Managing Logon Workstations

Managing Account Information

Using Low Speed Connection

To modify one user account

1 In User Manager for Domains, select a user account.

2 On the **User** menu, click **Properties**.

3 To change the **Full Name** or **Description**, type new text.

4 To change the password, type a password of up to 14 characters in both **Password** and **Confirm Password**.

5 If necessary, change the settings of the password and **Account Disabled** check boxes.

6 To administer a property associated with a button in the **User Properties** dialog box, click the button and complete the dialog box that appears; then click **OK**.

Notes

- For security, the existing password is represented by a row of asterisks; the number of asterisks displayed differs from the actual number of characters used in the password.
- Which buttons appear in the **User Properties** dialog box depends on whether you are administering domains or workstations.
- **Groups**, **Profile**, and **Dialin** always appear.
- **Hours**, **Logon From**, and **Account** appear only when you administer domains.

See Also

Selecting User Accounts

Managing Group Memberships for One User Account

Managing Terminal Server User Configuration

Managing the User Environment

Managing Dialin Permissions

Managing Logon Hours

Managing Logon Workstations

Managing Account Information

Using Low Speed Connection

To make the same modification to two or more user accounts

1 In User Manager for Domains, select two or more user accounts.

2 On the **User** menu, click **Properties**.

3 Type to enter new text in **Description** for all the selected user accounts.

4 Clear or select check boxes to change any settings for password or **Account Disabled**.

5 To administer a property associated with a button in the **User Properties** dialog box, click the button and complete the dialog box that appears; then click **OK**.

Notes

- In **Description**, text appears only if all the selected user accounts have identical descriptions. Otherwise, **Description** appears blank.
- If all the accounts have the same setting for an option, the setting for that check box is displayed. Otherwise, that check box is indeterminate (filled with gray).
- Which buttons appear in the **User Properties** dialog box depends on whether you are administering domains or workstations.
  - **Groups**, **Profile**, and **Dialin** always appear.
  - **Hours**, **Logon From**, and **Account** appear only when you administer domains.

See Also

Selecting User Accounts

Managing Group Memberships for Multiple User Accounts

Managing Terminal Server User Configuration

Managing the User Environment

Managing Dialin Permissions

Managing Logon Hours

Managing Logon Workstations

Managing Account Information

Using Low Speed Connection

To manage group memberships when only one user account is selected

1. Click **Groups** in the **New User**, **Copy Of**, or **User Properties** dialog box.
2. To add the user account to one or more groups, select one or more groups in **Not Member Of**, and then click **Add**.
3. To remove the user account from one or more groups, select one or more groups in **Member Of**, and then click **Remove**.
4. To change the user-account primary group, select one global group from **Member Of**, and then click **Set**.

Note

- You cannot remove the primary group.

To manage common group memberships for two or more user accounts

1 In User Manager for Domains, select two or more user accounts

2 On the **User** menu, click **Properties**.

3 In the **User Properties** dialog box, click **Groups**.

4 Use the following methods to make the changes you want:

- To add all the user accounts to one or more groups, select one or more groups in **Not All Are Members Of**, and then click **Add**.
- To remove all the user accounts from one or more groups, select one or more groups in **All Are Members Of**, and then click **Remove**.
- To change the primary group for all the selected user accounts, select one global group from **All Are Members Of**, and then click **Set**.

Notes

- You cannot remove a primary group.
- If even one of the selected user accounts is not a member of a particular group, that group is listed in **Not All Are Members Of**.

See Also

Selecting User Accounts

To configure the user-environment profile

1. In the **New User**, **Copy Of**, or **User Properties** dialog box, click **Profile**.
2. To enable the user profile to be roaming or mandatory, create a share on the appropriate server, grant Full Control to Everyone, and type the full path in **User Profile Path**, such as:

   \\airedale\profiles\cristalw

   If the user will log on to computers running both Windows NT and Terminal Server, you can specify separate Windows NT and Terminal Server user profile paths.

   If you specify only the user profile path, that path is used for both Windows NT and Terminal Server logons.

   If you specify only the Terminal Server profile path, the default profile path is used for Windows NT logons, and the specified profile path is used for Terminal Server logons.
3. To assign a logon script:,

- Type the file name in **Logon Script Name**, such as:
  clerks.cmd
- If the logon script is stored in a subdirectory of the logon script path, precede the file name with that relative path, such as:
  clerks\cristalw.cmd

4. To specify a home directory for Windows NT logons, click **Connect** in the **Home Directory** area, specify a drive letter, click **To**, and then type a network path, such as:

   \\airedale\users\cristalw

   If the directory cristalw does not exist, User Manager for Domains creates it.

   If you specify only the home directory for Windows NT, that home directory is used for both Windows NT and Terminal Server logons.
5. To specify a home directory for Terminal Server logons, click **Connect** in the **Terminal Server Home Directory** area, specify a drive letter, click **To**, and then type a network path, such as:

   \\airedale\users\cristalw

   If the directory cristalw does not exist, User Manager for Domains creates it.

   If you specify only the Terminal Server home directory, the default home directory is used for Windows NT logons, and the specified home directory is used for Terminal Server logons.
6. Optionally, substitute %USERNAME% for the last subdirectory in the home directory path, such as:

   \\airedale\users\%username%

Notes

- In step 4 and step 5, you can type in **Local Path** (for example, **c:\users\cristalw**). Local home directories assigned in domain user accounts are not created automatically; they must be created manually.
- If the user will log on both to computers running Windows NT 3.x and to computers running Windows NT 4.0 or Terminal Server, the user-profile path must contain a file name. The file name can be that of a roaming user profile (.USR file name extension) or a mandatory user profile (.MAN file name extension). For example, you might type **\\airedale\profiles\clerks.man**.
- If the user will log on only to a computer running Windows NT 4.0 or Terminal Server, the user-profile path should be to a directory name and should not include an extension of .USR or .MAN. If the directory specified in the user profile path does not exist, it is automatically created the first time the user logs on.
- When administering multiple user accounts, do not assign one preconfigured, roaming user profile to multiple accounts unless it is a mandatory user profile. To assign the same preconfigured, roaming user profile to multiple user accounts, enter a separate user profile path for each user account, and use System in Control Panel (**User Profiles** tab) to copy the preconfigured user profile to the server location for each user.
- If no home directory is assigned here, the system assigns the user account the default local home directory (\USERS\DEFAULT on the user's local drive where Windows NT Workstation 4.0 or Windows NT Server 4.0 is installed as an upgrade, or the root directory where this version is installed as the initial version).

To manage the user's Terminal Server configuration

1. In the **New User**, **Copy Of**, or **User Properties** dialog box, click **Config**.
2. To permit or deny the user to log on at the Terminal Server, click to select or clear the **Allow Logon to Terminal Server** check box. A user's ability to log on can be disabled temporarily without deleting the user's account.
3. To change the time-out settings for the user, click one of the time-outs in **Timeout settings** and enter the desired value or select the **No Timeout** check box to disable the time-out. The time-out timers are:

- Connection time-out. This setting specifies how long the user is allowed to be logged on to the server at one time. One minute before the connection time-out interval expires, the user is notified of the pending disconnection. The user's session is disconnected or terminated, depending on the broken or timed-out connection action specified in the **User Configuration** dialog box. This timer is not cumulative; every time the user logs on, the timer is reset.
- Disconnection time-out. This setting specifies the maximum amount of time a disconnected session is retained in the disconnected state before the logon is terminated.
- Idle time-out. This setting specifies how long the session can remain idle (no keyboard or mouse activity) before the user's session is disconnected or terminated, depending on the broken or timed out connection action specified in the **User Configuration** dialog box. This timer is reset whenever there is keyboard or mouse activity on the user's client computer.

4. To specify an initial program to be executed when the user logs on, type the program information as you would type it at a command prompt into **Command Line** and type the working directory for the program into **Working Directory**. The **Inherit Client Config** check box, selected by default, causes the logon process to use any initial program specified by the client.
5. To specify what happens when a connection is lost due to a connection error or the Connection or Idle timers expiring, click one of the settings in **On a Broken or Timed-out Connection**. You can place the user session in a disconnected state or reset (terminate) the user session. If the user session is placed in a disconnected state, it will remain in that state until the session is reconnected or the disconnected session timer times out.
6. To specify whether to reestablish client disk and printer mappings when a user logs on, click one of the settings in **Client Devices**. Select **Connect Client Drives at Logon** to reestablish any previous client drive mappings when the user logs on; select **Connect Client Printers at Logon** to reestablish any previous printer mappings when the user logs on. To force the default client printer to the Terminal Server default printer, select **Default to Main Client Printer**.

   These options are supported for Citrix ICA-based clients only. For Terminal Server Clients, use logon scripts to map drives and printers.
7. To specify where a disconnected session for this user can be reconnected, click one of the settings in **Reconnect**. If you click **From Any Client**, any disconnected session for that user will be reconnected (no new logon) when the user logs on from any client. If you click **From Previous Client Only**, logging on from the same client that the session was disconnected from will reconnect the disconnected session, but logging on from any other client will start a new logon session. Note that sessions started at clients other than the system console cannot be connected to the system console, and sessions started at the system console cannot be disconnected.

   This option is supported only for Citrix ICA-based clients that provide a serial number when connecting.
8. To specify modem callback settings, click one of the items in **Callback**. The client can be configured so that, when a remote user dials in to a modem port, the application server hangs up the phone and dials the remote client back. This process is called *modem callback*.

   Modem dialback can be disabled (the default), enabled for a fixed telephone number, or enabled for a roving (user-specified) telephone number. If dialback to a fixed number is specified, a telephone number must be entered. If dialback to a roving number is selected, you can specify an optional default telephone number for callback.

   These options are supported for Citrix ICA-based clients only. Use Remote Access Service (RAS) to configure callback options for Terminal Server Clients.
9. To specify shadowing settings, click a setting in **Shadowing**. Shadowing allows a user to remotely monitor the on-screen operations of another user. Select Disabled to disable shadowing. Select Enabled to enable shadowing. Specifying Input allows the shadower to send mouse and keyboard data to the shadowed session. Specifying Notify requires the shadowed user to agree to be shadowed whenever another user attempts to

shadow this user. Note that sessions at the system console cannot be shadowed from other clients and the system console cannot be used to shadow other clients.

This option is supported for Citrix ICA-based clients only.

User Profile

A user profile defines the Windows NT environment that is loaded by the system when a user logs on. For Windows NT 4.0, a user profile is a directory of files. For Windows NT 3.x, a user profile is a single file. In both cases, a user profile includes all the user-specific settings of a user’s Windows NT environment: program items, screen colors, network connections, printer connections, mouse settings, window size and position, and more.

Roaming User Profile

A roaming user profile is a server-based user profile that is downloaded to the local computer when a user logs on and that is updated both locally and on the server when the user logs off. A roaming profile is available from the server when logging on to any computer running Windows NT Workstation or Windows NT Server. When the user logs on, if the local user profile is more current than the copy on the server, the user has the option to use the local user profile.

Mandatory User Profile

A mandatory user profile is a roaming user profile that is not updated when the user logs off.

Logon Script

A logon script allows an administrator to affect a user’s environment without managing all aspects of it. When a logon script is assigned to an user account, it runs each time the user logs on.

One logon script can be assigned to one or more user accounts. It can be a batch file (.cmd or .bat file name extension) or an executable program (.exe file name extension).

When a user logs on, the computer authenticating the logon locates the logon script by following the computer's logon script path, which is usually \winnt\system32\repl\import\scripts.

Note

The client computer executes the logon script file. Client computers running Microsoft Network Client for MS-DOS (version 3.0), Windows for Workgroups, Windows NT version 3.1, and LAN Manager 2.x, must use the .bat file name extension with the logon script name.

Home Directory for Windows NT and Terminal Server

An assigned home directory becomes a user's default directory for the **File Open** and **Save As** dialog boxes, for command prompt, and for all applications that do not have a defined working directory. It can be a local directory on a user’s computer or a shared network directory, and can be assigned to a single user or many users.

Each user on Terminal Server should have a unique home directory on the server. This ensures that application information is stored separately for each user in the multiuser environment.

Home directories make it easier for an administrator to back up user files and delete user accounts by collecting many or all of a user's files in one location.

To specify a network path for the home directory, you must first create the share and set permissions that allow the user access.

Usually, User Manager for Domains automatically creates the home directory. If it cannot, a message appears, instructing you to create the directory. If you do not assign a home directory to a user account, the system uses the default local home directory (\USERS\DEFAULT on the user's local drive where Windows NT Workstation 4.0 or Windows NT Server 4.0 is installed as an upgrade, or the root directory where this version is installed as the initial version).

Using %USERNAME% in the Home Directory Path

When typing the path for a home directory, %USERNAME% can be entered as the last subdirectory in the path, and the system later substitutes the user name of each user account for %USERNAME%. This is useful when multiple user accounts are selected.

For example, to administer six user accounts you might click the **Connect** option, select the drive letter H and, in **To**, type the path **\\airedale\users\%username%**. As the changes are saved, the system substitutes the actual user name for the %USERNAME% entry for each user account.

Notes

- MS-DOS client computers are not able to access the home directory on a FAT volume if the user name of at least one of the selected user accounts is longer than 8 characters (or has an extension name longer than 3 characters). These computers can access the root directory of the share instead.
- On NTFS volumes, you can use %USERNAME% regardless of the user-name length.

To manage logon hours

1 Click **Hours** in the **New User**, **Copy Of**, or **User Properties** dialog box.

2 In the **Logon Hours** dialog box, select the hours to be administered:

- To select one hour, click that hour.
- To select a block of time, click the beginning hour and drag through the rows and columns to the ending hour.
- To select an entire day, click that day in the left column.
- To select one hour for all seven days, click the top of that column.
- To select the entire week, click the upper-left box (above Sunday).

3 To allow connections during the selected hours, click **Allow**.

Or, to deny connections during the selected hours, click **Disallow**.

4 Repeat steps 2 and 3, as necessary.

Note

- The default setting allows users to connect at any time, but you can restrict individual users to certain days and hours. These settings affect only connections to the server; they do not affect a user's ability to use a workstation.

To manage logon workstations

1. Click **Logon From** in the **New User**, **Copy Of**, or **User Properties** dialog box.
2. Select either **User May Log On To All Workstations** or **User May Log On To These Workstations**.
3. If you select **User May Log On To These Workstations**, type a computer name in at least one and up to eight of the numbered boxes.

Note

The default is to allow a user to log on from any workstation, but you can restrict a user to logging on from only specified workstations.

To manage user account information

1 Click **Account** in the **New User**, **Copy Of**, or **User Properties** dialog box.

2 Under **Account Expires**, select either **Never** or **End Of**.

3 If you select **End Of**, enter an expiration date in **End Of**.

4 Under **Account Type**, select either **Global Account** or **Local Account**.

Note

Most accounts are global accounts. Assign local accounts only when a trust relationship does not exist with the user's home domain.

To disable or enable a user account

1 In the User Manager window, select one or more user accounts.

2 On the **User** menu, click **Properties**.

3 To prevent logons to the selected user accounts, select the **Accounts Disabled** check box.

Or, to permit logons to the selected user accounts, click to clear the **Accounts Disabled** check box.

Notes

- A disabled user account still exists and appears in the User Manager for Domains window, but logons to that account are not permitted. You can activate disabled accounts at any time.
- The built-in Administrator account cannot be disabled.

See Also

Selecting User Accounts

Deleting User Accounts

To delete one or more user accounts

1 In the User Manager window, select one or more user accounts.

2 On the **User** menu, click **Delete**.

3 If a confirmation message appears, click **OK**.

4 When the delete message appears, click **Yes**.

Or, if you selected multiple user accounts, click **Yes To All**.

Important

Deleted user accounts cannot be recovered. It is a good idea to first disable a user account, and then periodically delete the disabled accounts.

Note

The built-in Administrator and Guest accounts cannot be deleted.

See Also

Selecting User Accounts

Disabling and Enabling User Accounts

Using Low Speed Connection

To rename a user account

1 In the User Manager for Domains window, select one user account.

2 On the **User** menu, click **Rename**.

3 In **Change To**, type a user name.

Note

A user name cannot be identical to any other user or group name of the domain or computer being administered. It can contain up to 20 uppercase or lowercase characters except for the following:

" / \ [ ] : ; | = , + * ? < >

A user name cannot consist solely of periods (.) and spaces.

See Also

Selecting User Accounts

Using Low Speed Connection

To select multiple user accounts

1 In the User Manager for Domains window, do one of the following:

- Select the user accounts you want as the initial members of the new group
- Select any group to ensure no user accounts are initially selected.

2 On the **User** menu, click **Select Users**.

3 To select the member users of a group, select the group from the list, and then click **Select**.

4 To deselect the member users of a group, select the group from the list, and then click **Deselect**.

5 Repeat steps 3 and 4 as necessary.

When you finish selecting accounts, you can apply commands on the **User** menu to those accounts.

Notes

- Only the user accounts listed in the User Manager for Domains window can be selected or deselected. Although local groups can contain user or group accounts not from the local domain, those accounts are not affected by choices made in the **Select Users** dialog box.
- When **Low Speed Connection** is selected, **Select Users** is unavailable.
- You can hold down Ctrl and then click to select specific user accounts in the User Manager for Domains window, or hold down Shift and click to select a contiguous range of user accounts.

See Also

Using Low Speed Connection

To create a new global group

1. In the User Manager for Domains window, do one of the following:
   - Select the user accounts you want as the initial members of the new group.
   - Select any group to ensure no user accounts are initially selected.
2. On the **User** menu, click **New Global Group**.
3. In **Group Name**, type a group name.
4. In **Description**, type a description.
5. To add members, select one or more user accounts in **Not Members**, and then click **Add**.
6. To remove members from the new group, select one or more user accounts in **Members**, and then click **Remove**.

Notes

- A global group name cannot be identical to any other user or group name of the domain or computer being administered. It can contain up to 20 uppercase or lowercase characters except for the following:

  `" / \ [ ] : ; | = , + * ? < >`

  A global group name cannot consist solely of periods (.) and spaces.
- **New Global Group** is unavailable when **Low Speed Connection** is selected, or when you administer a computer running Windows NT Workstation or Windows NT Server that is not a domain controller.

See Also

Selecting User Accounts

Using Low Speed Connection

To make a copy of an existing global group

1 In the User Manager for Domains window, select one global group.

2 On the **User** menu, click **Copy**.

3 In **Group Name**, type a new group name.

4 You can make changes, as follows:

- To change the description, type new text in **Description**.
- To add members, select one or more user accounts in **Not Members**, and then click **Add**.
- To remove members from the global group, select one or more user accounts in **Members**, and then click **Remove**.

Notes

- The main advantage of copying a group is that the new group will have the same members as the original group. However, the permissions and rights of the original group are not copied to the new group.
- Global groups cannot be managed when **Low Speed Connection** is selected, or when you are administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller.

See Also

Using Low Speed Connection

To modify an existing global group

1. In the User Manager for Domains window, select the global group, and then click **Properties** on the **User** menu.
2. To change the description, type new text in **Description**.
3. To add members, select one or more user accounts in **Not Members**, and then click **Add**.
4. To remove members, select one or more user accounts in **Members**, and then click **Remove**.

Note

Global groups cannot be managed when **Low Speed Connection** is selected, or when you are administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller.

See Also

Using Low Speed Connection

To delete a global group

1 In the User Manager for Domains window, select one global group.

2 On the **User** menu, click **Delete**.

Notes

- Deleting a global group removes only that group; it does not delete the user accounts that were members of the deleted global group.
- A deleted group cannot be recovered. If you delete a group and then create another group with the same group name, the new group will not have any of the rights or permissions that were previously granted to the old group.
- A global group that is the primary group for one or more user accounts cannot be deleted.
- Built-in groups cannot be deleted.

See Also

Using Low Speed Connection

To create a new local group

1 In the User Manager for Domains window, do one of the following:

- Select the user accounts you want as the initial members of the new group.
- Select any group to ensure no user accounts are initially selected.

2 On the **User** menu, click **New Local Group**.

3 In **Group Name**, type a name for the new group.

4 If necessary, click **Show Full Names**.

This can be a lengthy operation if the group is large.

5 In **Description**, type a description of the new group.

6 To add members, click **Add** and then complete the **Add Users and Groups** dialog box.

7 To remove members from the new group, select one or more names in **Members**, and then click **Remove**.

Notes

- A local group name cannot be identical to any other group or user name of the domain or computer being administered. It can contain up to 256 uppercase or lowercase characters except for the backslash character (\).
- You can add user accounts and global groups from this domain and from trusted domains.

See Also

Selecting User Accounts

Using Low Speed Connection

To make a copy of an existing local group

1 In the User Manager for Domains window, select a local group.

2 On the **User** menu, click **Copy**.

3 In **Group Name**, type a new group name.

4 You can make changes, as follows:

- To change the description, type new text in **Description**.
- To add members, click **Add**, and complete the **Add Users and Groups** dialog box.
- To remove members from the local group, select one or more names in **Members**, and then click **Remove**.

Notes

- You can add user accounts and global groups from this domain and from trusted domains.
- The main advantage of copying a group is that the new group will have the same members as does the original group. However, the permissions, rights, and built-in abilities of the original group are not copied to the new group.
- A local group name cannot be identical to any other group or user name of the domain or computer being administered. It can contain up to 256 uppercase or lowercase characters except for the backslash character (\).

See Also

Using Low Speed Connection

To modify a local group

1 In the User Manager for Domains window, select the local group, and then click **Properties** on the **Use**r menu.

2 If necessary, click **Show Full Names**.

This can be a lengthy operation if the group is large.

3 To change the description, type new text in **Description**.

4 To add members, click **Add**, and complete the **Add Users and Groups** dialog box.

5 To remove members, select one or more names in **Members**, and then click **Remove**.

Note

You can add user accounts and global groups from this domain and from trusted domains.

See Also

Using Low Speed Connection

To delete a local group

1 In the User Manager for Domains window, select one local group.

2 On the **User** menu, click **Delete**.

3 If a confirmation message appears, click **OK**.

4 When the delete message appears, click **Yes**.

Notes

- A deleted group cannot be recovered. If you delete a group and then create another group with the same group name, the new group will not have any of the rights or permissions that were previously granted to the old group.
- Deleting a local group removes only that group; it does not delete the user accounts and global groups that were members of the deleted local group.
- Built-in groups cannot be deleted.

See Also

Using Low Speed Connection

To manage the Account policy

1 On the **Policies** menu, click **Account**.

2 Enter the values you want under any of the groups: **Maximum Password Age**, **Minimum Password Age**, **Minimum Password Length**, and **Password Uniqueness**.

Or, click **Password Never Expires**, **Allow Changes Immediately**, **Permit Blank Password**, or **Do Not Keep Password History**.

3 Click **Account lockout**, and then enter values in **Lockout after**, **Reset count after**, and **Lockout Duration**.

Or, click **No account lockout**.

4 If necessary, select or clear the **Forcibly disconnect remote users from server when logon hours expire** check box.

5 If necessary, select or clear the **Users must log on in order to change password** check box.

Notes

- Before you click **OK**, review the following guidelines:
- If you select **Allow Changes Immediately** under **Minimum Password Age**, you should also click **Do Not Keep Password History** under **Password Uniqueness**.
- If you enter a value under **Password Uniqueness**, you should also enter a value for **Allow Changes in _ Days** under **Minimum Password**.
- Maximum values for the various options are as follows:
- 1 to 999 days for **Maximum Password Age** and **Minimum Password Age**.
- 1 to 14 characters for **Minimum Password Length**.
- 1 to 24 passwords for **Remember _ Passwords** under **Password Uniqueness**.

To manage the Account policy

1. On the **Policies** menu, click **Account**.
2. Enter the values you want under any of the groups: **Maximum Password Age**, **Minimum Password Age**, **Minimum Password Length**, and **Password Uniqueness**.

   Or, click **Password Never Expires**, **Allow Changes Immediately**, **Permit Blank Password**, or **Do Not Keep Password History**.
3. If necessary, select or clear the **Forcibly disconnect remote users from server when logon hours expire** check box.
4. If necessary, select or clear the **Users must log on in order to change password** check box.

Notes

- Before you click **OK**, review the following guidelines:
- If you click **Allow Changes Immediately** under **Minimum Password Age**, you should also click **Do Not Keep Password History** under **Password Uniqueness**.
- If you enter a value under **Password Uniqueness**, you should also enter a value for **Allow Changes in _ Days** under **Minimum Password**.
- Maximum values for the various options are as follows:
- 1 to 999 days for **Maximum Password Age** and **Minimum Password Age**.
- 1 to 14 characters for **Minimum Password Length**.
- 1 to 24 passwords for **Remember _ Passwords** under **Password Uniqueness**.

To manage the User Rights policy

1 On the **Policies** menu, click **User Rights**.

2 Select a user right from those listed in **Right**.

The users and groups who currently have that right appear under **Grant To**.

3 To grant the selected right to additional groups or user accounts, click **Add**, and complete the **Add Users and Groups** dialog box.

4 To remove a group or user account from the list, select a name in the **Grant To** box, and then click **Remove**.

5 Repeat steps 2 through 4, as necessary.

6 To administer the advanced user rights, select the **Show Advanced User Rights** check box and repeat steps 2 through 4, as necessary.

Notes

- In most situations, the easiest way to provide rights to a user is to add that user's account to one of the built-in groups that already possesses the needed rights, rather than by managing the **User Rights** policy.
- Advanced rights are primarily used by programmers writing applications for computers running Windows NT Workstation and Windows NT Server.

See Also

The User Rights

To manage the Audit Policy

1 On the **Policies** menu, click **Audit**.

2 To record events in the security log, click **Audit These Events**.

Or, to not record any events in the security log, click **Do Not Audit**.

3 If you selected **Audit These Events**, select or clear the **Success** and **Failure** check boxes for each type of event.

Notes

- When administering domains, the **Audit** policy affects the security logs of all domain controllers in the domain because they share the same **Audit** policy.
- When administering a computer running Windows NT Workstation or Windows NT Server that is not a domain, the **Audit** policy affects only the security log of that computer.
- Entries in a security log can be reviewed using Event Viewer.
- Because the security log is limited in size, carefully select which events to log. The maximum size of each computer's security log is defined in Event Viewer.

To add a trusting domain

1 If necessary, click **Select Domain** on the **User** menu, and complete the **Select Domain** dialog box, specifying the name of the domain that will add to its list of trusting domains.

2 On the **Policies** menu, click **Trust Relationships**.

3 Click **Add** and type the name of the Windows NT Server domain that will trust your domain in **Trusting Domain**.

5 Type a password in both **Password** and **Confirm Password**.

Passwords are case sensitive.

6 Provide the password to the administrator of the domain that you have added to the **Trusting Domains** list.

That administrator must complete the trust relationship by adding your domain to the list of trusted domains.

Notes

- Establishing a trust relationship requires both domain administrators to take action in their respective domains.
- You can type a domain name using both uppercase and lowercase characters, but the name is always displayed in uppercase.

See Also

Adding a Trusted Domain

To add a trusted domain

1. Obtain a password from the administrator of the domain that will be trusted.
2. If necessary, click **Select Domain** on the **User** menu, and complete the **Select Domain** dialog box, specifying the name of your domain that will be configured to trust the other domain.
3. On the **Policies** menu, click **Trust Relationships**.
4. Click **Add**, and type the name of the Windows NT Server domain that is to be trusted in **Trusted Domains**.
5. In **Password**, type the password required by that domain.

   Passwords are case sensitive.

Notes

- Establishing a trust relationship requires both domain administrators to take action in their respective domains.
- You can type a domain name using both uppercase and lowercase characters, but the name is always displayed in uppercase.

See Also

Adding a Trusting Domain

The User Rights

The list below provides descriptions of user rights that can be managed with the **User Rights** policy. Two advanced user rights (**Bypass traverse checking**, and **Log on as a service**) may be of interest to administrators, and are therefore included in the list.

Click the following for more information:

- Access this computer from network
- Add workstations to domain
- Back up files and directories
- Change the system time
- Force shutdown from a remote system
- Load and unload device drivers
- Log on locally
- Manage auditing and security log
- Restore files and directories
- Shut down the system
- Take ownership of files or other objects
- Bypass traverse checking (advanced right)
- Log on as a service (advanced right)

Note

- Some advanced user rights can also be managed with the **User Rights** policy. Most of these are useful only to programmers writing applications for computers running Windows NT Workstation or Windows NT Server, and will not usually be granted to a group or user. For information about advanced user rights, see the Win32 Programmer's Reference in the Win32 SDK documentation.

See Also

Managing the User Rights Policy

Access this computer from network

Allows a user to connect to the computer over the network.

Notes

- When administering a domain, this right applies to all domain controllers in the domain.
- When administering a workstation, this right applies to only that workstation.

Add workstations to domain

Allows a user to add workstations to the domain. Adding a workstation to a domain enables the workstation to recognize the domain's user and global groups accounts.

Note

By default, members of domain Administrators and Account Operators groups have the right to add a workstation to a domain. This right cannot be taken away. They can also grant this right to other users.

Back up files and directories

Allows a user to back up files and directories of the computer. This right supersedes files and directory permissions.

Notes

- When administering a domain, this right applies to the primary and backup domain controllers of the domain.
- When administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller, this right applies to only that computer.

Change the system time

Allows a user to set the time for the internal clock of the computer.

Notes

- When administering a domain, this right applies to the primary and backup domain controllers of the domain.
- When administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller, this right applies to only that computer.

Force shutdown from a remote system

This right is not currently implemented. It is reserved for future use.

Load and unload device drivers

Allows a user to dynamically load and unload device drivers.

Notes

- When administering a domain, this right applies to the primary and backup domain controllers of the domain.
- When administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller, this right applies to only that computer.

Log on locally

Allows a user to log on at the computer.

Notes

- Users must have this right to log on to Terminal Server from a client computer.
- When administering a domain, this right applies to the primary and backup domain controllers of the domain.
- When administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller, this right applies to only that computer.

Manage auditing and security log

Allows a user to manage the auditing of files, directories, and other objects. A user with this right can use the **Security** tab in the **Properties** dialog box to specify auditing options for the selected objects, users and groups, and types of access.

This right does not enable a user to use **Audit** on the **Policies** menu to configure security events to be audited. This ability is always held only by Administrators.

Audited events can be viewed in the security log using Event Viewer.

Notes

- When administering a domain, this right applies to the primary and backup domain controllers of the domain.
- When administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller, this right applies to only that computer.

Restore files and directories

Allows a user to restore files and directories of the computer. This right supersedes files and directory permissions.

Notes

- When administering a domain, this right applies to the primary and backup domain controllers of the domain.
- When administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller, this right applies to only that computer.

Shut down the system

Allows a user at the computer to shut down a computer running Windows NT Workstation or Windows NT Server.

Notes

- When administering a domain, this right applies to the primary and backup domain controllers of the domain.
- When administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller, this right applies to only that computer.

Take ownership of files or other objects

Allows a user to take ownership of files, directories, and other objects of the computer.

Notes

- When administering a domain, this right applies to the primary and backup domain controllers of the domain.
- When administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller, this right applies to only that computer.

Bypass traverse checking

Allows a user to change directories and travel through directory trees of the computer, even if the user has no permissions for the traversed directories. This is an advanced user right.

Notes

- When administering a domain, this right applies to the primary and backup domain controllers of the domain.
- When administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller, this right applies to only that computer.

Log on as a service

Allows a process to register with the system as a service. This is an advanced user-right.

Notes

- When administering a domain, this right applies to the primary and backup domain controllers of the domain.
- When administering a computer running Windows NT Workstation or Windows NT Server that is not a domain controller, this right applies to only that computer.

User

The name of the user whose properties you are viewing.

Object ID

The internal ID number assigned to this user account.

Grace Logins

Grace logins are the number of extra times a user can log in after his or her password has expired. Grace logins provide the user with a chance to change the expired password. The number of grace logins a user has remaining is displayed.

To set the maximum number of grace logins

- Click **Limit Grace Logins**, and then enter a number in **Allow**.

  Or, click **Unlimited Grace Logins**.

Edit Login Script

Opens a dialog box that you can use to create or modify the user’s personal login script.

Note

Do not use this button to edit the server’s system login script. Instead, use Notepad or another text editor to edit the NET$LOG.DAT file, in the SYSVOL\PUBLIC directory.

Edit Login Script

Used to create or modify the personal login script for this user.

Note

To edit the server’s system login script, use Notepad or another text editor to edit the NET$LOG.DAT file in the SYSVOL\PUBLIC directory.

To grant dialin permission to users connecting from remote locations

1 In the User Manager for Domains window, select one or more user accounts.

2 On the **User** menu, click **Properties**.

3 In the **User Properties** dialog box, click **Dialin**.

4 In the **Dialin Information** dialog box, click **Grant dialin permission to user**.

5 Under **Call Back**, select only one of the following:

- To disable callback for a user account, click **No Call Back** (the default setting).
- To cause the server to prompt the user for a telephone number, click **Set By Caller**.
- To cause the server to call the user at a fixed telephone number, click **Preset To**, and then type in the fixed phone number.

  The server will call the user back at this number only.

Click **Help Topics** for a list of Help topics.

Confirm that there are no open sessions from this computer to the primary domain controller in the target trusted domain.

1 In Windows NT Explorer, click **Disconnect Network Drive** on the **Tools** menu to disconnect any connections currently open to the primary domain controller.

2 At the command prompt, use the **net use** command to disconnect any remaining connections.

3 Try again to add the trusted domain.

New User

Used to create new user accounts.

For more information about this dialog box, click the following:

- Username
- Full Name
- Description
- Password and Confirm Password
- User Must Change Password At Next Logon
- User Cannot Change Password
- Password Never Expires
- Account Disabled
- Groups
- TS Config
- Profile
- Hours
- Logon To
- Account
- Dialin
- Add

See Also

Creating a New User Account

Username

The user name identifies the user account. A user name cannot be identical to any other user or group name of the domain or computer being administered. It can contain up to 20 uppercase or lowercase characters except for the following:

" / \ [ ] : ; | = , + * ? < >

A user name cannot consist solely of periods (.) and spaces.

Username

The user name identifies the user account. The user name cannot be changed from this dialog box. To change the user name of an existing user account, click **Rename** on the **User** menu.

Users

The user accounts being administered. Any changes made to the entries and settings of this dialog box are applied to all these accounts.

Full Name

The full name is the user's complete name. It is a good idea to establish a standard for entering full names so that they always begin with either the first name (Louise G. Morgan) or the last name (Morgan, Louise G.). The first few characters of the full name determine the user account sort order in the User Manager for Domains window when **Sort by Full Name** is selected on the **View** menu.

Description

The description can be any text describing the user account or the user.

Description

The description is copied from the original account, and can be any text describing the user account or the user. You can accept the description that was copied, or you can replace it by typing.

Description

The description can be any text describing the user account or the user. You can accept the existing description, or you can replace it by typing.

Description

If all the selected user accounts have an identical description, that text appears in **Description**. If one or more of the accounts have a different description, **Description** is empty. You can leave the descriptions unchanged, or you can type a new description that will replace existing descriptions in all the selected user accounts.

Password and Confirm Password

A password can be up to 14 characters and is case sensitive. To enter or change a password, you must type the exact same set of characters in both **Password** and **Confirm Password**.

Password and Confirm Password

A password can be up to 14 characters. It is case sensitive.

You can change the existing password or leave it unchanged. To change a password, you must type the exact same set of characters in both **Password** and **Confirm Password**.

User Must Change Password At Next Logon

Forces the user to change the password at the next logon.

User Must Change Password At Next Logon

After a copy, this check box is usually selected, regardless of its setting in the original account. However, if **User Cannot Change Password** is selected in the original account, that selection is copied instead.

User Must Change Password At Next Logon

After a copy, this check box is initially cleared regardless of the setting in the original account.

User Cannot Change Password

Usually applied only to user accounts that are used by more than one person, such as the Guest account. This setting has no effect on members of the Administrators local group.

User Cannot Change Password

Usually applied only to user accounts that are used by more than one person, such as the Guest account. This setting has no effect on members of the Administrators local group.

During a copy, the setting for this check box is copied from the original account.

Users Cannot Change Password

Usually applied only to user accounts that are used by more than one person, such as the Guest account. This setting has no effect on members of the Administrators local group.

If all the selected user accounts have the same setting for this check box, that setting is displayed. If one or more of the accounts have different settings, the check box is undefined (grey).

User Cannot Change Password

Usually applied only to user accounts that are used by more than one person, such as the Guest account. This setting has no effect on members of the Administrators local group.

User Cannot Change Password

Usually applied only to user accounts that are used by more than one person, such as the Guest account. This setting has no effect on members of the Administrators local group.

During a copy, the setting for this check box is copied from the original account.

Users Cannot Change Password

Usually applied only to user accounts that are used by more than one person, such as the Guest account. If all the selected user accounts have the same setting for this check box, that setting is displayed. If one or more of the accounts have different settings, the check box is undefined (grey).

Password Never Expires

Prevents the password from expiring, overriding **Maximum Password Age** and **User Must Change Password At Next Logon**. Select this check box for user accounts that will be assigned to services (for example, to Directory Replicator) using Server Manager, or Services in Control Panel.

Password Never Expires

Prevents the password from expiring, overriding **Maximum Password Age** and **User Must Change Password At Next Logon**. Select this check box for user accounts that will be assigned to services (for example, to Directory Replicator) using Server Manager, or Services in Control Panel.

During a copy, the setting for this check box is copied from the original account.

Password Never Expires

Prevents the password from expiring, overriding **Maximum Password Age** in the Account policy. Select this check box for user accounts that will be assigned to services (for example, to Directory Replicator) using Server Manager, or Services in Control Panel.

If all the selected user accounts have the same setting, this check box is available. If one or more of the accounts have different settings, the check box is undefined (grey).

Account Disabled

Prevents use of an account.

You can disable a new account to create an inactive, template account that you can copy to create new accounts. Or, you can temporarily disable an account if it does not need to be used until a later date.

The built-in Administrator account cannot be disabled.

Account Disabled

Prevents use of an account. During a copy, this check box is cleared, regardless of the setting in the original account.

You can disable a new account to create an inactive, template account that you can copy to create new accounts. Or, you can temporarily disable an account if it does not need to be used until a later date.

The built-in Administrator account cannot be disabled.

Accounts Disabled

Prevents use of an account.

You can disable a new account to create an inactive template that you can copy to create new accounts, or you can temporarily disable an account if it does not need to be used until a later date.

If all the selected user accounts have the same setting, this check box is available. If one or more of the accounts have different settings, the check box is undefined (grey).

Account Locked Out

If the account is currently locked out, this check box is selected. Otherwise, it is cleared and unavailable.

You cannot lock an account using this check box; you can use it only to unlock accounts that become locked because of too many failed logon attempts. If you want to prevent use of an account, disable the account.

Accounts Locked Out

If all selected accounts are currently locked out, this check box is selected. If only some of the accounts are locked out, the check box is undefined (grey). If none are locked, the check box is cleared and unavailable.

You can use this check box only to unlock accounts that become locked because of too many failed logon attempts; you cannot use it to lock accounts. If you want to prevent the use of accounts, disable them.

Groups

Used to specify the groups in which the user account has membership.

Groups

Used to specify the group memberships of the new user account. The initial group memberships for the new user account are copied from the original account.

Groups

Used to specify the groups in which the selected user accounts will have membership.

Config

Used to specify Terminal Server configuration information for the user account.

Config

Used to specify Terminal Server configuration information for the new user account. The initial Terminal Server configuration information for the new user account is copied from the original account.

Config

Used to specify Terminal Server configuration information for the selected user accounts.

Profile

Used to assign a user profile path, logon script name, or home directory path to the user account.

Profile

Used to assign a user profile path, logon script name, or home directory path to the selected user accounts.

Profile

Used to assign a user profile path, logon script name, or home directory path to the user account.

Profile

Used to assign a user profile path, logon script name, or home directory path to the selected user accounts.

Dialin

Used to grant permission to use Dial-Up Networking to the selected user account.

Dialin

Used to grant permission to use Dial-Up Networking to all the selected user accounts.

Hours

Used to restrict the hours during which the user can connect to a server. This setting does not affect a user's ability to use a workstation.

Hours

Used to restrict the hours during which the user can connect to a server. This does not affect a user's ability to use a workstation.

The initial settings for the logon hours are copied from the original account.

Hours

Used to restrict the hours during which all the selected user accounts can connect to a server. This does not affect those users' ability to use workstations.

Logon To

Used to restrict the workstations from which a user will be permitted to log on to this domain account.

Logon To

Used to restrict the workstations from which a user will be permitted to log on to this domain account.

The initial settings for the logon workstations are copied from the original account.

Logon To

Used to restrict the workstations from which users will be permitted to log on to these domain accounts.

Account

Used to manage the account expiration date and to specify whether this is a global or a local user account.

Account

Used to manage the account expiration date and to specify whether this is a global or a local user account.

The initial settings for this information are copied from the original user account.

Account

Used to manage the account expiration date for all the selected user accounts and to specify whether these are global or local user accounts.

Account

Used to manage the account expiration date for the user account and to specify the privilege level.

Account

Used to manage the account expiration date for all the selected user accounts and to specify their privilege level.

Add

Adds the new user account.

The **New User** dialog box reverts to its default settings. You can now add another new user account.

Add

Adds the new user account.

The **Copy Of** dialog box reverts to its initial settings. You can now add another copy of the original account.

New User

Used to add new user accounts.

For more information about this dialog box, click the following:

- Username
- Full Name
- Description
- Password and Confirm Password
- User Must Change Password At Next Logon
- User Cannot Change Password
- Password Never Expires
- Account Disabled
- Groups
- TS Config
- Profile

See Also

Creating a New User Account

New User

Used to add new user accounts.

For more information about this dialog box, click the following:

- Username
- Full Name
- Description
- Password and Confirm Password
- User Cannot Change Password
- Account Disabled
- Groups
- TS Config
- Profile
- Hours
- Logon To
- Account
- Dialin
- Add

See Also

Creating a New User Account

Copy of User Account

Used to create new user accounts copied from an existing one. For example, you can copy an existing account in order to add a new user who will belong to the same groups as the account you copy.

For more information about this dialog box, click the following:

- Username
- Full Name
- Description
- Password and Confirm Password
- User Must Change Password At Next Logon
- User Cannot Change Password
- Password Never Expires
- Account Disabled
- Groups
- TS Config
- Profile
- Hours
- Logon To
- Account
- Dialin
- Add

See Also

Copying a User Account

Copy of User Account

Used to create new user accounts copied from an existing one. For example, you can copy an existing account in order to add a new user who will belong to the same groups as the account you copy.

For more information about this dialog box, click the following:

- Username
- Full Name
- Description
- Password and Confirm Password
- User Must Change Password At Next Logon
- User Cannot Change Password
- Password Never Expires
- Account Disabled
- Groups
- TS Config
- Profile
- Hours
- Logon To
- Account
- Dialin

See Also

Copying a User Account

Copy of User Account

Used to create new user accounts copied from an existing one. For example, you can copy an existing account in order to add a new user who will belong to the same groups as the account you copy.

For more information about this dialog box, click the following:

- Username
- Full Name
- Description
- Password and Confirm Password
- User Cannot Change Password
- Account Disabled
- Groups
- TS Config
- Profile
- Hours
- Logon To
- Account
- Dialin
- Add

See Also

Copying a User Account

User Properties

Used to modify the selected user account.

For more information about this dialog box, click the following:

- Username
- Full Name
- Description
- Password and Confirm Password
- User Must Change Password At Next Logon
- User Cannot Change Password
- Password Never Expires
- Account Disabled
- Account Locked Out
- Groups
- TS Config
- Profile
- Hours
- Logon To
- Account
- Dialin

Note

- If you have additional services installed, you may have additional options. For information about those options, see the documentation for those services.

See Also

Managing Properties for One User Account

User Properties

Used to modify the selected user account.

For more information about this dialog box, click the following:

- Username
- Full Name
- Description
- Password and Confirm Password
- User Must Change Password At Next Logon
- User Cannot Change Password
- Password Never Expires
- Account Disabled
- Account Locked Out
- Groups
- TS Config
- Profile
- Hours
- Logon To
- Account
- Dialin

See Also

Managing Properties for One User Account

User Properties

Used to modify the selected user account.

For more information about this dialog box, click the following:

- Username
- Full Name
- Description
- Password and Confirm Password
- User Cannot Change Password
- Account Disabled
- Account Locked Out
- Groups
- TS Config
- Profile
- Hours
- Logon To
- Account
- Dialin

See Also

Managing Properties for One User Account

User Properties

Used to modify all the selected user accounts in the same way.

For more information about this dialog box, click the following:

- Users
- Description
- Users Cannot Change Password
- Password Never Expires
- Accounts Disabled
- Accounts Locked Out
- Groups
- TS Config
- Profile
- Hours
- Logon To
- Account
- Dialin

Note

- If you have additional services installed, you may have additional options. For information about those options, see the documentation for those services.

See Also

Managing Properties for Multiple User Accounts

User Properties

Used to modify all the selected user accounts in the same way.

For more information about this dialog box, click the following:

- Users
- Description
- Users Cannot Change Password
- Password Never Expires
- Accounts Disabled
- Accounts Locked Out
- Groups
- TS Config
- Profile
- Hours
- Logon To
- Account
- Dialin

See Also

Managing Properties for Multiple User Accounts

User Properties

Used to modify all the selected user accounts in the same way.

For more information about this dialog box, click the following:

- Users
- Description
- Users Cannot Change Password
- Accounts Disabled
- Accounts Locked Out
- Groups
- TS Config
- Profile
- Hours
- Logon To
- Account
- Dialin

See Also

Managing Properties for Multiple User Accounts

Group Memberships

Used to establish or change the memberships this user account has in the groups of this domain.

For more information about this dialog box, click the following:

- User
- Member Of
- Not Member Of
- Add
- Remove
- Set
- Primary Group

See Also

Managing Group Memberships for One User Account

User

The user account being administered.

Users

The selected user accounts.

Member Of

The user account is a member of these groups.

All Are Members Of

Every one of the selected user accounts belongs to these groups.

Note

If even one of the selected user accounts does not belong to a particular group, that group does not appear here.

Not Member Of

The user account does not belong to these groups.

Not All Are Members Of

If even one of the selected user accounts is not a member of a particular group, that group appears in **Not All Are Members Of**.

Add

Adds a user account to one or more groups selected in **Not Member Of**. You can do this either by clicking **Add** or by dragging from list to list.

Add

Adds a user account to one or more groups selected in **Not Member Of**. You can do this either by clicking **Add** or by dragging from list to list.

Remove

Removes a user account from one or more groups selected in **Not Member Of**. You can do this either by clicking **Remove** or by dragging from list to list.

You cannot remove the primary group.

Remove

Removes a user account from one or more groups selected in **Not Member Of**. You can do this either by clicking **Remove** or by dragging from list to list.

You cannot remove the primary group.

Set

Changes the primary group for a user account to the selected global group in **Member Of**.

A primary group is used when a user running Windows NT Services for Macintosh or POSIX applications logs on. Only a global group can be set as the primary group. A user account cannot be removed from membership in its primary group.

Set

Changes the primary group for a user account to the selected global group in **Member Of**.

A primary group is used when a user running Windows NT Services for Macintosh or POSIX applications logs on. Only a global group can be set as the primary group. A user account cannot be removed from membership in its primary group.

Primary Group

The global group set as the primary group for this user. A primary group is used when a user running Windows NT Services for Macintosh or POSIX applications logs on. Only a global group can be set as the primary group. A user account cannot be removed from membership in its primary group.

Primary Group

The global group set as the primary group for this user. A primary group is used when a user running Windows NT Services for Macintosh or POSIX applications logs on. Only a global group can be set as the primary group. A user account cannot be removed from membership in its primary group.

Group Memberships

Used to establish or change the group memberships for all the selected user accounts.

For more information about this dialog box, click the following:

- User
- Member Of
- Not Member Of
- Add
- Remove

See Also

Managing Group Memberships for One User Account

Group Memberships

Used to add all the selected user accounts to one or more groups of this domain or workstation, or to remove all the selected user accounts from one or more groups of this domain or workstation.

For more information about this dialog box, click the following:

- Users
- All Are Members Of
- Not All Are Members Of
- Add
- Remove
- Set
- Primary Group

See Also

Managing Group Memberships for Multiple User Accounts

Group Memberships

Used to add all the selected user accounts to one or more groups of this domain or workstation, or to remove all the selected user accounts from one or more groups of this domain or workstation.

For more information about this dialog box, click the following:

- Users
- All Are Members Of
- Not All Are Members Of
- Add
- Remove

See Also

Managing Group Memberships for Multiple User Accounts

User Environment Profile

Used to add a user profile path, logon script name, or home directory path to this user account.

For more information about this dialog box, click the following:

- User
- User Profile Path
- Terminal Server Profile Path
- Logon Script Name
- Home Directory
- Terminal Server Home Directory
- Local Path
- Connect To
- Using %USERNAME% in the Home Directory Path

Note

- If you have additional services installed, you may have additional options. For information about those options, see the documentation for those services.

See Also

Managing the User Environment

Terminal Server User Configuration

Used to configure the selected user accounts for Terminal Server access.

For more information about this dialog box, click the following:

- Allow Logon to Terminal Server
- Timeout settings
- Initial Program
- Client Devices
- Broken or timed-out connection
- Reconnect sessions
- Modem callback
- Shadowing

See Also

Managing Terminal Server User Configuration

Allow Logon to Terminal Server

Specifies whether the user account is permitted to log on to Terminal Server.

Timeout settings

These settings (specified in minutes) specify time-out intervals for a Terminal Server connection. The time-outs are:

- **Connection** Specifies the maximum connection duration. If a connection duration is specified, the session is disconnected or terminated when the specified duration elapses. If **No Timeout** is selected, the connection timer is disabled.
- **Disconnection** Specifies the maximum duration that a disconnected session is retained. If a duration is specified, sessions in the disconnected state are terminated when the specified duration elapses. If **No Timeout** is selected, the disconnection timer is disabled.
- **Idle** Specifies the maximum idle time (time without client activity) allowed before the session is disconnected or terminated. If an idle duration is specified, the session is disconnected or terminated when the specified interval elapses without any activity at the client computer. If **No Timeout** is specified, the idle timer is disabled.

Initial Program

Specifies the program to execute automatically when a user logs on to Terminal Server.

- To specify a program, enter the appropriate data into **Command Line** and **Working Directory**.
- To inherit these values from the client, select the **(inherit client config)** checkbox.

Client Devices

These settings specify whether or not Terminal Server automatically reestablishes client device mappings at logon.

- To automatically reconnect to mapped client drives, select the **Connect client drives at Logon** checkbox.
- To automatically reconnect to mapped client printers, select the **Connect client printers at Logon** checkbox.
- To use the client's default printer as the default for printing from the client session, select the **Default to main client printer** checkbox.

These options are supported for Citrix ICA-based clients only. For Microsoft Terminal Server Clients, use logon scripts to map drives and printers.

Broken or timed-out connection

This selects the action taken when the user's session is disconnected due to a disconnect request, connection error, modem carrier drop, idle time-out, or connection time-out.

- Select **disconnected** to place the session in the disconnected state.
- Select **reset** to terminate the session.

Reconnect sessions

This specifies whether a disconnected session can be reconnected using any client computer or using the original client only.

- To allow reconnections from any computer, select **from any client**.
- To restrict reconnections to the original computer, select **from previous client only**.

This option is supported only for Citrix ICA-based clients that provide a serial number when connecting.

Modem callback

Three options are available to configure the user session for modem callback:

- **disabled** The server does not attempt to call the user back.
- **to a roving phone number** The server prompts the user to enter a phone number and calls the user back at that phone number. You can specify a default phone number in **Phone Number**.
- **to a fixed phone number** The server automatically attempts to call the user back at the phone number specified in **Phone Number**.

These options are supported for Citrix ICA-based clients only. Use Microsoft Remote Access Service (RAS) to configure callback options for Terminal Server clients.

Shadowing

Specifies whether the user session can be shadowed.

- Select **is disabled** to disable shadowing of the user's session.
- Select an option that specifies **input ON** to allow the shadower to input keyboard and mouse actions to the shadowed session.
- Select an option that specifies **notify ON** to display a message on the client that asks permission to shadow the session.

This option is supported for Citrix ICA-based clients only.

User Profile Path

Used to enter a network path when enabling a roaming or mandatory user profile for a selected user.

The path you enter follows the form: *servername**profilesfoldername**username*. For example, **\\puma\profiles\jeffho**.

When assigning a mandatory user profile, open System in Control Panel to the **User Profiles** tab and copy a preconfigured user profile to the user profile path location. Then, rename the NTUser.dat file in the user profile to NTUser.man.

If you specify both a user profile path and a Terminal Server profile path, the user profile path is used for Windows NT logons and the Terminal Server profile path is used for Terminal Server logons. If you specify only a user profile path, that path is used for both Windows NT and Terminal Server logons.

The Terminal Server profile path is used for Terminal Server logons only.

User Profile Path

Used optionally to enter a network path when enabling a mandatory user profile for all selected user accounts.

The path you enter follows the form: *servername**profilesfoldername**userprofilename*. For example, **\\puma\profiles\clerks**. Then, you must open System in Control Panel, and on the **User Profiles** tab, copy a preconfigured user profile to the user profile path location. Then, rename the NTUser.dat file in the user profile to NTUser.man. Do not create individual folders for the users in the user profile path location.

Do not assign the same preconfigured roaming user profile by selecting multiple accounts unless it is a mandatory user profile. To assign the same preconfigured user profile to multiple user accounts, you must enter a separate user profile path for each user account and use System in Control Panel to copy the preconfigured user profile to the server location for each user.

If you specify both a user profile path and a Terminal Server profile path, the user profile path is used for Windows NT logons and the Terminal Server profile path is used for Terminal Server logons. If you specify only a user profile path, that path is used for both Windows NT and Terminal Server logons.

The Terminal Server profile path is used for Terminal Server logons only.

Terminal Server Profile Path

Used to enter a network path for Terminal Server logons. This is used only when enabling a roaming or mandatory user profile for a selected user.

The path you enter follows the form: *servername**profilesfoldername**username*. For example, **\\puma\profiles\jeffho**.

When assigning a mandatory user profile, open System in Control Panel, and on the **User Profiles** tab, copy a preconfigured user profile to the user profile path location. Then, rename the NTUser.dat file in the user profile to NTUser.man.

If you specify both a user profile path and a Terminal Server profile path, the user profile path is used for Windows NT logons and the Terminal Server profile path is used for Terminal Server logons. If you specify only a user profile path, that path is used for both Windows NT and Terminal Server logons.

The Terminal Server profile path is used for Terminal Server logons only.

Terminal Server Profile Path

Used optionally to enter a network path when enabling a mandatory user profile for all selected user accounts.

The path you enter follows the form: *servername**profilesfoldername**userprofilename*. For example, **\\puma\profiles\clerks**. Then, you must open System in Control Panel and on the **User Profiles** tab, copy a preconfigured user profile to the user profile path location. Then, rename the NTUser.dat file in the user profile as NTUser.man. Do not create individual folders for the users in the user profile path location.

Do not assign the same preconfigured roaming user profile by selecting multiple accounts unless it is a mandatory user profile. To assign the same preconfigured user profile to multiple user accounts, you must enter a separate user profile path for each user account, and use System in Control Panel to copy the preconfigured user profile to the server location for each user.

If you specify both a user profile path and a Terminal Server profile path, the user profile path is used for Windows NT logons and the Terminal Server profile path is used for Terminal Server logons. If you specify only a user profile path, that path is used for both Windows NT and Terminal Server logons.

The Terminal Server profile path is used for Terminal Server logons only.

Logon Script Name

Used to assign a logon script to selected users. If the logon script is located in a subdirectory of the logon script path, that relative path precedes the file name.

When a logon script is assigned to a user account, it runs each time the user logs on. It can be a batch file (.cmd or .bat file name extension) or an executable program (.exe file name extension). One logon script can be assigned to one or more user accounts. When a user logs on, the server authenticating the logon locates the logon script by following the logon script path (usually \WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS).

For example, you might type **clerks.cmd**; or, you might type **admins\ernesta.bat**.

Note


Computers running Microsoft Network Client for MS-DOS (version 3.0), Windows for Workgroups, Windows NT version 3.1, and LAN Manager 2.x must use the .bat file name extension.

Logon Script

For Microsoft LAN Manager, a logon script is a batch program containing LAN Manager and operating system commands used to configure workstations. A logon script can be assigned to one or more users. When the user logs on, the logon script runs on the client computer.

When assigning a logon script, use the .bat extension for the file name you type.

Logon Script Name

Used to assign a logon script to a selected user. If the logon script is located in a subdirectory, the relative path must precede the file name in **Logon Script Name.**

For example, you might type **clerks.cmd**; or, you might type **admins\ernesta.bat**.

When a logon script is assigned to a user account, it runs each time the user logs on. It can be a batch file (.cmd or .bat file name extension) or an executable program (.exe file name extension). One logon script can be assigned to one or more user accounts. When a user logs on, the workstation locates the logon script by following the workstation's logon script path (usually \WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS).

Note

The client computer executes the logon script file. For client computers running Microsoft Network Client for MS-DOS (version 3.0), Windows for Workgroups, Windows NT version 3.1, and LAN Manager 2.x, the logon script name must use the .bat file name extension.

Home Directory for Windows NT and Terminal Server

An assigned home directory becomes a user's default directory for the **File Open** and **Save As** dialog boxes, for command prompt, and for all applications that do not have a defined working directory. Home directories make it easier for an administrator to back up user files and delete user accounts by collecting many or all of the files in one location.

Each user on Terminal Server should have a unique home directory on the server. This ensures that application information is stored separately for each user in the multiuser environment.

The home directory can be a local directory on a user’s computer or a shared network directory and can be assigned to a single user or many users.

If the home directory is to have a server location, you must first create the share and then add the path for the share (including the home directory name) to the user’s account.

Usually, User Manager for Domains automatically creates the home directory if you set a path for it. If not, a message appears, instructing you to manually create the directory. If you do not assign a home directory to a user account, the system uses the default local home directory (\USERS\DEFAULT on the user's local drive where Windows NT Workstation version 4.0 or Windows NT Server version 4.0 is installed as an upgrade, or the root directory where Windows NT version 4.0 is installed as the initial version).

Notes

- If you specify only the home directory for Windows NT, that home directory is used for both Windows NT and Terminal Server logons.
- If you specify only the Terminal Server home directory, the default home directory is used for Windows NT logons, and the specified home directory is used for Terminal Server logons.

Home Directory

Specifies the location of a user’s home directory. You use **Local Path** to enter the path to the user’s local computer.

A home directory is a directory that is accessible to a user (has appropriate permissions applied) and contains files and programs for that user. For Microsoft LAN Manager, this can be a directory on the user’s local hard disk, or a shared directory on a server.

Local Path

One of the options for specifying a home directory at the workstation where the user logs on.

For example, you might type **c:\users\johnbr**.

Connect To

One of the options for specifying a shared network directory as the home directory and having the user’s computer connect to that share at logon.

For example, you might specify drive J in **Connect**, and then type **\\airedale\users\johnbr**.

User Environment Profile

Used to add a user profile path, logon script name, or home directory path to all the selected user accounts.

For more information about this dialog box, click the following:

- Users
- User Profile Path
- Terminal Server Profile Path
- Logon Script Name
- Home Directory
- Terminal Server Home Directory
- Local Path
- Connect To
- Using %USERNAME% in the Home Directory Path

See Also

Managing the User Environment

User Environment Profile

Used to add a logon script name or home directory path to this user account. These additions are optional.

For more information about this dialog box, click the following:

- User
- Logon Script
- Home Directory

User Environment Profile

Used to add a logon script name or home directory path to all the selected user accounts. These additions are optional.

For more information about this dialog box, click the following:

- Users
- Logon Script
- Home Directory

Logon Hours

Used to restrict the days and hours during which a user can connect to a server. The default is to allow a user to connect during all hours of all days of the week, but you can restrict a user’s server access to certain days and hours. This does not affect a user's ability to use a workstation.

For more information about this dialog box, click the following:

- About the Calendar
- Allow
- Disallow

See Also

Managing Logon Hours

About the Calendar

Displays a one-week calendar, with logon hours indicated in one-hour increments across seven days. One box represents each hour.

The first box in each row represents the hour from midnight through 12:59 A.M.; the last box in each row represents the hour from 11:00 P.M. through 11:59 P.M.

When a hour in a box is selected, the user is allowed to connect to servers during that hour. When an hour in a box is clear, the user cannot connect to servers during that hour.

Allow

Allows a user to connect to a server during certain hours.

Selected boxes specify the hours during which connections are allowed.

Disallow

Denies a user connections to a server during certain hours.

Cleared boxes indicate that connections are not allowed during those hours.

When a user is connected to a server and logon hours are exceeded, the user is either disconnected from all server connections or is allowed to remain connected but is denied any new connections. This depends on the setting for **Forcibly disconnect remote users from server when logon hours expire** in the **Account Policy** dialog box.

Logon Workstations

Specifies the workstations from which a user can log on to this domain account. The default is to allow a user to log on from any workstation, but you can allow a user to log on from only specified workstations.

For more information about this dialog box, click the following:

- User
- User May Log On To All Workstations
- User May Log On To These Workstations
- Boxes 1 through 8

Note

- If you have additional services installed, there might be additional options. For information about those options, see the documentation for those services.

See Also

Managing Logon Workstations

User May Log On To All Workstations

Allows the user to log on from all workstations.

Users May Log On To All Workstations

Allows the selected users to log on from all workstations.

User May Log On To These Workstations

Allows the user to log on only from the computers entered in boxes 1 through 8.

Users May Log On To These Workstations

Allows the selected users to log on only from the computers entered in boxes 1 through 8.

Boxes 1 through 8

Specify the only workstations from which the user can log on when **User May Log On To These Workstations** is selected.

Boxes 1 through 8

Specify the only workstations from which the user can log on when **User May Log On To These Workstations** is selected.

Logon Workstations

Restricts the workstations from which users can log on to selected domain accounts. The default is to allow users to log on from any workstation, but you can restrict users to logging on from only specified workstations.

For more information about this dialog box, click the following:

- Users
- Users May Log On To All Workstations
- Users May Log On To These Workstations
- Boxes 1 through 8

Note

- If you have additional services installed, you may have additional options. For information about those options, see the documentation for those services.

Managing Logon Workstations

Account Information

Specifies an account expiration date (if any) and the account type for this user account.

For more information about this dialog box, click the following:

- User
- Account Expires
- Never
- End Of
- Account Type
- Global Account
- Local Account

See Also

Managing Account Information

Account Expires

When an account has an expiration date, the account is disabled at the end of the specified day. When an account is disabled, a user who is logged on remains logged on but cannot establish new network connections. After logging off, that user cannot log on again.

Never

Specifies that the account will not expire.

End Of

If you click **End Of**, you must specify an expiration date. The account becomes disabled at the end of the specified day.

Account Type

User accounts are either global or local accounts. Most accounts are global accounts.

A global account is a normal user account in the user's home domain. A local account is an account provided in this domain for a user whose global account is not in a trusted domain.

Global Account 

A global account is a normal user account in the user's home domain. Most accounts are global accounts, which is the default setting. If multiple domains are available, it is best if each user in the network has only one global account in only one domain so that the user has only one password.

In the User Manager window, global accounts are represented by the global account icon.

Local Account 

A local account is an account provided in this domain for a user whose regular account is not in a trusted domain. This might be a Windows NT Server domain, a LAN Manager domain, or another type of domain or network that is not trusted by this domain.

Local accounts can be used to access computers running Windows NT Workstation or Windows NT Server over the network, and can be granted resource permissions and user rights. However, local accounts cannot be used to log on interactively. Local accounts created in one domain cannot be used in trusting domains, and do not appear in the **Add Users and Groups** dialog boxes of trusting domains.

It is best for a local account to use the same password both here and in its home domain.

Administrator

The user who can perform all actions on the server.

Always assign a password to a user account that is granted Administrator-level permissions.

User

A user who can employ network resources (subject to the access permissions for the resources), view information about shared resources, view printer and communication-device queue status, and send and receive messages. The user account is a member of the special Users group to which permissions can be assigned. This is the default permission level and is granted to most network users.

An account granted the User permission level can be assigned one or more of the user-operator permissions.

Guest

A user who has the same permissions as one who is granted User permissions, but who is a member of the special Guest group instead of the Users group. Use Guest permissions to exclude temporary or occasional user accounts from the Users group.

Account Operator

A user who can create, remove, and modify user accounts that have User or Guest permissions; create, remove and modify groups; modify logon restrictions; and add workstations to the domain.

The account operator cannot modify an account that has Administrator permissions, except to change group memberships. The user cannot change an account's permission to the Administrator level.

Print Operator

A user can share and stop sharing printer queues; create, remove, and modify printer queues; control print jobs; and view a list of all resources shared on the server, including resources available only to Administrators.

Server Operator

A user who can start and stop services; share and stop sharing resources; read and clear the error log; close user sessions and the files users have opened; and view a list of all the resources shared on the server, including resources available only to Administrators.

Comm Operator

A user who can share and stop sharing communication-device queues; control communication-device-queue requests; and view a list of all resources shared on the server, including resources available only to Administrators.

Account Information

Specifies an account expiration date (if any), and the permission level for the user account.

For more information about this dialog box, click the following:

- User
- Account Expires
- Never
- End Of
- Administrator
- User
- Guest
- Account Operator
- Print Operator
- Server Operator
- Comm Operator

See Also

Managing Account Information

Account Information

Specifies an account expiration date (if any) and the account type for all the selected user accounts.

For more information about this dialog box, click the following:

- Users
- Account Expires
- Never
- End Of
- Account Type
- Global Account
- Local Account

See Also

Managing Account Information

Account Information

Specifies an account expiration date (if any), and the permission level for all the selected user accounts.

For more information about this dialog box, click the following:

- Users
- Account Expires
- Never
- End Of
- Administrator
- User
- Guest
- Account Operator
- Print Operator
- Server Operator
- Comm Operator

Rename User

Used to change the user name assigned to an existing user account. A user name cannot be identical to any other user or group name of the domain or computer being administered. **Change To** is used to enter a new user name of up to 20 characters. These can be any uppercase or lowercase characters, except for the following:

" / \ [ ] : ; | = , + * ? < >

A user name cannot consist solely of periods (.) and spaces.

See Also

Renaming User Accounts

Delete Multiple Users

Used to delete user accounts.

User accounts that have been created using User Manager for Domains can be deleted, but the built-in Administrator and Guest accounts cannot.

For more information about this dialog box, click the following:

- Delete User
- Yes
- Yes to All
- No

See Also

Disabling User Accounts

Deleting User Accounts

Delete User

The name of the account that will be deleted if you click **Yes**. Only one user name is shown, even though two or more were selected in the User Manager for Domains window.

Yes

Used to delete the user account named in **Delete User**.

Yes To All

Used to delete all the user accounts that were selected in the User Manager for Domains window.

No

Skips the deletion of the user account named in **Delete User**.

When **No** is clicked, the next user account selected for deletion appears in **Delete User**

Select Users

Used to select and deselect the user-account membership of groups.

Only user accounts from the domain or computer being administered (those listed in the User Manager for Domains window) can be selected or deselected. For example, if you are administering a domain and you click **Select** for a selected local group, member user accounts from trusted domains are not affected.

Once accounts are selected, you can apply commands on the **User** menu to them.

For more information about this dialog box, click the following:

- Group
- Select
- Deselect

See Also

Selecting User Accounts

Group

Lists the groups for the domain or computer being administered.

Select

Used to select all members of a selected group in **Group**.

Only user accounts from the domain or computer being administered (those user accounts listed in the User Manager for Domains window) can be selected. For example, if you are administering a domain and you click **Select** for a selected local group, member user accounts from trusted domains are not affected.

Deselect

Used to deselect all user accounts that are members of the selected group in **Group**.

Only user accounts from the domain or computer being administered (those user accounts listed in the User Manager for Domains window) can be deselected. For example, if you are administering a domain and you click **Deselect** for a selected local group, member user accounts from trusted domains are not affected.

Global Group

Used to create or copy a global group.

When you want to modify a global group, use the **Global Group Properties** dialog box.

For more information about the **Global Group** dialog box, click the following:

- Group Name
- Description
- Members
- Not Members
- Add
- Remove

See Also

Creating a New Global Group

Copying a Global Group

Managing Global Group Properties

Group Name

Used to enter a name for a new or existing global group.

The group name identifies the global group. A global group name cannot be identical to any other group or user name of the domain or computer being administered. It can contain up to 20 uppercase or lowercase characters, except for the following:

" / \ [ ] : ; | = , + * ? < >

A global group name cannot consist solely of periods (.) and spaces.

When modifying a global group, the name cannot be changed.

Description

Used to enter or change the group description.

Members

Lists the members of the global group. User accounts from this domain can be members.

When you click **New Global Group** on the **User** menu, any user accounts currently selected in the User Manager for Domains window become members of the new global group and appear in **Members**.

When you copy a global group, the list in **Members** is copied from that global group.

When you modify an existing global group, **Members** shows the current members of the group.

Not Members

Lists the user accounts of this domain that are not members of the global group.

Add

Adds the user accounts selected in **Not Members** to the group membership.

Remove

Removes the user accounts selected in **Members** from the group membership.

Global Group

Used to create or copy a global group.

To modify a global group, use the **Global Group Properties** dialog box.

For more information about the **Global Group** dialog box, click the following:

- Group Name
- Description
- Members
- Not Members
- Add
- Remove

See Also

Creating a New Global Group

Copying a Global Group

Managing Global Group Properties

Local Group

Used to modify a local group.

For more information about this dialog box, click the following:

- Group Name
- Description
- Show Full Names
- Members
- Add
- Remove

See Also

Creating a New Local Group

Copying a Local Group

Managing Local Group Properties

Group Name

Used to enter a name to identify the local group. A local group name cannot be identical to any other group or user name of the domain or computer being administered. It can contain up to 256 uppercase or lowercase characters, except for the backslash character (\).

When modifying a local group, the group name cannot be changed.

Description

Used to enter or change the group description.

Show Full Names

Used to display the full names for users in **Members**. Otherwise, the user accounts are identified only by the user names.

This can be a lengthy operation when the local group contains numerous users from other domains.

Members

Lists the members of the local group. User accounts and global groups from either this domain and from trusted domains can be members.

When you click **New Local Group** on the **User** menu, any user accounts currently selected in the User Manager for Domains window become members of the new local group and appear in **Members**.

When you copy a local group, the list in **Members** is copied from that local group.

When you modify an existing local group, **Members** shows the current members of the group.

Add

Opens the **Add Users And Groups** dialog box, which you can use to add new members to the local group. You can add user accounts and global groups from this domain and trusted domains.

Remove

Removes the members selected in **Members** from this local group.

Local Group

Used to modify a local group.

For more information about this dialog box, click the following:

- Group Name
- Description
- Show Full Names
- Members
- Add
- Remove

See Also

Creating a New Local Group

Copying a Local Group

Managing Local Group Properties

Members

Lists the members of the local group. User accounts from this workstation can be members. If this workstation participates in a domain, user accounts and global groups from the local domain and trusted domains can also be members.

When you click **New Local Group** on the **User** menu, any user accounts currently selected in the User Manager for Domains window become members of the new local group and appear in **Members**.

When you copy a local group, the list in **Members** is copied from that local group.

When you modify an existing local group, **Members** shows the current members of the group.

Add

Opens the **Add Users And Groups** dialog box, which you can use to add members to this local group.

User accounts from this workstation can be added to the group. If this workstation participates in a domain, user accounts and global groups from the local domain and trusted domains can also be added.

Account Policy

Used to control how passwords must be used by all user accounts, and whether user accounts are automatically locked out after a series of failed logon attempts.

For more information about this dialog box, click the following:

- Domain
- Maximum Password Age
- Minimum Password Age
- Minimum Password Length
- Password Uniqueness
- No Account Lockout
- Account Lockout
- Forcibly disconnect remote users from server when logon hours expire
- Users must log on in order to change password

See Also

Managing the Account Policy

Domain

The name of the domain being administered.

Computer

The name of the computer being administered.

Maximum Password Age

The period of time a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can select **Password Never Expires**.

Minimum Password Age

The period of time a password must be used before the user can change it. You can set values between 1 and 999 days, or you can select **Allow Changes Immediately**.

Do not allow immediate changes if you enter a value for **Remember _ Passwords** under **Password Uniqueness**.

Minimum Password Length

The fewest characters a password can contain. The value must be between 1 and 14 characters, or it can be zero if you select **Permit Blank Password**.

Password Uniqueness

The number of new passwords that must be used by a user account before an old password can be reused. The value must be between 1 and 24 passwords, unless you select **Do Not Keep Password History**.

For uniqueness to be effective, immediate changes should not be allowed under **Minimum Password Age**.

No Account Lockout

When selected, never locks out user accounts, no matter how many failed logon attempts are made.

Account Lockout

When selected, subjects all user accounts to lockout. If too many failed logon attempts are made on a user account within a specified amount of time, the account is locked out. A locked account cannot log on.

If you select **Account Lockout**, you should also do the following:

- In **Lockout After**, specify the number of failed logon attempts that will cause the account to be locked. The range is 1 to 999.
- In **Reset Count After**, specify the maximum number of minutes that can occur between any two failed logon attempts for lockout to occur. The range is 1 to 99999.
- In **Lockout Duration**, select one of the following:
- Click **Forever** to cause locked accounts to remain locked until an administrator unlocks them.
- Click **Duration**, and then type a number of minutes for locked accounts to remain locked before automatically becoming unlocked. The range is 1 to 99999.

Note

- Failed password attempts against workstations or member servers that have been locked using either Ctrl+Alt+Delete, or password protected screen savers do not count against account lockout settings entered in User Manager for Domains.

Forcibly Disconnect Remote Users From Server When Logon Hours Expire

When selected, disconnects a user account from any servers on the domain when it exceeds its logon hours.

When cleared, does not allow the user account to make new connections after exceeding its logon hours, but does not disconnect it.

This option interacts with the Logon Hours defined for a user account.

Users Must Log On In Order to Change Password

When selected, requires users to log on before changing their password. If a user's password expires, the user will not be able to change the expired password, but must have an administrator change the password.

When cleared, allows users to change their expired passwords without notifying an administrator.

Account Policy

Used to control how passwords must be used by all user accounts of the workstation or member server.

For more information about this dialog box, click the following:

- Computer
- Maximum Password Age
- Minimum Password Age
- Minimum Password Length
- Password Uniqueness
- No Account Lockout
- Account Lockout
- Forcibly disconnect remote users from server when logon hours expire
- Users must log on in order to change password

See Also

Managing the Account Policy

Account Policy

Used to control how passwords must be used by all user accounts.

For more information about this dialog box, click the following:

- Domain
- Maximum Password Age
- Minimum Password Age
- Minimum Password Length
- Password Uniqueness
- Forcibly disconnect remote users from server when logon hours expire
- Users must log on in order to change password

See Also

Managing the Account Policy

Account Policy

Used to control how passwords must be used by all user accounts of the workstation.

For more information about this dialog box, click the following:

- Computer
- Maximum Password Age
- Minimum Password Age
- Minimum Password Length
- Password Uniqueness
- Forcibly disconnect remote users from server when logon hours expire
- Users must log on in order to change password

See Also

Managing the Account Policy

Account Policy

Used to control how passwords must be used by all user accounts.

For more information about this dialog box, click the following:

- Domain
- Maximum Password Age
- Minimum Password Age
- Minimum Password Length
- Password Uniqueness
- Forcibly disconnect remote users from server when logon hours expire
- Users must log on in order to change password

See Also

Managing the Account Policy

User Rights Policy

The User Rights policy manages the rights granted to groups and user accounts.

A right authorizes a user logged on to an account to perform certain actions on the system. When a user does not have appropriate rights, attempts to carry out those actions are blocked. Rights apply to the system as a whole and are different from permissions, which apply to specific objects.

Members of a group have all the rights granted to that group. In most situations, the easiest way to provide rights to a user is to add that user's account to one of the built-in groups that already possesses the needed rights, rather than by administering the User Rights policy.

For information about this dialog box, click the following:

- Domain
- Right
- Grant To
- Show Advanced User Rights
- Add
- Remove

See Also

The User Rights

Managing the User Rights Policy

Right

Contains a list of the available rights, and displays the selected right. Select rights in **Rights** when you want to manage them.

The list of groups and user accounts granted that right can then be viewed, and names can be added to or removed from the list.

Grant To

Lists the groups and user accounts that are assigned the selected right.

Show Advanced User Rights

When selected, shows certain rights in addition to the default rights.

Most advanced rights are useful only to programmers writing applications for computers running Windows NT Workstation or Windows NT Server.

Add

Click to open the **Add Users And Groups** dialog box, which you can use to grant the selected right to additional groups or user accounts.

Groups and user accounts from this domain and from trusted domains can be granted rights.

Add

Click to open the **Add Users And Groups** dialog box, which you can use to grant the selected right to additional groups or user accounts.

Local groups and user accounts from this workstation can be granted rights. If this workstation participates in a domain, user accounts and global groups from the local domain and trusted domains can also be granted rights.

Remove

Click to remove the group or user account selected in **Grant To** for a selected right.

User Rights Policy

The User Rights policy manages the rights granted to groups and user accounts.

A right authorizes a user logged on to an account to perform certain actions on the system. When a user does not have appropriate rights, attempts to carry out those actions are blocked. Rights apply to the system as a whole and are different from permissions, which apply to specific objects.

Members of a group have all the rights granted to that group. In most situations, the easiest way to provide rights to a user is to add that user's account to one of the built-in groups that already possesses the needed rights, rather than by administering the User Rights policy.

For information about this dialog box, click the following:

- Computer
- Right
- Grant To
- Show Advanced User Rights
- Add
- Remove

See Also

The User Rights

Managing the User Rights Policy

Audit Policy

Selected activities of users can be tracked by auditing security events and then placing entries in a computer's security log. Use the Audit policy to determine the types of security events that will be logged.

When administering domains, the Audit policy affects the security logs of the domain controller and of all servers in the domain, because they share the same Audit policy.

When administering a computer running Windows NT Workstation or a Windows NT Server that is not a domain controller (a member server), this policy affects only the security log of that computer.

Because the security log is limited in size, click events to be logged carefully. The maximum size of each computer's security log is defined in Event Viewer. Entries in a security log can be reviewed using Event Viewer.

For more information, click the following:

- Domain
- Do Not Audit
- Audit These Events
- Success
- Failure
- Logon and Logoff
- File and Object Access
- Use of User Rights
- User and Group Management
- Security Policy Changes
- Restart, Shutdown, and System
- Process Tracking

See Also

Managing the Audit Policy

Do Not Audit

No events will be recorded in the security log.

Do Not Audit

No events will be recorded in the security log.

Audit These Events

The selected events will be logged.

Success

When selected, adds an entry to the security log when the event occurs successfully.

Failure

When selected, adds an entry to the security log when an attempted occurrence of the event fails.

Logon and Logoff

A user logged on, logged off, or made a network connection.

File and Object Access

A user accessed a directory or a file that is set for directory or file auditing, or a user sent a print job to a printer that is set for printer auditing.

Use of User Rights

A user exercised a user right (except those rights related to logon and logoff.)

User and Group Management

A user account or group was created, changed, or deleted; a user account was renamed, disabled, or enabled; or a password was set or changed.

Security Policy Changes

A change was made to the User Rights, Audit, or Trust Relationships policies.

Restart, Shutdown, and System

A user restarted or shut down the computer; or an event has occurred that affects either the system security or the security log.

Process Tracking

These events provide detailed tracking information for such events as program activation, some forms of handle duplication, indirect object accesses, and process exit.

Audit Policy

Selected activities of users can be tracked by auditing security events and then placing entries in the computer's security log. Use the Audit policy to determine the types of security events that are logged.

Because the security log is limited in size, carefully select events to be logged. The maximum size of the computer's security log is defined in Event Viewer.

Entries in a security log can be reviewed using Event Viewer.

For more information, click the following:

- Computer
- Do Not Audit
- Audit These Events
- Success
- Failure
- Logon and Logoff
- File and Object Access
- Use of User Rights
- User and Group Management
- Security Policy Changes
- Restart, Shutdown, and System
- Process Tracking

See Also

Managing the Audit Policy

Audit Policy

Selected activities of users can be tracked, by auditing security events and then placing entries in a computer's security log. Use the Audit policy to determine the types of security events that will be logged.

For more information, click the following:

- Domain
- Do Not Audit
- Audit These Events
- Success
- Failure
- Logon and Logoff
- File and Object Access
- Use of User Rights
- User and Group Management
- Security Policy Changes
- Restart, Shutdown, and System
- Process Tracking

See Also

Managing the Audit Policy

Trust Relationships

Use the **Trust Relationships** dialog box to add and remove domain names from the list of trusted domains and the list of trusting domains.

Establishing a trust relationship requires two steps performed in two different domains:

- First, the domain that will be the trusted domain adds a domain to its list of trusting domains.
- Then, the trusting domain must add the first domain to the list of trusted domains.

Establishing a two-way trust relationship (where each domain trusts the other) requires that both steps be performed twice, once in each domain.

Removing a trust relationship also requires two steps, one in each domain:

- The trusted domain must remove the second domain from its list of trusting domains.
- The trusting domain must remove the first domain from its list of trusted domains.

Note

- Trust relationships can be established only between Windows NT Server domains.

For more information about this dialog box, click the following:

- Domain
- Trusted Domains
- Trusting Domains
- Adds
- Removes

See Also

Adding a Trusting Domain

Adding a Trusted Domain

Trust relationship

A trust relationship is a link between two Windows NT Server domains.

Trust relationships specify trusting (resource) domains and trusted (account) domains.

- A trusting domain allows the users of another domain (the trusted domain) access to its resources.
- Trusted-domain users and groups can hold user rights, resource permissions, and local group memberships in the trusting domains.

Trust relationships allow users to access resources on the entire network through a single user account and a single password. This moves the convenience of centralized administration from the domain level to the network level.

Note

- Trust relationships can be established only between Windows NT Server domains.

Trusted Domains

Lists the domains that this domain trusts to use its resources.

Only Windows NT Server domains can be trusted domains.

Trusting Domain

Lists the domains that trust this domain to use its resources.

Only Windows NT Server domains can be trusting domains.

Add

Opens a dialog box that you can use to add a new trusted or trusting domain, depending on which **Add** button you click.

Establishing a trust relationship requires two steps, each step performed in a different domain: First, one domain (the trusted domain) must add a second domain to the list of domains that trust it, and then the second domain (the trusting domain) must add the first domain to the list of domains that it trusts.

Remove

Removing a trust relationship between domains requires two steps, one in each of the two domains:

- The trusted domain must remove the trusting domain from its list of trusting domains.
- The trusting domain must remove the trusted domain from its list of trusted domains.

The order of performing these steps is not important.

Never remove a trust relationship by performing just one of the steps; always administer both domains.

Add Trusted Domain

Used to add a Windows NT Server domain to this domain's list of trusted (account) domains.

Domain

Type the name of the trusted domain (the domain whose accounts will be trusted to use resources in this domain).

You can type a name using both uppercase and lowercase characters, but the name is always displayed in uppercase.

Password

Type the password required by the trusting domain.

Passwords are case sensitive; use the same password that was entered in the **Add Trusting Domain** dialog box for that domain.

Note

Once a trust relationship is established, the system changes this password. You cannot remove one side of an established trust relationship and use the original password later to reestablish that trust. You must always remove both sides of a trust relationship, and then completely reestablish it.

See Also

Adding a Trusting Domain

Adding a Trusted Domain

Add Trusting Domain

Used to add a Windows NT Server domain to the list of trusting (resource) domains.

Trusting Domain

Type the name of the trusting domain (the domain that will trust accounts in this domain to use its resources).

You can type a name using both uppercase and lowercase characters, but the name is always displayed in uppercase.

Initial Password and Confirm Password

Type the same password in both places.

Passwords are case sensitive.

Note

Once a trust relationship is established, the system changes this password. You cannot remove one side of an established trust relationship and use the original password later to reestablish that trust. You must always remove both sides of a trust relationship, and then completely reestablish it.

See Also

Adding a Trusting Domain

Adding a Trusted Domain

Select Domain

When User Manager for Domains starts, it displays the domain where your user account is defined. Use **Select Domain** to display a different domain.

You can display an individual computer, but only a computer that maintains its own security database, such as a computer running Windows NT Workstation, a computer running Windows NT Server that is not a domain controller (a member server), or a Microsoft LAN Manager server. If you specify a primary or backup domain controller, the domain is displayed instead.

For more information, click the following:

- Domain
- Select Domain
- Low Speed Connection

See Also

Selecting a Domain

Using Low Speed Connection

Domain

Used to display a domain. You can type the domain name in **Domain**, and then click **OK**.

If you want to display only one computer, you can type *computername* (precede computer names with two backslashes,) and then click **OK**.

Names can use both uppercase and lowercase characters, but the name is always displayed in uppercase.

Select Domain

Displays a selected domain when you click **OK**.

Low Speed Connection

When administering a domain or computer that communicates with your computer across a connection providing relatively low transmission rates, some functions in User Manager for Domains might perform slowly. You can reduce delays by using **Low Speed Connection**. **Low Speed Connection** prevents the lists of users and groups from being displayed but still allows you to administer users and local groups (but not global groups).

For example, from a domain controller you might administer a remote computer that is running the Microsoft Windows NT Remote Access Service (RAS) and is connected to the network by a modem over telephone lines. When entering the computer name in the **Select Domain** dialog box, select the **Low Speed Connection**.

You can also select or clear **Low Speed Connection** on the **Options** menu.

Add Users and Groups

Used to grant the selected right to groups and user accounts. Groups and user accounts from the local domain and trusted domains can be granted rights.

For more information about this dialog box, click the following:

- List Names From
- Names
- Add
- Show Users
- Members
- Search
- Add Names

List Names From

Contains a list of domain and computer names, and displays the selected name. When an asterisk (*) appears next to a domain or computer name, this indicates that the local groups of that domain or computer can be listed in **Names**. When the asterisk is absent, it indicates that local groups cannot be listed.

Names

Lists the groups of the domain or computer selected in **List Names From**. If **Show Users** is selected, **Names** also lists the user accounts.

Names

Lists the user accounts of the domain or computer selected in **List Names From**. If a domain is selected, global groups are also listed.

Add

Used to enter the names selected in **Names** to **Add Names**.

Show Users

Displays the user accounts in **Names**.

By default, only groups are listed.

Members

Displays the members of the group selected in **Names**.

Search

Opens the **Find Account** dialog box, which you can use to look for a particular group or user account.

Add Names

You can add groups and user accounts in a number of ways.

- You can type the account names (separated by semicolons) in **Add Names**.
- You can select the account names in **Names** and click **Add**.
- You can click **Search** and complete the **Find Account** dialog box.
- You can select a group in **Names**, click **Members**, and then complete the **Group Membership** dialog box.
- To grant the selected right to the names in **Add Names**, click **OK**.

Add Names

You can add groups and user accounts in a number of ways.

- You can type the account names (separated by semicolons) in **Add Names**.
- You can select the account names in **Names** and click **Add**.
- You can click **Search** and complete the **Find Account** dialog box.
- You can select a group in **Names**, click **Members**, and then complete the **Group Membership** dialog box.
- To grant the selected right to the names in **Add Names**, click **OK**.

Add Users and Groups

Used to add members to the local group.

For more information about this dialog box, click the following:

- List Names From
- Names
- Add
- Members
- Search
- Add Names

Local Group Membership

Lists the user accounts and global groups that are members of the selected local group.

For more information about this dialog box, click the following:

- Members of Local Group
- Add
- Members

Members Of Local Group

Lists the members of the selected local group.

Add

Adds the user accounts or global groups selected in **Members Of** in the **Local Group Membership** dialog box to **Add Names** in the **Add Users And Groups** dialog box.

Members

Displays the members of the selected global group (that is itself a member of this local group) in **Members Of**.

Global Group Membership

Lists the user accounts that are members of the selected global group.

Members of Global Group

Lists the members of the selected global group.

Add

Adds the user accounts or global groups selected in **Members Of** in the **Local Group Membership** dialog box to **Add Names** in the **Add Users And Groups** dialog box.

Find Account

Used to locate a user account or group.

For more information about this dialog box, click the following:

- Find User or Group
- Search All
- Search Only In
- Search
- Search Results
- Add

Find User or Group

Used to enter the name you want to search for.

The system will search for user accounts or groups of that exact name.

Search All

When selected, sets searches to look for a matching user or group name in both the local domain or computer and in all domains trusted by the local domain.

Search Only In

When selected, sets searches to look for a matching user or group name in only the selected domains and computers.

Search

Begins a search based on the parameters specified in **Find User Or Group** and by **Search All** or **Search Only In**.

Search Results

Displays the user accounts and groups found by a search. This list is continuously filled as a search progresses.

One or more names can be selected from **Search Results** and added to **Add Names** in the **Add Users and Groups** dialog box by clicking **Add** in the **Find Account** dialog box.

The list presents the matching users in the form *domainname**username* (full name) description, or *computername**username* (full name) description.

The list presents the matching groups in the form *domainname**groupname* description, or *computername**groupname* description.

Add

Closes the **Find Account** dialog box and adds the accounts selected in **Search Results** to **Add Names** in the **Add Users and Groups** dialog box.

Enter Server

The domain could not be found. It may not exist; you may have misspelled the domain name; or the domain may be located across a network bridge.

Note

- Broadcast messages such as the one generated by **Add Trusted Domain** are not usually passed across wide area network (WAN) bridges.

If you misspelled the domain name, do the following:

- Click **Cancel**, and then type the correct domain name in the **Add Trusted Domain** dialog box.

If the domain is located across a network bridge, do the following:

- In **Server**, type the computer name of any server running Windows NT Server in that domain, and then click **OK**.

Copy User or Group

Used to select a user account or local group for copying. (In **Low Network Connection** mode, global groups cannot be copied.)

Enter user name or local group name

Used to select a user account or group for copying by typing a user name or local group name here, and then clicking **OK**.

See Also

Using Low Speed Connection

Delete User or Group

Used to select a user account, local group, or global group for deletion.

Enter user name or group name

- To select one user account, one global group, or one local group for deletion, type its name here, and then click **OK**.
- To select multiple user accounts for deletion, type the user names here, separated by semicolons, and then click **OK**.

See Also

Using Low Speed Connection

Manage User or Group Properties

Used to select a user account or local group for administration. (In **Low Speed Connection** mode, global groups cannot be administered.)

Enter user name or local group name

- To select one user account or one local group for administration, type its name here, and then click **OK**.
- To select multiple user accounts for administration, type the user names here, separated by semicolons, and then click **OK**.

See Also

Using Low Speed Connection

Rename User

Used to select a user account for renaming. (Groups cannot be renamed.)

Enter user name

- To select a user account for renaming, type the user name here, and then click **OK**.

See Also

Using Low Speed Connection

Dialin Information

Used to grant users permission to use Dial-Up Networking for connecting to the network. When administering a domain or a group of servers, you can set domain-wide permissions. When administering a workstation or member server, you can set permission for only that computer.

Grant dialin permission to a user

When selected, grants the permission to the selected user. You can revoke the selected user's permission by clearing the check box.

Call Back

Used to set up callback for a user account.

- To disable callback for a user account, click **No Call Back** (the default setting).
- To have the server to prompt the user for a number, click **Set By Caller**.

  The server calls the user back at the number entered by the user, and thus incurs the telephone charges for the session.
- To have the server call the user at a fixed telephone number, click **Preset To**, and then type the fixed phone number.

  The server will call the user back at only this number, which reduces the risk of an unauthorized use of the account.

Note

- Do not assign callback permission to users who are connecting to the network through a switchboard.
- **Preset To** interferes with the ability to make multilink calls if the user's equipment requires more than one phone number for the group of multilinked lines.

See Also

Managing Dialin Permissions