Microsoft

Microsoft Endpoint Administrator

Exam Ref MD-102

Andrew Bettany
Andrew Warren

Microsoft

Exam Ref MD-102 Microsoft Endpoint Administrator

Andrew Bettany
Andrew Warren

CHAPTER 2

Manage identity and compliance

Two of the most important elements of your IT infrastructure are identity and device compliance. Identity provides knowledge of who somebody or something is, while compliance enables you to determine the overall health of a device. By implementing these two technologies, you can improve your organization's overall security and help protect your organizational data. Compliance policies, especially when implemented with conditional access, are an important part of the MD-102 exam.

Skills covered in this chapter:

- Skill 2.1: Manage identity
- Skill 2.2: Implement compliance policies for all supported device platforms by using Intune

Skill 2.1: Manage identity

Identity services provide authentication and authorization to help protect your organizational resources and data. Over the years, Microsoft has implemented several such identity services: Active Directory Domain Services (AD DS), Azure Active Directory (Azure AD), and Azure AD Domain Services. The MD-102 exam primarily covers content that relates to Azure AD.

This skill covers how to:

- Implement user authentication on Windows devices, including Windows Hello for Business, passwordless, and tokens
- Manage role-based access control (RBAC) for Intune
- Register devices in and join devices to Azure AD
- Implement the Intune Connector for Active Directory
- Manage the membership of local groups on Windows devices
- Implement and manage Local Administrative Passwords Solution (LAPS) for Azure AD

Overview of identity solutions

Before we get into the specific content covered in the exam, it's perhaps worth reviewing these identity providers. There are two identity providers you must be familiar with in the Endpoint Administrator role:

- **AD DS** Windows Server role used to support identity in on-premises environments
- **Azure AD** Cloud-based identity solution used to provide single sign-on (SSO) for cloud apps such as Microsoft 365 and Azure

A third identity provider, Azure AD Domain Services, is a managed Azure service that provides an identity solution that closely resembles the behavior of AD DS but runs in the cloud without needing Windows server computers configured as domain controllers. This identity solution is out of this course's scope.

NEED MORE REVIEW? **IMPLEMENT HYBRID IDENTITY WITH WINDOWS SERVER**

For more information about Azure AD Domain Services, refer to the Microsoft Learn website at *https://learn.microsoft.com/training/modules/implement-hybrid-identity-windows-server.*

Active Directory Domain Services

Detailed knowledge of Windows Server and AD DS is outside the scope of the MD-102 exam. However, it's probably worth at least discussing the fundamentals of AD DS to help put Azure AD into context.

AD DS, commonly referred to as either Windows Active Directory or just Active Directory, is a role of associated services installed on Windows Servers. Windows Server installed with the AD DS role is a complex environment that has benefitted organizations for more than 20 years and has many legacy components necessary to support AD feature backward compatibility. AD DS has the following features:

- Hierarchical and granular and based on the X.500 standard.
- Implements Lightweight Directory Access Protocol (LDAP) for managing directory objects.
- Administrative ability is defined by group membership.
- Objects are stored in containers called organizational units (OUs) that represent the structure of your organization, as shown in Figure 2-1.
- Group Policy manages the administration of objects, as indicated in Figure 2-1.
- Kerberos protocol is primarily used for AD DS authentication.
- Computer objects represent computers that join an Active Directory domain.

NOTE **JOINING AN AD DS DOMAIN**

Only computers running the Windows operating system can be domain-joined.

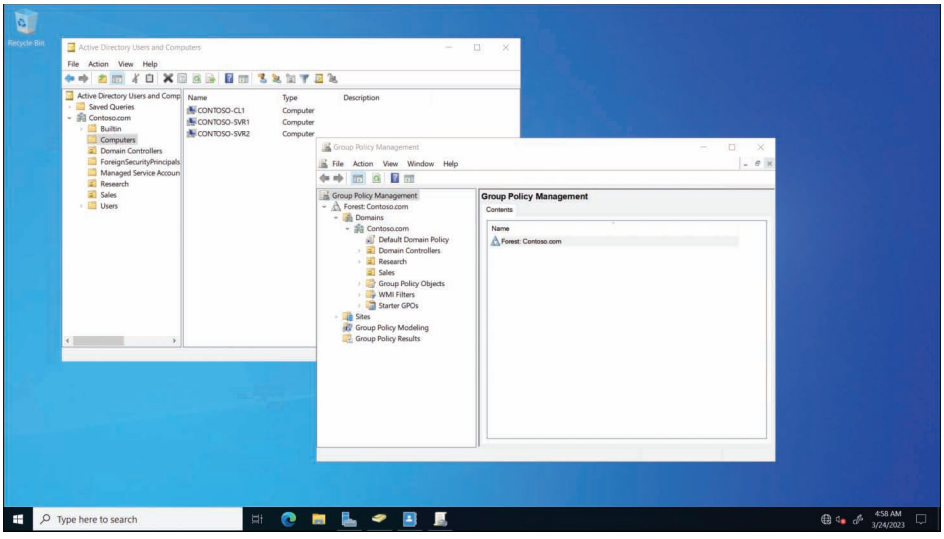

FIGURE 2-1 Management tools on an Active Directory domain controller

Azure Active Directory

Microsoft provides each cloud-based services subscriber, such as Microsoft 365, an instance of Azure AD (a tenant). Organizations can choose to add additional subscriptions, such as Microsoft Azure, and use the same Azure AD tenant for authentication and authorization. Alternatively, organizations can implement a separate Azure AD tenant for each subscribed service or app.

When you subscribe to a cloud service, like Microsoft 365, you can select a specific edition of Azure AD. The free version of Azure AD provides capabilities useful to most organizations; however, paid Azure AD Premium editions are also available, adding capabilities more relevant to large organizations.

It's important not to think of Azure AD as Active Directory in the cloud; instead, it's an entirely different authentication and authorization solution designed to support the cloud environment, unlike AD DS. Azure AD has the following features:

- Is flat, with no container hierarchy
- Provides for less fine-grained administrative control
- Uses role-based access control (RBAC)
- Supports administration management with profiles and group assignments
- Relies on Security Assertion Markup Language (SAML) and Open Authorization (OAuth)

When working with devices, you can add devices to Azure AD that are running a variety of operating systems, including

- Android
- iOS

- Linux
- macOS
- Windows 10 and newer

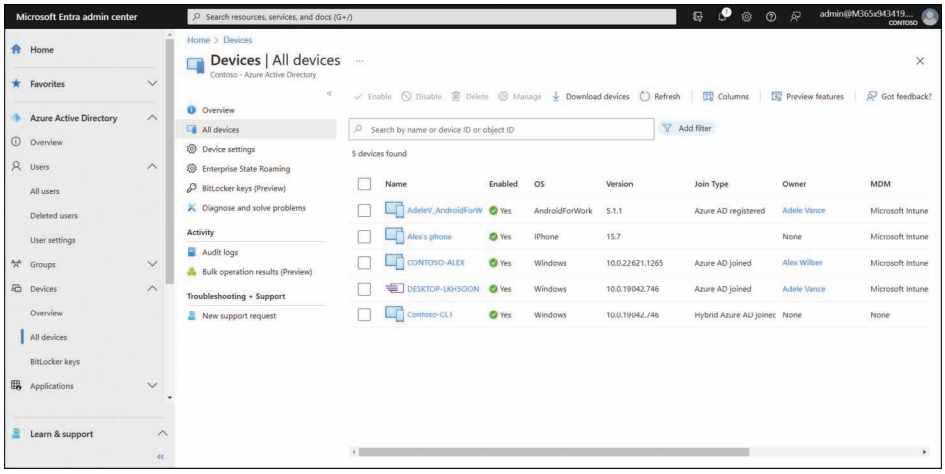

FIGURE 2-2 The Microsoft Entra admin center displaying the Azure Active Directory | All devices folder.

Implement user authentication on Windows devices, including Windows Hello for Business, passwordless, and tokens

You can sign in to your Windows 11 computer by using a variety of user accounts, depending on the configuration of your computer. The following list describes these account types:

- **Microsoft account** A consumer Microsoft account, often with an Outlook.com or Hotmail.com suffix.
- **Microsoft 365 account** An Azure AD account, usually called a Work or School account. Typically has an organizational suffix, such as Contoso.com. When a user adds a Work or School account to their device, they sign in using those account details, all services and apps accessed by the user automatically use the account to authenticate; this provides for cloud-based SSO.

EXAM TIP

By default, all Azure AD accounts are configured with a default tenant domain suffix. This default suffix is created when you obtain your Microsoft 365 subscription and always ends with `.onmicrosoft.com`. When configuring your Azure AD tenant, you typically add a custom domain name, such as `Contoso.com`, that your organization owns. Users can then sign in using either the custom domain suffix or the default domain suffix, although users find it easier and more logical to use the custom domain suffix.

- **Domain account** An AD DS account. If a computer is AD DS domain-joined, then a user can sign in at their computer using a domain account. When a user signs in using a domain account, all services and apps accessed by the user automatically use the account to authenticate; this provides for AD DS forest-wide SSO.
- **Local account** A computer user account. Typically, Windows 11 computers have local user and group accounts. A user might sign in using a local account when the computer belongs to them rather than the organization they work for. When users sign in using local accounts, they must configure the organizational account for each app or service they want to connect to. For example, they must add a Work or School account as part of a Microsoft Outlook profile to connect to Exchange Online.

Most users are probably familiar with signing in using a username and password. While that's acceptable and fairly common, Microsoft has added support for different authentication methods in Windows 11. These methods are designed to improve the sign-in experience and help make it more secure.

Understand multifactor authentication

Traditional computer authentication is based on users providing a name and password. This enables an authentication authority to validate the exchange and grant access. Although password-based authentication is acceptable in many circumstances, Windows 11 provides a number of additional more secure methods for users to authenticate with their devices, including multifactor authentication (sometimes referred to as two-factor authentication).

Multifactor authentication is based on the principle that users who want to authenticate must have two (or more) things to identify themselves:

- Know something (such as a password)
- Have something (such as a security token)
- Be something (such as fingerprints or biometrics)

For example, a user might know a password, have a security token (in the form of a digital certificate), and be able to prove who they are with biometrics, such as fingerprints or facial recognition.

EXPLORE BIOMETRICS

Biometrics, such as a fingerprint, provides more secure and often more convenient methods for identifying and verifying users and administrators. Windows 11 includes native support for biometrics through the Windows Biometric Framework (WBF), and when used as part of a multifactor authentication plan, biometrics is increasingly replacing passwords in modern workplaces.

Biometric information is obtained from the individual and stored as a biometric sample which is then securely saved in a template and mapped to a specific user. You can use a fingerprint reader to capture a person's fingerprint. (You "enroll" the user when configuring this.) Also, you can use a person's face, retina, or even voice. The Windows Biometric service can also be extended to include behavioral traits, such as body gait and typing rhythm.

Windows includes several Group Policy settings related to biometrics, as shown in Figure 2-3, that you can use to allow or block biometrics from your devices. You can find Group Policy Objects here: `Computer Configuration\Administrative Templates\Windows Components\Biometrics`.

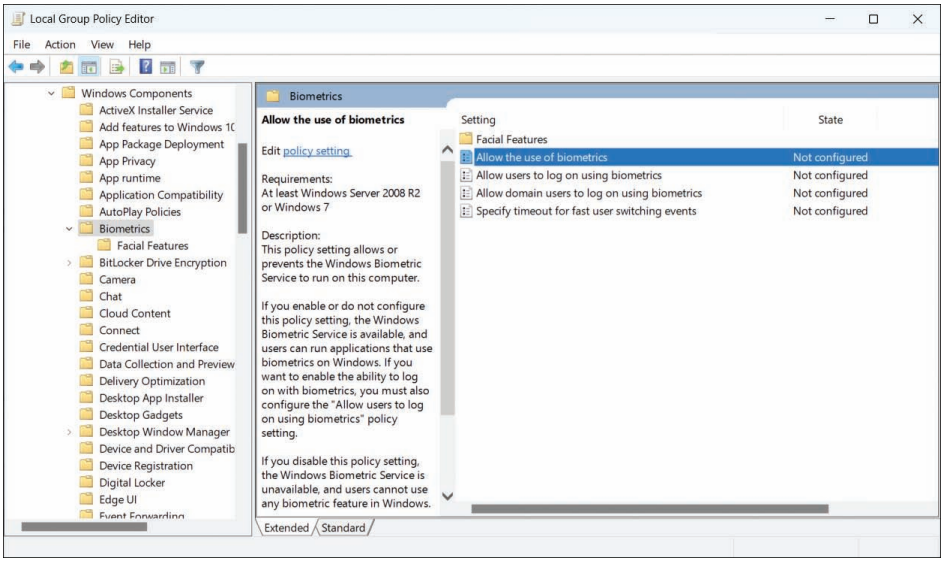

FIGURE 2-3 Biometrics Group Policy settings

Configure Windows Hello and Windows Hello for Business

Windows Hello is a two-factor biometric authentication mechanism built into Windows 11, and it is unique to the device on which it is set up. Windows Hello enables users to unlock their devices using facial recognition, fingerprint scanning, or a PIN.

Windows Hello for Business is the enterprise implementation of Windows Hello and enables users to authenticate to an AD DS or Azure AD account, and it allows them to access network resources. Administrators can configure Windows Hello for Business using Group Policy or mobile device management (MDM) policy and use asymmetric (public/private key) or certificate-based authentication.

Windows Hello provides the following benefits:

- Strong passwords can be difficult to remember, and users often reuse them on multiple sites, reducing security. Windows Hello enables them to authenticate using their biometric data.
- Passwords are vulnerable to replay attacks, and server breaches can expose password-based credentials.
- Passwords offer less security because users can inadvertently expose their passwords because of phishing attacks.