Microsoft Security, Compliance, and Identity Fundamentals

Exam Ref SC-900

Yuri Diogenes
Nicholas DiCola
Kevin McKinnerney
Mark Morowczynski

Microsoft

Exam Ref SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Yuri Diogenes
Nicholas DiCola
Kevin McKinnerney
Mark Morowczynski

- **Security Questions** These are only available to Azure AD self-service password reset and can only be used with accounts that have not been assigned administrative roles. Questions are stored on the user object in Azure AD and cannot be read or modified by an administrator. They should be used in conjunction with another method. A user must answer three, four, or five questions to pass this gate. This is configurable by the administrator. Azure AD includes the following predefined questions, and it is possible to create custom questions:
  - In what city did you meet your first spouse/partner?
  - In what city did your parents meet?
  - In what city does your nearest sibling live?
  - In what city was your father born?
  - In what city was your first job?
  - In what city was your mother born?
  - What city were you in on New Year's 2000?
  - What is the last name of your favorite teacher in high school?
  - What is the name of a college you applied to but didn't attend?
  - What is the name of the place in which you held your first wedding reception?
  - What is your father's middle name?
  - What is your favorite food?
  - What is your maternal grandmother's first and last name?
  - What is your mother's middle name?
  - What is your oldest sibling's birthday month and year? (for example, November 1985)
  - What is your oldest sibling's middle name?
  - What is your paternal grandfather's first and last name?
  - What is your youngest sibling's middle name?
  - What school did you attend for sixth grade?
  - What was the first and last name of your childhood best friend?
  - What was the first and last name of your first significant other?
  - What was the last name of your favorite grade-school teacher?
  - What was the make and model of your first car or motorcycle?
  - What was the name of the first school you attended?
  - What was the name of the hospital in which you were born?
  - What was the name of the street of your first childhood home?
  - What was the name of your childhood hero?
  - What was the name of your favorite stuffed animal?
  - What was the name of your first pet?

- What was your childhood nickname?
- What was your favorite sport in high school?
- What was your first job?
- What were the last four digits of your childhood telephone number?
- When you were young, what did you want to be when you grew up?
- Who is the most famous person you have ever met?

MORE INFO **AUTHENTICATION METHODS**

You can learn more about authentication methods at *https://aka.ms/SC900_AADAuthMethods*.

Azure AD Self-service password reset can also reset the password of hybrid users in Active Directory. Azure AD Connect is required with password writeback enabled, as shown in Figure 2-15. In this scenario, the password reset is first written to an on-premises Active Directory. If it's successful, the user receives the message that their password has been successfully changed. If password hash sync is enabled, the new password is synced to Azure Active Directory through Azure AD Connect. No other directory type supports writeback.

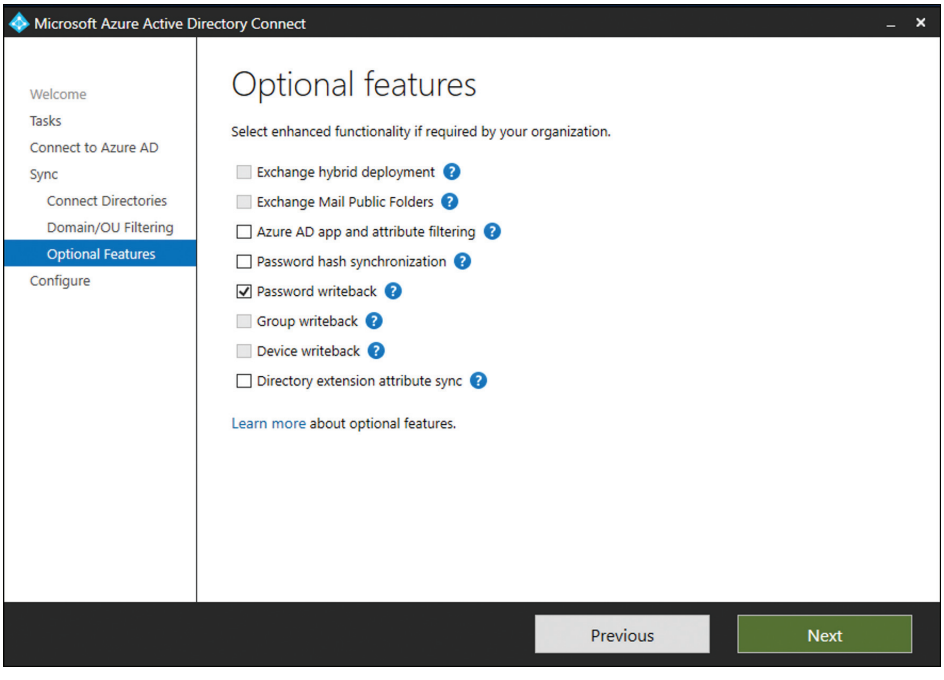

FIGURE 2-15 Azure AD SSPR Password writeback enabled

MORE INFO **SELF-SERVICE WRITEBACK**

You can learn more about how SSPR writeback works at *https://aka.ms/SC900_SSPRWriteback*.

Azure AD self-service password reset also is integrated with the Windows 10 lock screen, as shown in Figure 2-16. For the user to log in to the workstation after resetting their password through Azure AD SSPR, they would need network connectivity to a domain controller, either through the corporate network or the VPN. This does not update the local cached credentials on the workstation.

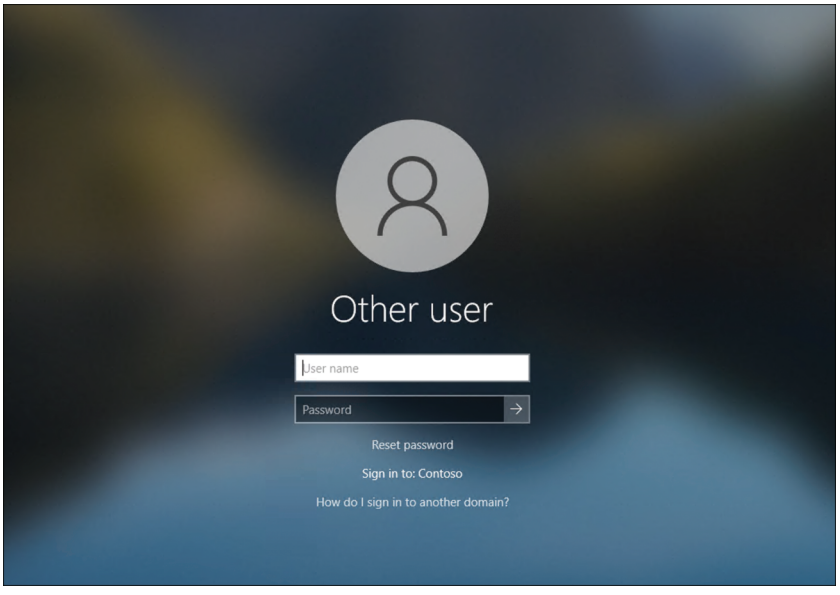

FIGURE 2-16 Azure AD SSPR enabled at the Windows lock screen

MORE INFO **SELF-SERVICE PASSWORD RESET LOCK SCREEN DEPLOYMENT**

You can learn more about deploying Azure AD SSPR at the Windows lock screen at *https://aka.ms/SC900_SSPRLockScreen*.

Describe multifactor authentication

As described earlier, multifactor authentication requires a user to authenticate with two or more different factor types. These factor types are something you know (typically a password), something you have (typically a phone or other physical device), or something you are (biometrics). Having a user enter two different passwords would not count as multifactor authentication because passwords use the same type of factor—in this case, knowledge. Azure MFA includes several different authentication options.

- **Phone** The user will get a phone call and must press a specific key, such as #, or they will get an SMS text message containing a code that they will need to enter into the log in screen.

- **Mobile app notification** The Microsoft Authenticator application receives a push notification from Azure MFA. The user sees the notification in which they must verify their authentication. The user approves it if the user performed the authentication or denies it otherwise.
- **Mobile app code/Software Tokens** The Microsoft Authenticator app supports the Open Authentication (OATH) time-based, one-time password (TOTP) standard. The code rotates every 30 or 60 seconds. Other software tokens that support OATH-TOTP can also be used, as well as any other software authenticator apps that support OATH-TOTP.
- **Hardware Tokens** OATH-TOTP SHA-1 tokens that refresh every 30 or 60 seconds can also be used.

As you'll notice, there is some overlap between the methods available for SSPR and Azure MFA. Depending on the factors you've set up, users can register for both SSPR and MFA at the same time they are registering for either SSPR or MFA if you have enabled combined security information registration (see Figure 2-17).

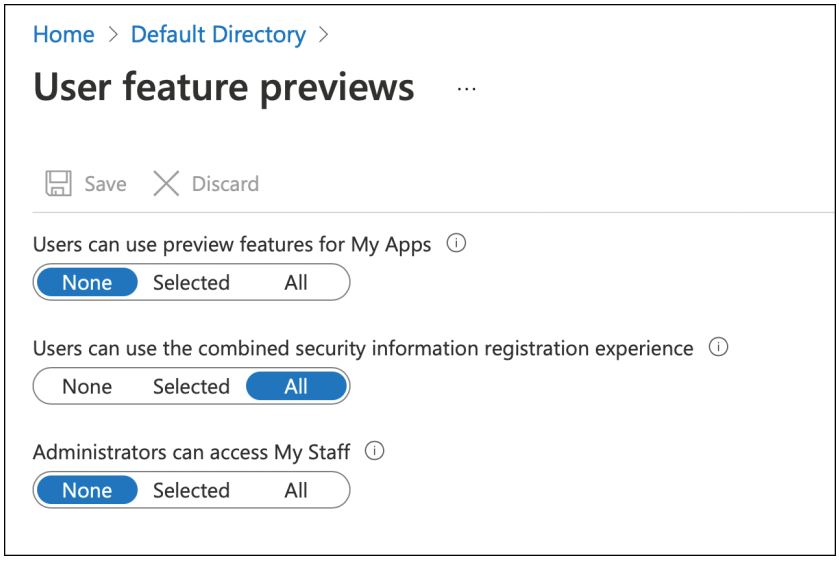

FIGURE 2-17 Azure AD combined security information registration experience

MORE INFO **COMBINED SECURITY INFORMATION**

You can learn more about deploying the combined security information at *https://aka.ms/SC900_CombinedRegistration*.

To require users to perform Azure MFA when accessing a resource, make sure to configure the option in conditional access. (This will be covered in Skill 2-3.) Applications that leverage modern protocols such as WS-Fed, SAML, OAuth, and OpenID Connect and that are integrated

with Azure Active Directory can require MFA before they can be accessed. Also, applications connected to Azure Active Directory through Azure AD Application Proxy can leverage Azure MFA because the user is performing Azure MFA against Azure Active Directory before accessing the application. This means the application doesn't need to make any changes to take advantage of Azure MFA or any other conditional access controls.

Finally, be mindful of over-prompting users. This can lead to MFA fatigue where they mistakenly accept an MFA prompt that was generated by an attacker, which defeats the purpose of MFA altogether. Another method is to leverage a passwordless technology like Windows Hello For business or FIDO2 at sign-in to the workstation. This would satisfy any future MFA prompts because strong authentication is being performed at sign-in. MFA is really the bare minimum that can be done today, but the direction you should be moving to is passwordless authentication. It's the strongest form of authentication and provides the best user experience. It's truly a win-win.

EXAM TIP

Make sure you understand what makes up MFA and the methods that can be used for MFA authentication (phone, text, Authenticator app, and a hardware token).

Describe Windows Hello for Business and passwordless credentials

Passwordless credentials are the latest form of strong authentication providing the best balance between user experience and security. They authenticate the user by combining MFA methods— something you have (the device), something you know (in this case, a PIN tied to the device), or something you are (biometrics). Biometrics include fingerprint or facial recognition.

NOTE **PIN VERSUS PASSWORD**

The important thing to understand that separates a PIN from a password is that a PIN can only be used on that device where it's registered. A password could be used anywhere. This is a huge security improvement because knowing the PIN is only valuable to the attacker if they have that specific device.

Also, because the user is performing MFA on sign-in to the device, their authentication token will reflect that they've already completed MFA. That means future MFA challenges are automatically satisfied when this token is used, which will drastically cut down on the MFA prompts the user would normally see without compromising the security. This makes for a great user experience and prevents over-prompting for MFA. There are three types of passwordless credentials in Azure Active Directory: Windows Hello for Business, Microsoft Authenticator app, and FIDO2.

Windows Hello for Business is a great passwordless solution for when a user uses the same device every day. Think of your traditional information worker who is assigned a workstation that only they use. To use Windows Hello for Business, a user must complete Windows Hello for Business registration, as shown in Figure 2-18, by performing strong authentication. During this registration process, the user would create their PIN and optionally enroll in biometrics, such as fingerprint or facial recognition if the device hardware supports it and is configured to do so by the administrator. A public/private key is also generated with the private key being stored in the Trust Platform Module (TPM) chip. The user logs in by either entering their PIN or using a biometric method. This act unlocks the TPM chip to access the private key. Windows then uses the private key to authenticate the user with Azure AD.

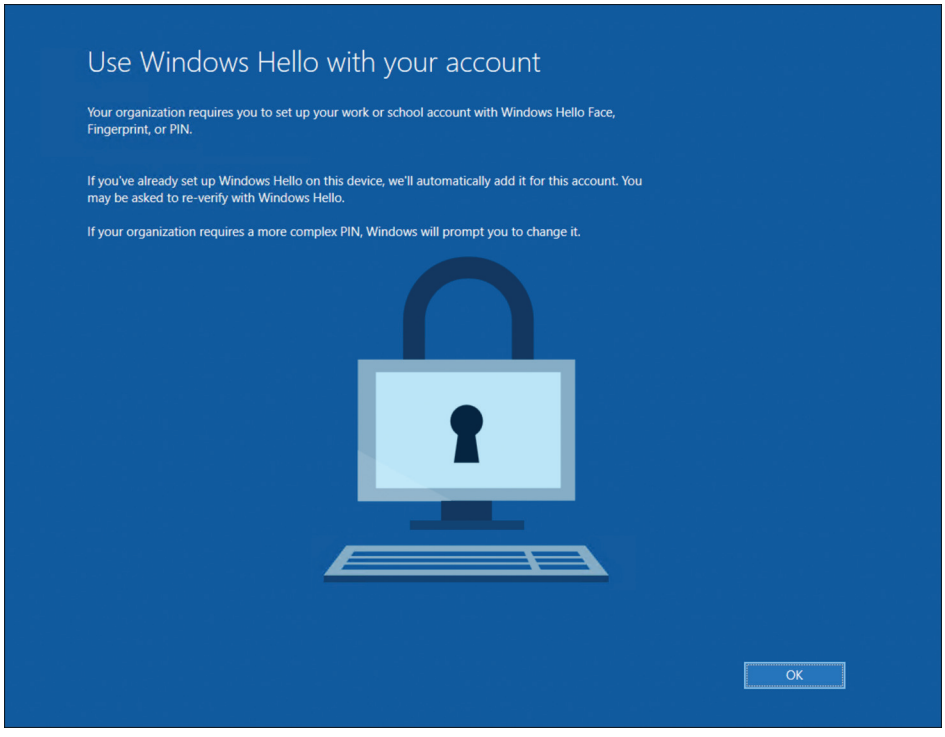

FIGURE 2-18 Windows Hello for Business registration screen

There are two important things to understand about this process.

- First, the PIN and biometrics (if used) never leave the device. They aren't stored in Azure AD and do not roam to any other devices. They are completely local to the device where registration took place.
- Second, the PIN and biometrics are not used to authenticate the user to Azure AD. This is a common misconception. The private key is used to do the authentication. The PIN and biometrics are used to unlock the TPM to access the private key. The private key (protected by the TPM) is used to authenticate the user to Azure AD, NOT the PIN or biometric.