6.2.3 Configure and Manage AD DS Passwords Facts

This lesson covers the following topics:

- Account lockout and password policies
- Granular password policies
- Azure username and password policies
- Azure self-service password reset
- Organizational password strategies
- Organizational password policies

Password policies define characteristics of passwords that are enforced by the system, such as the minimum number of characters or how often the passwords must be changed.

Account Lockout and Password Policies

Account lockout and password policies control passwords and user lockout properties for the entire domain.

- Password Policy settings control characteristics enforced for user passwords.
- Account Lockout Policy settings control what happens when a user enters one (or more) incorrect passwords.
- Policy settings apply to the computer, not the user.
- Although you can configure Account Policies settings in any GPO, only the settings configured in a GPO linked to the domain take effect.

The following table describes the password and account lockout policy settings:

Password Policy Setting	Description
Enforce password history	Enforce password history requires users to create unique passwords. Set this to a high number to keep users from frequently repeating passwords. Windows can remember up to 24 old passwords.
Maximum password age	Maximum password age requires the user to change the password after a given time. Setting this value to 0 means that the password never expires. A maximum password age must be configured for this setting to take effect.
Minimum password age	Minimum password age keeps users from changing passwords immediately after resetting their passwords. Doing so prevents users from defying the password history by initiating multiple password changes in a sequence to get back to their preferred password. The value must be less than the maximum age and should be a setting greater than 0. A setting of 0 allows the user to reset the password immediately.

Password Policy Setting	Description
Minimum password length	Minimum password length prevents users from using passwords that are too short. At a minimum, enforce passwords of eight characters or longer.
Complexity requirements	Password must meet complexity requirements prevents passwords that are easy to guess or crack. This setting: • Requires users to create a password with a minimum of three of the four types of special characters (lowercase letters, uppercase letters, numbers, or !, @, #, $, %, ^, &, *). • Prevents the use of dictionary words or any part of the user's login identification. • Requires that passwords be six characters long (or longer).
Store passwords using reversible encryption	Store passwords using reversible encryption is equivalent to storing plaintext passwords. This setting should be disabled unless a specific application requires access to the plaintext password.
Account lockout duration	Account lockout duration determines the duration the account will be disabled (in minutes). When the time expires, the account will be unlocked automatically. When set to a value of 0, an administrator must unlock the account.
Account lockout threshold	Account lockout threshold determines the number of attempts a user can make before the account is locked. A typical setting is 3.
Reset account lockout counter after	Reset account lockout counter after determines the amount of time (in minutes) that must pass before the number of invalid attempts counter resets.

Granular Password Policies

Granular password policies allow you to create password policies for users and global groups separate from the password policy applied to the entire domain. For example, you could require an eight-character password for regular users and use granular password policies to require administrators to use 14-character passwords. Generally, it would be best to use account policies to enforce a domain-wide password policy. Then you would use granular password policies for groups of users with more restrictive password policy needs than the domain-wide password policy.

You should know the following facts about granular password policies:

- The domain must be running at the Windows Server 2008 domain functional level or higher.
- Password policies affect only user account passwords, not computer account passwords.
- Only members of the Domain Admins group can set granular password policies, but you can delegate the permission.
- Granular password policies are saved as a Password Settings Object (PSO) in the Password Settings Container (PSC).
    - There is one default PSC. It cannot be renamed, deleted, or moved.
    - You can create additional PSCs, but they will not take effect.
    - The PSC holds one or more PSOs. You can define multiple PSOs with unique password policy settings.
- PSOs have attributes for all the settings defined in the Default Domain Policy except Kerberos settings.
- Policies can be applied to user accounts or global security groups.
    - You can apply each granular policy to multiple users and/or groups.
    - Granular password policies affect only users within the current domain.
- When applied to OUs, the domain policies (or other group types) are excluded.

When you move a user account to a different OU, remember to also change the group membership so that the granular password policy no longer applies.

Azure Username and Password Policies

Users have a User Principal Name (UPN) and password associated with their account. The following policies apply to these usernames and passwords:

Type	Description
Username	The User Principal Name must follow the following length constraints: • Up to 64 characters can be entered before the “@” symbol. • Up to 48 characters can be entered after the “@” symbol. • Up to 113 characters can be entered in total. The following character types are allowed in a UPN: • a-z • A-Z • 0-9 • .’_-#!~^ The following character types are not allowed in a UPN: • An “@” symbol cannot immediately precede the “.” character. • The “@” sign can only be used when separating the username and domain.
Character types	The following character types are allowed in an Azure AD password: • a-z

Type	Description
	• A-Z • Blank space • 0-9 • @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < > The following password restrictions apply to Azure AD: • Unicode characters cannot be used. • Passwords must use at least three of the following: symbols, numbers, uppercase letters, and lowercase letters. • A minimum of eight characters is required. • A maximum of 256 characters can be used. • Azure AD provides a global banned password list based on ongoing security analysis. An administrator cannot edit the default list but can add up to 100 banned words for a custom banned password list.
Default policies	The following default policies apply to Azure AD passwords: • The maximum password age (password expiration policy) is 90 days. • Users are notified of this expiration 14 days before the password expires. • The user cannot use the last password again when changing or resetting their password.

Azure Self-Service Password Reset

If a user forgets their password or gets locked out of their account, Azure AD provides the convenient option of a user self-service password reset. This reduces the time and effort needed to contact the help desk or administrator for a password reset.

Note the following about the self-service password reset (SSPR):

- SSPR can be enabled for none, all, or selected users.
- If the user needs additional help with their reset, they can click on the **contact your administrator** link. Administrators can customize this button with their help desk email or URL.
- By default, regular users are required to use one authentication method, and admin accounts are required to use two authentication methods for password resets. You can enable additional authentication methods as needed.
- Before a user can unlock or reset, they need to register their contact information with Azure AD. This information is used for authentication.

Best practices for the self-service password reset include:

- If you are using SSPR for the first time, start with a small group of users before expanding to the full organization. Doing so helps you to work through potential user concerns. It also gives you time to familiarize yourself and your users with the registration process and workflow.

- User contact information should be kept up to date. This ensures that the user can unlock their account when needed.
- When testing the self-service password reset, you should use a non-administrator account.

Organizational Password Strategies

Use the following strategies to protect against password attacks:

- Educate users on how to create and remember strong passwords. Enforcing strict password restrictions might weaken network security if you do not educate users about taking proper procedures to protect login credentials. If users do not understand the restrictions that have been implemented, users might try to circumvent these restrictions by writing down passwords. Take the following measures to educate users:
    - Tell users that they should not write down passwords or share login credentials with other users.
    - Teach users how to construct and remember complex passwords. For example, for the password bw2Fs3d , users might create the following sentence: bob went 2 the capital Florist shop 3 times daily .
    - Educate users about social engineering tactics. Instruct them not to respond to requests for passwords from administrators or other seemingly trusted personnel. Implement policies that prevent administrators from asking for sensitive information.
- Implement two-factor authentication.

Organizational Password Policies

Password policies detail the requirements for an organization's passwords. These policies can include the following:

- The same password should never be used for different systems.
- Accounts should be disabled or locked out after a specified amount of failed login attempts.
- Passwords should never contain words, slang, or acronyms.
- Users should be required to change their passwords within a certain time frame and use a rotation policy.
- A strong password policy should be enforced. Strong passwords:
    - Contain multiple character types, uppercase letters, lowercase letters, numbers, and symbols.
    - Have a minimum length of eight characters or more.
    - Use no part of a username or email address.