ANSWER KEY: IMPLEMENT AND MANAGE IDENTITY AND ACCESS IN AZURE AD

When preparing for directory synchronization, you should clean up your Active Directory by removing duplicate proxyAddress and userPrincipalName attributes.

Before deploying directory synchronization, you need to make sure your on-premises user objects have a UPN suffix configured, and that its value is correct for both the Active Directory domain and Microsoft 365.

The Microsoft 365 IdFix tool can help you identify and fix most object synchronization errors in Active Directory forests.

When setting up Azure AD Connect, Express Setup is the default option, which works for most organizations with a single forest.

When setting up Azure AD Connect, Custom Setup is designed for organizations with more advanced configurations.

Azure AD Connect Health is part of Azure AD Premium.

When forcing a manual synchronization in Azure AD Connect, using PowerShell, the *Start-ADSyncSyncCycle -PolicyType Delta* command starts a delta synchronization.

Windows Hello for Business replaces passwords with strong two-factor authentication that's tied to a device and uses either biometrics or a PIN.

As an administrator, you can create policies to manage Windows Hello for Business use on devices that connect to your organization. Biometric sign-in options include facial recognition, fingerprint recognition, and iris recognition.

Microsoft Authenticator is a mobile app that adds extra security to your accounts with two-factor authentication, protecting you from unauthorized access and phishing attacks.

To use self-service password reset, users must first register their desired authentication methods.

Users can register for SSPR by browsing to https://aka.ms/ssprsetup, or by clicking on the "Register for password reset" link under the Profile tab in the Access Panel.

Users can register a mobile app when registering for SSPR at https://aka.ms/mfasetup, or in the combined security info registration at https://aka.ms/setupsecurityinfo.

You can enable or disable password writeback through the Azure portal. When enabled, federated, pass-through authentication, or password hash synchronized users are allowed to reset their passwords.

The global banned password list is created by the Azure AD Identity Protection team, which constantly analyzes Azure AD security telemetry data to identify weak or compromised passwords.

The custom banned password list allows you to add your own disallowed terms to this list of terms banned by the global banned list.

Organizations can enable MFA in three primary ways: Conditional Access, Security Defaults, and the Microsoft 365 admin center.

Conditional Access policies enhance security by enabling MFA based on specific conditions.

To access a sign-in log, you can navigate to the Azure Active Directory menu and open the sign-in log within the Monitoring section.

When reviewing a failed sign-in in the sign-in logs, you can get more information about the reason for the failure in the Basic info section of the related log item.

Azure AD Identity Protection helps organizations secure their users' identities by automating the detection and remediation of identity-based risks, investigating these risks using data in the portal, and exporting risk detection data to other tools for further analysis.

Identity Protection detects various risks, including anonymous IP address use, atypical travel, malware-linked IP addresses, unfamiliar sign-in properties, leaked credentials, password spray attacks, and more.

Identity Protection detects risks, reports them, and allows administrators to investigate and remediate them, keeping organizations safe. Risks can also be fed into tools like Conditional Access or a SIEM tool for further investigation.

Microsoft recommends enabling email notifications to respond promptly when users are flagged as at risk. To do this, you can set up weekly digest emails to get an overview of risk events that have occurred.

Azure AD Conditional Access works with Microsoft Intune compliance policies to control the devices and apps that can access your company resources.

You can implement device-based and app-based Conditional Access policies.