8.8.8 User Account Management Facts

One of an administrator's most important jobs is to create and manage user accounts. Windows Server offers powerful tools for managing users.

When creating users:

- Each user name must be unique.
- It is good policy to use complex passwords and require the user to change their password at the next login.
- The password Never Expires feature saves time when the user is using applications that require a user account login.
- You can also add users from the command line using the **net** or **dsadd** commands.

Keep in mind the following recommendations when managing user accounts:

- To modify properties on multiple user accounts at the same time, use the **Shift** or **Ctrl** keys to select all users, and then edit the necessary properties. Properties such as the login name or password cannot be modified in this way.
- You can move user accounts to add them to the appropriate organizational units (OUs). Grouping users within OUs allows you to apply Group Policy settings to groups of users.
- When creating a new user account or resetting a forgotten password, a common practice is to reset the user account password, then select **User must change password at next logon**. This forces the user to reset the password immediately following login, ensuring that the user is the only person who knows the password.
- Enable the **User cannot change password** option when you want to maintain control over a guest, service, or temporary account. For example, many applications use service accounts for performing system tasks. The application must be configured with the user account name and password. If you allow changing the user account password for the service account, you would also need to change the password within every application that uses that account.
- To reset the user account password, right-click the user object and select **Reset Password**.
- An account that has been locked out because too many incorrect passwords have been entered must be unlocked. To unlock an account, select the **Account** tab in the account object's **Properties** dialog box and select **Unlock Account**. The **Reset Password** dialog also gives you the option to unlock a user account.
- You can configure an expiration date for temporary user accounts. After the account is expired, it cannot be used for login.
- If a user will be gone for an extended period of time, disable the account. This prevents the account from being used during the user's absence. Enable the account when the user returns.
- Configure the login hours for a user account to allow the account to only be used between specific hours.
  - Login attempts outside of the specified hours will not be allowed.
  - Users who are currently logged in will be allowed to continue working when the login hours expire.
  - To log a user off when the login hours pass, configure Group Policy settings to log the user off automatically.
- You can configure a list of workstations that a user is allowed to log on to. When configured, login to other workstations is not allowed.
- The user profile tracks user environment settings, such as program-specific settings, user security settings, and desktop settings (including the files, folders, and shortcuts on the desktop).
  - By default, the profile is stored on the local computer. A profile will be created on each computer when a user logs in.
  - To make profile settings consistent across computers, use a roaming user profile (where the profile is saved on a network share). When the user logs in, profile settings are copied from the network to the local computer. Changes made on the local computer are saved back to the network share.
  - To use a roaming profile, edit the user account properties and specify the profile path. To simplify administration, use the **%username%** variable in the Profile path. Active Directory replaces **%username%** with the user login name.
- If you accidentally delete a user account, restore it from backup rather than create a new one with the same name. Creating a new account with the same name results in a user account with a different SID and will not automatically assume the permissions and memberships of the previously deleted account.
- *Deprovisioning* is the process of removing access rights for users when they leave your organization.
  - If the user will be replaced by another user, disable the existing account.
  - If the user will not be replaced, you can delete the account. Be sure to reassign any permissions to other users, reassign ownership over files, or delete unnecessary files, such as the user profile. After a user account has been deleted, all permissions and memberships that are associated with that user account are permanently deleted. All permissions and memberships must be recreated manually if you want to duplicate a deleted user account.
  - Many third party tools exist that can simplify the deprovisioning process. For example, you can delete the user account and automatically reassign permissions or file ownership with a single step. You can also create your own deprovisioning solution through a programming language to synchronize accounts between databases or applications.
- To create another user account similar to an existing user, copy the existing user account. You will be prompted for a new name and password. Existing account settings and group memberships will be copied to the new account. Permissions will not be copied to the new account.
- If you regularly create user accounts with the same settings, you should create a template account. The template account is a normal user account with the settings you need for subsequent accounts.
  - Copy the account whenever you need to create a new one.
  - New accounts retain group memberships, but not direct permission assignments.
  - Disable this account to prevent it from being used for login.

Every directory object has attributes that are populated with values.

User Properties	Description

General	The General tab allows you to modify the following information: ▪ First name ▪ Last name ▪ Display name ▪ Description ▪ Office ▪ Telephone number ▪ Email ▪ Web page
Address	The Address tab allows you to modify the user's home address.

Account	The Account tab allows you to modify the following:
	▪ Login name
	▪ Login hours
	▪ Computers that users log in to
	▪ Unlock account
	▪ A date on which the account expires. The account isn't deleted, just locked.
	▪ Account options can be controlled on an individual basis or on a group policy management console.
	  ▪ Storing password using reversible encryption prevents anyone from using a password cracking tool.
	  ▪ Disable the account if the user is not currently working for the company.
	  ▪ Specify security mechanisms such as a smart card. Smart cards and digital certificates are some of the strongest security mechanisms you can use.
	  ▪ Specify that a sensitive account in an organizational unit cannot be delegated.
	  ▪ Set the encryption type. Kerberos AES encryption is the default encryption type.
	  ▪ Specify that the account doesn't need Kerberos preauthentication if the account is a service account or you are working with a web-based application.

Profile	The Profile tab allows you to modify the following:
	▪ The location where information such as network drive mappings, desktop settings, and screen savers are stored.
	  ▪ By default, this is contained in a local profile.
	  ▪ A roaming profile is configured by setting the profile location to a shared folder.
	▪ A login script
	and network drives.
	  ▪ Group policy preferences replace login scripts for mapping drives and connecting to remote printers.
	▪ A home folder for the user.

Member Of	The Member Of tab allows you to modify the organizational groups (OGs) to which the user will be a member. All users are members of the Domain Users group.
Dial-in	The Dial-in tab allows you to modify the dial-in or VPN access for a user.
Environment	The Environment tab allows you to modify the following: ▪ A program to start at login. ▪ The client devices to connect to at login.
Sessions	The Sessions tab allows you to modify the following: ▪ The period of time before disconnecting remote desktop or terminal services session. ▪ The time limit for an active remote desktop or terminal services session. ▪ The time limit for an idle remote desktop or terminal services session. ▪ The actions that will be taken when a remote desktop or terminal services connection is broken. ▪ The ability to reconnect a remote desktop or terminal services session from a different client.
Remote Control	The Remote Control tab allows you to: ▪ Enable remote control. ▪ Determine whether the user's permission is required. ▪ Specify the level of control the administrator will have.

Users with the same access needs are easier to manage as a group. On a Windows server, navigate to where in the tree you want to create the group, right-click, and select **New** and **Group**. There are two types of groups, security groups and distribution groups. Security groups are security principles and have security identifiers (SIDs). The key difference between security groups and distribution groups is that you can't apply security to distribution groups. For example, you cannot apply permissions to a distribution group. When creating groups, you specify the following:

- Whether to nest one or more groups within a group.
- Group scope:
  - Domain local groups have access within the domain only. To change a group to a domain local group from a global group, select **Universal** and apply the change. The domain local group will then be available.
  - Global is the default. Global groups are good for organizing users.
  - Universal groups can access all domains and have an unlimited number of users, groups, and computers from multiple domains within the forest. Universal groups increase global catalog traffic.

You can also select multiple users, right-click, and select **Add to a group**.

TestOut Corporation All rights reserved.