13.7.10 Authentication Management Facts

Authentication is the process of submitting and checking credentials to validate or prove user identity. On a computer system, authentication typically occurs during logon where the user provides a username and password or some other form of credential (such as a smart card or a biometric scan). The system verifies the credentials, allowing access if the credentials are valid.

Be aware of the following when troubleshooting user authentication on Windows systems.

- For a workgroup, the username must match a user account configured on the local system. However, if the computer is a member of a domain, the username must match a user account configured in the domain database on the domain controller.
- Usernames are not case sensitive.
- Passwords are case sensitive. Having the Caps Lock on (or the Fn key or the Num Lock on a laptop) could result in incorrect characters in the password.
- Password Policy settings in the Local Security Policy control characteristics about a password such as how long it must be, how often it must be changed, or whether complex passwords are required.
- Account Lockout Policy settings in the Local Security Policy control what happens when users enter incorrect passwords. With account lockout, an account is locked (and cannot be used for logon) when a specified number of incorrect passwords are entered.
  - Depending on the policy settings, locked accounts might be unlocked automatically after a period of time.
  - You can unlock a locked account by editing the account properties in Local Users and Groups.
  - If an account is locked because the user forgot the password, an administrator can change the password using Local Users and Groups. As a best practice, when changing the password for a user, the password the administrator configures should be a temporary password. In the user account properties, select **User must change password at next logon** to require the user to change the password after logging on with the temporary password.
- A disabled account cannot be used for logon.
  - You will typically disable an account that is no longer needed or that will not be used for a long period of time.
  - You can manually disable and enable an account; however, you cannot manually lock an account (you can only unlock a locked account). Accounts are locked automatically through the account lockout settings.
  - By default, the Guest account is disabled. On later versions of Windows, the built-in Administrator account is also disabled during installation. Both of these accounts are usually left disabled.
- To access a shared folder, shared printer, or Remote Desktop within a workgroup environment, you must supply credentials that match a valid user account configured on the remote computer you are trying to access. The user account you specify must have a password configured. User accounts with blank passwords cannot be used to access a computer over the network.
- By default, members of the Administrators group are allowed Remote Desktop access. To allow non-administrators access, add them to the list of authorized users for Remote Desktop. This automatically makes them members of the Remote Desktop Users group.

To increase authentication security, consider implementing multiple authentication factors. Three commonly used types of authentication factors are listed in the following table:

Type	Description

Type 1
Something you know
	Something you know authentication requires you to provide a password or some other data that you know. This is the weakest type of authentication. Examples of something you know include:
	- Passwords, codes, or IDs
	- PINs
	- Passphrases (long, sentence-length passwords)
	- *Cognitive* information such as questions that only the user can answer, including:
	  - Your mother's maiden name
	  - The model or color of your first car
	  - The city where you were born
	
	Usernames are not a form of Type 1 authentication. Usernames are often easy to discover or guess. Only the passwords or other information associated with the usernames can be used to validate identity.

Type 2 Something you have	Something you have (also called token-based authentication) is authentication based on something a user has in their possession. Examples of something you have authentication controls are:

	▪ *Swipe cards* (similar to credit cards) with authentication information stored on the magnetic strip.
	▪ *Smart cards* with a memory chip containing encrypted authentication information. Smart cards can:
	  ▪ Require contact such as swiping, or they can be contactless.
	  ▪ Contain microprocessor chips with the ability to add, delete, and manipulate data on it.
	  ▪ Can store digital signatures, cryptography keys, and identification codes.
	  ▪ Use a private key for authentication to log a user into a network. The private key will be used to digitally sign messages.
	  ▪ Be based on challenge-response. A user is given a code (the challenge) which he or she enters into the smart card. The smart card then displays a new code (the response) that the user can present to log in.

Type 3
Something you are
	Something you are authentication uses a biometric system. A biometric system attempts to identify a person based on *metrics* or a mathematical representation of the subject's biological attribute. This is generally considered to be the most secure form of authentication.
	
	Common attributes used for biometric systems are:
	
	▪ Fingerprints (end point and bifurcation pattern)
	▪ Hand topology (side view) or geometry (top down view)
	▪ Palm scans (pattern, including fingerprints)
	▪ Retina scans (blood vein pattern)
	▪ Iris scans (color)
	▪ Facial scans (pattern)
	▪ Voice recognition
	▪ Handwriting dynamics
	▪ Keyboard or keystroke dynamics (behavioral biometric systems)
	  ▪ Dwell time (key press time)
	  ▪ Flight time (how fingers move from key to key)
	
	When implementing a biometric system, the attribute that is used for authentication must meet the following criteria:
	
	▪ *Universality* means that all individuals possess the attribute.
	▪ *Uniqueness* means that the attribute is different for each individual.
	▪ *Permanence* means that the attribute always exists and will not change over time.
	▪ *Collectability* ensures that the attribute can be measured easily.
	▪ *Performance* means that the attribute can be accurately and quickly collected.
	▪ *Circumvention* allows for acceptable substitutes for the attribute in case the original attribute is missing or can't be read.
	▪ *Acceptability* identifies the degree to which the technology is accepted by users and management.

True multifactor authentication requires the user to provide an authentication factor from more than one category. For example, requiring users to provide a username and password is not true multifactor authentication because both the user and the password are something the user knows. To strengthen authentication, you could require the user to provide a fingerprint (something the user is) and a password (something the user knows).
