Chapter 1

Identity: Azure Active Directory

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Manage Azure Active Directory (Azure AD) objects**
  - **Create users and groups**
  - **Manage user and group properties**
  - **Manage device settings**
  - **Perform bulk user updates**
  - **Manage guest users**
  - **Configure Azure AD Join**
  - **Configure self-service password reset**

With the recent cloud transformation, the number of organizations migrating to the cloud has drastically increased, and security has become one of the primary concerns. In on-premises, the IT administrator and security administrators controlled the overall security of the organization. When it comes to the cloud, the traditional methods we are accustomed to should be replaced by modern identity and access management tools.

In Microsoft Azure, Azure Active Directory is a cloud-based directory and identity management service. Though the name looks like the Active Directory that we use on our on-premises Windows Servers for identity and access management, this one is completely different and takes access management to the next level. As an administrator, you will be working with Azure Active Directory day in and day out for various administrative tasks, including user management, group management, password reset, joining, registering your devices to Azure AD, and so on. Although these are basic tasks, sometimes administrative tasks include complex integrations such as single sign-on (SSO), multifactor authentication (MFA), and conditional access. From an exam standpoint, fulfilling the basic tasks is more than enough; however, having knowledge of the complex configurations will help you progress in your career.

Azure Active Directory

As mentioned in the introduction of this chapter, Azure AD is Microsoft's cloud-based identity and access management (IAM) solution. Azure AD is an especially useful solution for IT admins, developers, and subscribers of various Microsoft solutions (such as Microsoft 365, Dynamics 365, and Azure). Primarily, Azure AD deals with helping employees to sign-in to various resources such as O365, M365, Dynamics, Azure, etc. However, the integration does not stop here; you can integrate Azure AD as the IAM solution for third-party applications and your internal applications as well. Developers are constantly working on integrating Azure AD as the IAM solution because of the increased reliability it provides. Since this book is about Azure administration, we will focus on how Azure AD is intended to help IT admins.

Benefits

Let's explore the different benefits of Azure AD and why organizations should consider Azure AD as the IAM solution.

SSO to Cloud and On-Premises Applications Having too many credentials for different applications increases the complexity and results in a higher chance of human error because an SSO solution will help users to sign in to all cloud applications, on-premises applications, and devices using their corporate credentials. Azure AD is not only meant for Microsoft Stack, but for thousands of SaaS applications such as Dropbox, ServiceNow, DocuSign, etc.

Easily Extend On-Premises Active Directory to the Cloud When organizations move from on-premises to the cloud, there is a need to synchronize the users with the cloud. Otherwise, users will end up with two credentials, one for on-premises and another one for the cloud. To avoid this scenario and to provide a seamless SSO experience, Azure AD allows administrators to synchronize users, groups, passwords, and devices across both on-premises and the cloud. This is accomplished using a tool called Azure AD Connect that needs to be installed on your on-premises domain controller or any other domain-joined server with Windows Server 2012 or later, and it will help with the synchronization.

Cross-Platform Support Regardless of what platform the user is using, be it iOS, Android, Windows, Linux, or macOS, the sign-in experience is going to be the same, and the users can sign-in to their applications using their work credentials.

Increase Security of Your On-Premises Applications You can use the Azure AD Application Proxy service to access your on-premises applications via a secured remote access. The best part is you do not have to expose any additional ports on your on-premises firewalls; the access is managed by application proxy endpoints. The access can be tightened using multifactor authentication and conditional access policies.

Better Monitoring and Data Protection Azure AD amplifies the overall security posture of your environment by providing unique identity protection features. Azure AD Identity Protection comprises several features including suspicious sign-in activity, risk alerts, etc. These triggers can be further integrated with conditional access policies to make business decisions. In addition to these capabilities, administrators can leverage security reports, sign-in activities, and potential vulnerability reports that are available off the shelf without the need to deploy any additional components.

Self-Service Capabilities If you have worked as an IT administrator, you know most of the calls to the help desk will be regarding password resets. Azure AD offers a feature called Self-Service Password Reset by which users can reset their own passwords with the help of an authentication method such as phone, email, security questions, or a combination of these. IT admins need to enroll users into the SSPR program before they can use this feature. Enrolling is also self-serve, and the user will be prompted to verify the authentication methods. Enabling SSPR in your environment can elevate the security and reduce help-desk engagements.

If you are using Office 365, Azure, or Dynamics 365 in your environment, knowingly or unknowingly you are interacting with Azure AD to complete the authentication process.

We have been talking about Azure AD for a while now, and it is time that we understand the concepts that are part of Azure AD.

Concepts

Understanding the various terminologies that are related to Azure AD is the first step in learning Azure AD. The following are the Azure AD concepts:

Identity An object that can interact with Azure AD and get authenticated is called an *identity*. A user is an exceptionally good example of an identity; to get authenticated, a user will present the username and password to Azure AD. Upon receiving these credentials, Azure AD will substantiate and confirm if the authentication was successful. Servers and applications can also use their identity to authenticate with Azure AD; since these can be authenticated, they are also called *identities*. When it comes to servers or applications, they use certificates or secrets for completing the authentication.

Account Any identity that has data associated with it is called an *account*. For example, if we take a user named John Doe, the user will have different data attributes associated to it such as user principal name, sign-in name, manager name, department, etc. All the data associated to the user identity will make the identity an account. Since identity is required for mapping these attributes, you cannot have an account without an identity. The account can be on-premises as well as in the cloud.

Azure AD Account Usually known as work or school accounts, these accounts are provisioned in Azure AD or via other cloud services such as Office 365, etc. The data associated to these identities is stored in Azure AD and can be used to log in to services that use Azure AD as the authentication provider.

Azure Subscription This is the container created in Azure to separate billing and environments. An account can have multiple subscriptions that can be used to create isolated environments and billing boundaries. Each subscription you create will be mapped to a tenant, and it is always a one-to-one mapping. You can always move subscriptions across tenants if you have a multitenant environment.

Azure AD Tenant/Directory The term *tenant* means a single instance of Azure AD denoting a single organization. When you sign up for any Microsoft cloud service (Azure, O365, etc.), a dedicated instance of Azure AD is provisioned for you. There will be a unique name associated to this tenant that will have the suffix `onmicrosoft.com` and a unique ID assigned to the tenant called the *tenant ID*. An organization can create multiple directories/tenants for creating disparate environments or realms with different users and groups.

Now that we are familiar with the concepts related to Azure AD, the next question you will have in your mind is how Azure AD is different from Active Directory Domain Services.

Azure AD vs. Active Directory Domain Services

You might have already worked or heard about Active Directory Domain Services (AD DS) in your on-premises environment. If you have not heard about AD DS, this is a deployment

of the Active Directory service/role on Windows Server. The server can be a physical or virtualized one. The primary focus of AD DS is to work as a directory service. There are several other components of Active Directory that get installed along with the directory service such as Active Directory Lightweight Directory Service (AD LDS), Active Directory Federation Services (AD FS), Active Directory Certificate Services (AD CS), and Active Directory Rights Management Service (AD RMS). You can also implement AD DS in Azure by installing the Active Directory Domain Services role on your Windows virtual machines deployed in Azure. This is not a recommended scenario unless you have a special scenario that requires AD DS deployment; for all other scenarios, Azure AD is recommended.

At first look, AD DS and Azure AD may look the same and both can be used for authentication and offer directory services; however, there are some differences in the way things work under the hood. The key point to understand here is if you install the AD DS role on an Azure Windows virtual machine, it is not equivalent to Azure AD. A lot of beginners have this misconception and assume both are the same. Well, that is wrong. The following are some of the key differences that make Azure AD different from AD DS:

Hierarchy A flat structure is used by Azure AD to represent or provision the users and groups. Therefore, organizational units (OUs) and Group Policy objects (GPOs), which exist in AD DS, do not exist in Azure AD.

Federation Services Azure AD supports Federation Services as an authentication method, and you can further integrate with third-party providers such as Twitter, Facebook, etc. On the other hand, in the case of AD DS, we can set up federation with another domain controller or forest only, and third-party integration is not supported.

Lack of LDAP In AD DS, we used a protocol called LDAP to query users, groups, or objects in Active Directory. In the case of Azure AD, since this is an HTTP/HTTPS-based service, we will be using the REST API for querying instead of LDAP.

Lack of Kerberos AD DS deployment uses Kerberos authentication; however, Azure AD uses HTTP/HTTPS protocols like SAML, OpenID Connect for authentication, OAuth for authorization, and SAML. Developers can choose any of these communication protocols while they design security for their applications.

Management Azure AD is a managed service, and it is an underlying infrastructure; the availability is managed by Microsoft. If AD DS is deployed on an Azure Windows virtual machine, the configuration, management, virtual machine patching, updates, upgrades, and other maintenance tasks should be taken care by the end customer.

Azure AD: Licensing

You have seen that Azure AD offers a lot of add-on features more than legacy identity and management solutions. These features come with a price, and not all organizations need all these features. Licenses are categorized based on the number of premium features it supports. There are four editions of Azure Active Directory.

Azure Active Directory Free As the name implies, this is the free version of Azure Active Directory and offers minimal features such as user management, group management, Azure AD Connect for syncing on-premises identities, basic reporting, SSO, SSPR, etc. If you have not purchased any Azure AD license, this is going to be your default edition.

Azure Active Directory Microsoft 365 Apps If you have O365, this edition of Azure AD is automatically provisioned for you. Besides the features offered by Azure AD Free, this edition offers additional functionalities such as IAM for Microsoft 365 Apps, branding, MFA, etc.

Azure Active Directory Premium P1 Azure AD Premium P1 offers all the capabilities of Azure AD Free and some additional premium features that can increase the overall security of your environment. Dynamic groups, self-serve group management, Microsoft Identity Manager, and password writeback are some of the additional features offered by Azure AD Premium P1.

Azure Active Directory Premium P2 This is the top edition of Azure AD and offers all features in the P1 and Azure AD Free editions; additionally, Identity Protection and Identity Governance are offered.

Table 1.1 provides a quick comparison of all editions of Azure AD and the features offered by each edition.

TABLE 1.1 Comparison of Azure AD Editions

Feature	Free	Microsoft 365 Apps	Premium P1	Premium P2
Directory objects	500,000	Unlimited	Unlimited	Unlimited
Single sign-on	Unlimited	Unlimited	Unlimited	Unlimited
Core identity and access management	✓	✓	✓	✓
Business-to-business collaboration	✓	✓	✓	✓
Identity and access management for Microsoft 365 apps	×	✓	✓	✓
Hybrid identities (password writeback)	×	×	✓	✓
Advanced group access management	×	×	✓	✓
Conditional access	×	×	✓	✓
Identity protection	×	×	×	✓
Identity governance	×	×	×	✓

The pricing of Azure AD licensing can be reviewed on the Azure AD pricing page.

`https://azure.microsoft.com/en-us/pricing/details/active-directory`

In addition to these editions, if you already have an Office 365 E3/E5 license, then you can use the premium features of Azure AD, and you do not have to pay for these licenses separately. P1 is included in E3, and P2 is included in E5, respectively.

Since you have the basic understanding of the editions of Azure AD and how they are different from a traditional Active Directory deployment, let's talk quickly about custom domains in Azure AD.

Custom Domains in Azure AD

Every tenant will have two properties that make it unique from other tenants created by other organizations (tenant ID and the tenant initial domain). By default, when you create a tenant, there will be a default domain that will look like `<yourdomainname>.onmicrosoft.com`. This initial domain cannot be changed or deleted once the tenant is provisioned. Because of the uniqueness of this domain name, sometimes you will not get the domain name that you are looking for. For example, when you try to sign up for a Gmail or Outlook mailbox, you get an option to choose a username. Though you have a choice, username allocation works based on the availability of the username. Sometimes you might try to get an email with your name, and you might end up with Gmail suggesting some usernames having random numbers because the one you asked for is not available. The same concept applies to the initial domains as well; if the name you request is taken, then you must append some letters or numbers to make the name unique.

If the tenant was created while you signed up for the Azure subscription using your email address, then Microsoft Azure uses your email address and considers that as the initial domain name. You can create additional domains, and at that point you will get an option to choose the initial domain name. Refer to the "Managing Multiple Directories" section in this chapter to understand multitenant environments.

The problem with this approach is that all the users you create will have this initial domain assigned to their username. Since you have added letters and numbers to make it unique, this initial domain is hard to remember and not user friendly. To resolve this issue, you can use custom domains in Azure AD.

Using custom domains, you can use your domain that you created with the domain registrar. Adding custom domains requires you to validate and prove to Azure that you own the domain. This verification can be completed by adding a TXT/MX record to your DNS domain. The value for this DNS record will be given by Azure. When you add a domain to Azure AD, it will be unverified. After you add the DNS record to your DNS zone, you can initiate the verification request, and Azure AD will start querying your domain to verify if the value given by Azure is returned as the answer for the DNS query. Once the record

is returned, Azure AD will mark the domain as verified, and you will be able to use the domain when you create users. You can have multiple domains and keep one of them as your primary.

Nevertheless, this is not a daily task for the administrators, and this is a one-time setup. In the future, if more domains need to be linked, then you may have to repeat the verification process. This topic is not part of the exam; however, understanding custom domains will help you set up your test environment with a custom domain. In this chapter, the exercises will have a custom domain name instead of the `onmicrosoft.com` domain name. I hope that this quick introduction of custom domains will help you understand why your test environment has an `onmicrosoft.com` domain and the exercises have a proper domain name.

If you would like to add your custom domain to Azure AD, please follow the process outlined in this documentation:

```
https://docs.microsoft.com/en-us/azure/active-directory/
fundamentals/add-custom-domain
```

On that note, we will start with users and groups in Azure AD.

Users and Groups

Users and groups are the primary objects of every IAM solution, and Azure AD also has a user and group management system, which is the backbone for access management. You have seen what an account is; just to refresh what we discussed; an account is an identity that has data associated to it. In Azure AD, you have user accounts and group accounts for managing users and groups. Let's get started with user accounts and see the operations that are available for administrators.

User Accounts

As the name suggests, user accounts consist of user identities, which will be used by users to log in to services such as Azure, O365, Dynamics 365, SaaS applications, and other third-party applications that are integrated with Azure AD.

You should create a subscription for testing all labs in this book. You can create a Free Trial subscription. If you are using your personal email address to sign up for the subscription, a new tenant will be automatically provisioned for you. All operations can be performed on that tenant.

Now that you know what a user account is, it is time to see how you can see users in our directory.

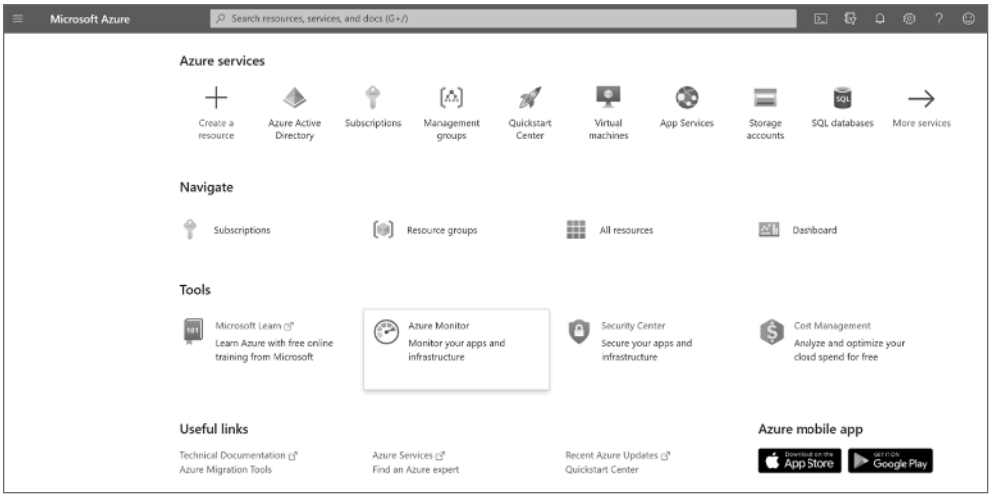
Viewing User Accounts

If you are working on a new directory that was set up for testing the exercises in this book, then you won't have any additional users apart from the account that you used to sign up for the subscription. However, in a production environment, there will be hundreds of users. As an administrator, you will be asked to verify if the account exists in Azure AD or get information about a particular user. Hence, knowing how to view user accounts is particularly important in an IT admin's daily job. We will follow a step-by-step process to view the users in your directory, as shown in Exercise 1.1.

EXERCISE 1.1

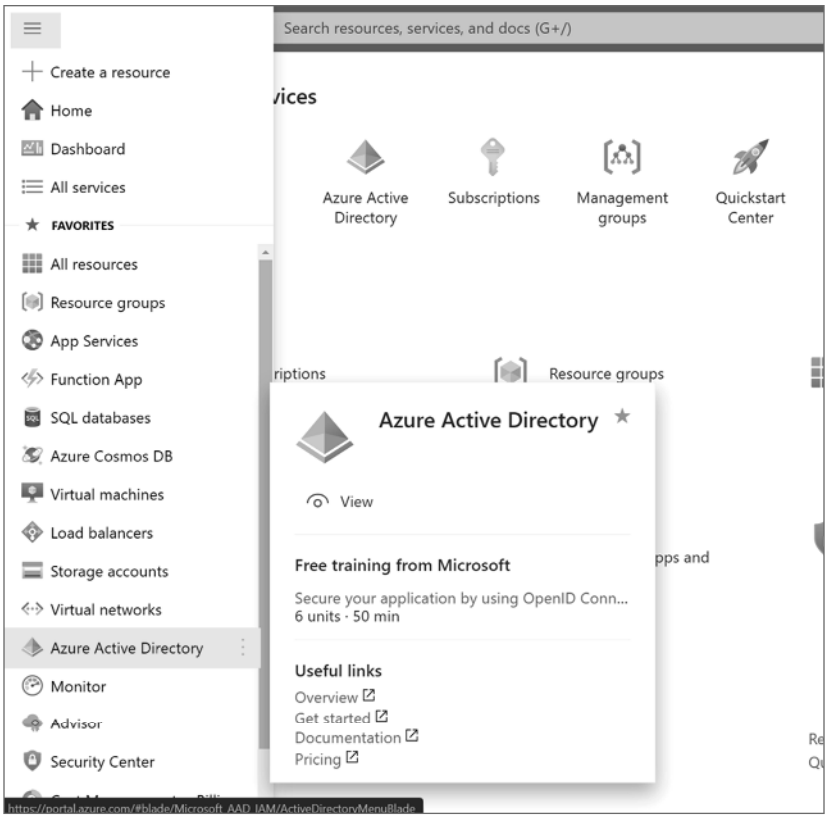
Viewing Users in Your Directory

1. Open your browser (Microsoft recommends that you use the latest version of your favorite browser) and navigate to the Azure portal, which is available at `https://portal.azure.com`.
2. A sign-in screen will be presented to you. Sign in using the email address that you used to create the subscription. The data you enter (username and password) will be sent to Azure AD. If the credentials are correct, then you will be logged in.

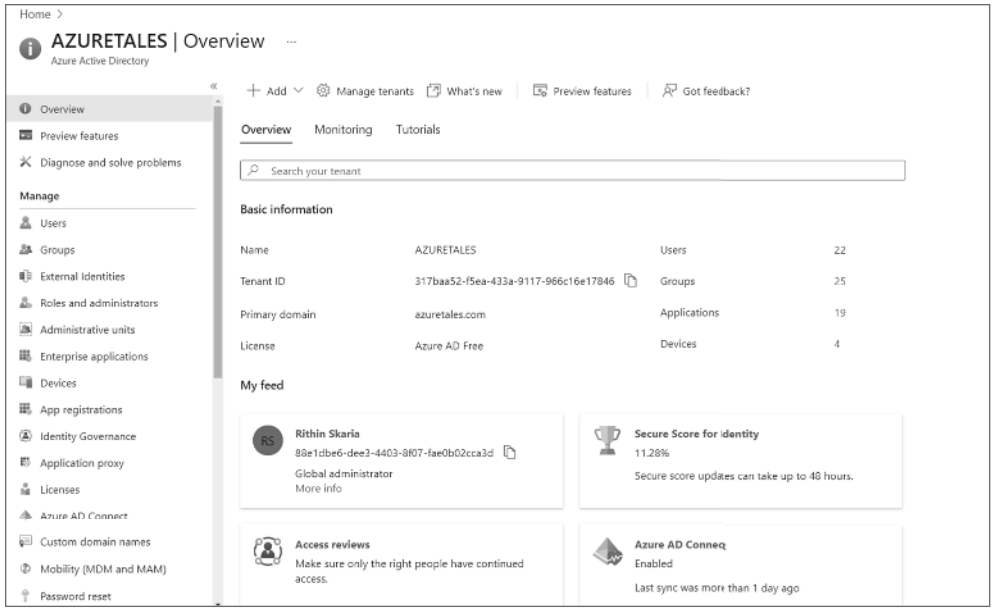


3. Now that you are in the Azure portal, you can click the hamburger icon at the top-left corner and click Azure Active Directory.

EXERCISE 1.1 *(continued)*

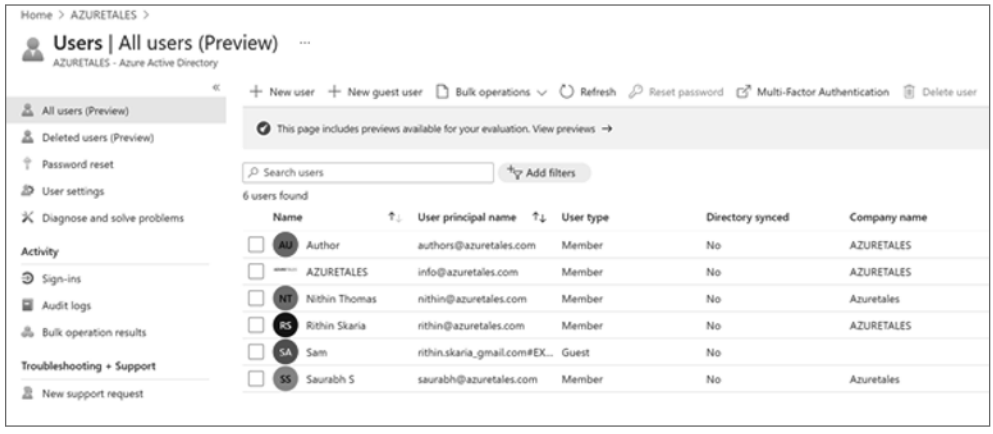


4. Selecting Azure Active Directory will take you to the Overview blade of Azure Active Directory. This blade gives you some idea about certain aspects of your Azure AD such as the tenant ID, tenant name, primary domain associated to your tenant, edition of Azure AD, and number of users, groups, applications, and devices. If you scroll down, you will see more information such as your account, Azure AD connect, secure score, etc. The graphic here shows the overview of the tenant that is used for the demonstration.



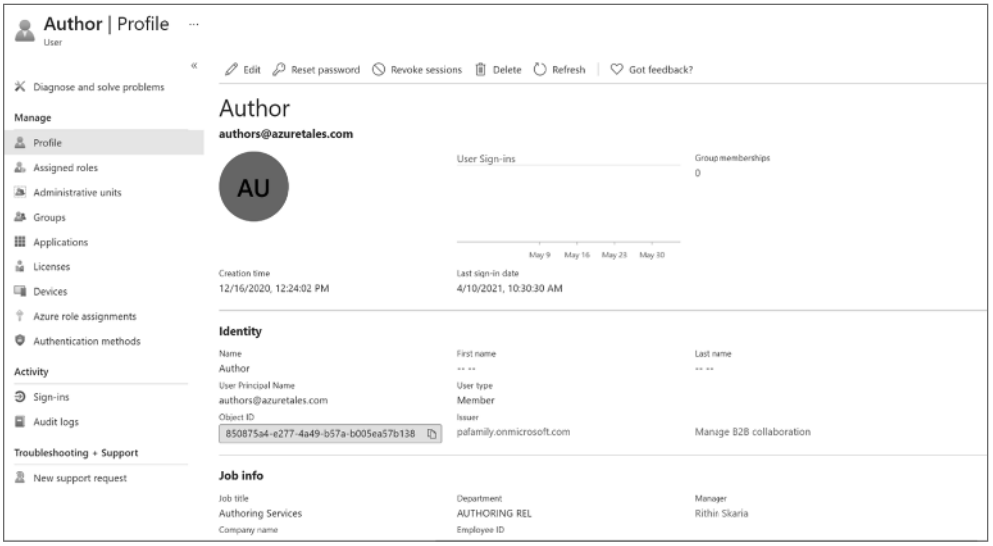
If you take a close look at the graphic, you can see at the top the option that will let you create, manage, and delete tenants. These options are quite useful if you are managing a multi-tenant environment. One thing to note here is that deleting a tenant requires you to cancel all active Azure subscriptions that are part of the tenant. You cannot delete a tenant when there is an active Azure subscription associated with that tenant. Since we are working on user management, let's shift our focus to the Users blade under the Manage section.

5. Once you click the Users blade, you will be presented with the All Users view. Your view might be different from what is shown here as it is displaying the users in the demo tenant.



EXERCISE 1.1 *(continued)*

6. If you click any user, you will be presented with the details of the user such as name, user principal name, job title, department, manager, etc., along with the creation date and last sign-in date.



In this section you saw how to view the existing users in the directory and find the details of a user. Now that you know how to find a user in the directory, let's see how to add a new user to the directory.

Adding Users

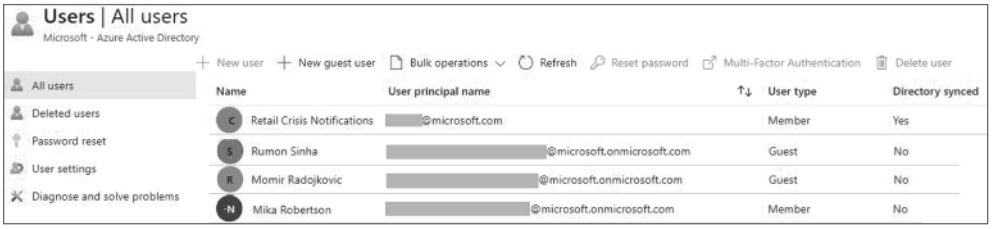
In an enterprise environment, user insertion happens frequently, and cloud administrators are responsible for this. Whenever a new employee joins the organization, administrators are required to create their account, add the necessary licenses, complete their profile, set up their initial password, etc. In this section, we will add users from the Azure portal to understand the user insertion process. Before we start the exercise, it is important you know the user types that are available in Azure AD. There are three types of users in Azure AD.

Cloud Identities As the name implies, these are identities that are created in Azure AD and exist only in Azure AD. In the upcoming exercise, we are going to create a user called John Doe in Azure AD. This user is going to be a cloud identity as the user will exist only in Azure AD. Another point to note here is that the user can be part of another Azure AD as in an Azure AD of another organization. For instance, assume that there is a company `abc.onmicrosoft.com` with a user called Jane Doe. Jane Doe can be added to another company's Azure AD, say, `xyz.onmicrosoft.com`, through an

invitation process also known as *business-to-business collaboration*. In this case, Jane Doe is a cloud identity of `abc.onmicrosoft.com` and she is added to `xyz.onmicrosoft.com` for collaboration. When Jane's account is deleted from her primary directory (`abc.onmicrosoft.com`), her presence in the other directory is not automatically removed; we have to perform this action manually.

Directory Synchronized Identities As mentioned earlier, one of the features in Azure AD is that you can synchronize your on-premises Active Directory to Azure AD. If you have an identity that is synchronized, then you will see Yes in the Directory Synced column for the user in the All Users view (Figure 1.1).

FIGURE 1.1 Distinguishing directory synchronized users



Guest Users These are accounts that exist outside of Azure. These include Microsoft accounts (earlier known as Live accounts) or accounts from other identity providers and accounts from other organizations. The identities are not part of your organizational Azure AD; they need to be invited to your tenant for collaboration. These accounts will be shown as Guest if you look at the User Type value of the user (refer to Figure 1.1). Once the collaboration is no longer required, you can delete these accounts from your user list, and the access will be revoked.

Additionally, we need to keep a couple of points in mind while managing users.

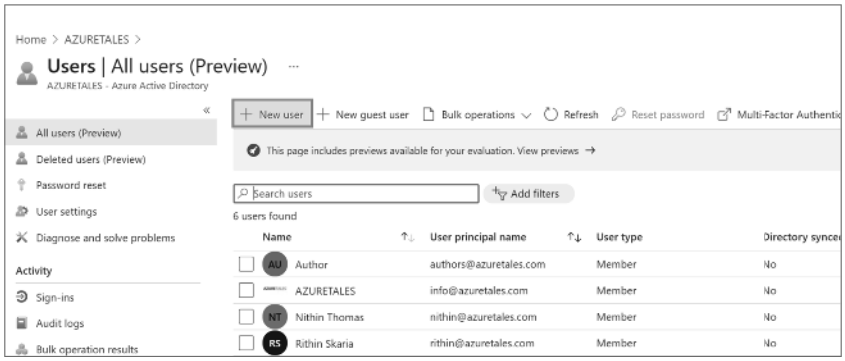
- You must be a Global Administrator of the tenant to manage the users. This is one of the Azure AD roles that we will discuss later in this chapter. The Global Administrator role is like a superuser role and should be granted to users who need to manage all aspects of Azure AD. There are other roles like User Administrator who can manage the users, but this can be used only for managing non-admin accounts.
- While creating a username, the name and password are the only mandatory options. You have two choices with password. First, you can let the system generate a password for the user. The second option is to bring your own password. In both cases, the user will be asked to change the password during the first sign-in, and as an administrator, you should be finding a way to securely share the password with the new user. The commonly used method is to email the new user's manager.
- Even though the users can be deleted (will be covered in the "Deleting and Modifying Users" section), you can restore these users within 30 days from the deletion date.

Now that we are clear about the different user types and key points, let's create users in Azure AD, as shown in Exercise 1.2.

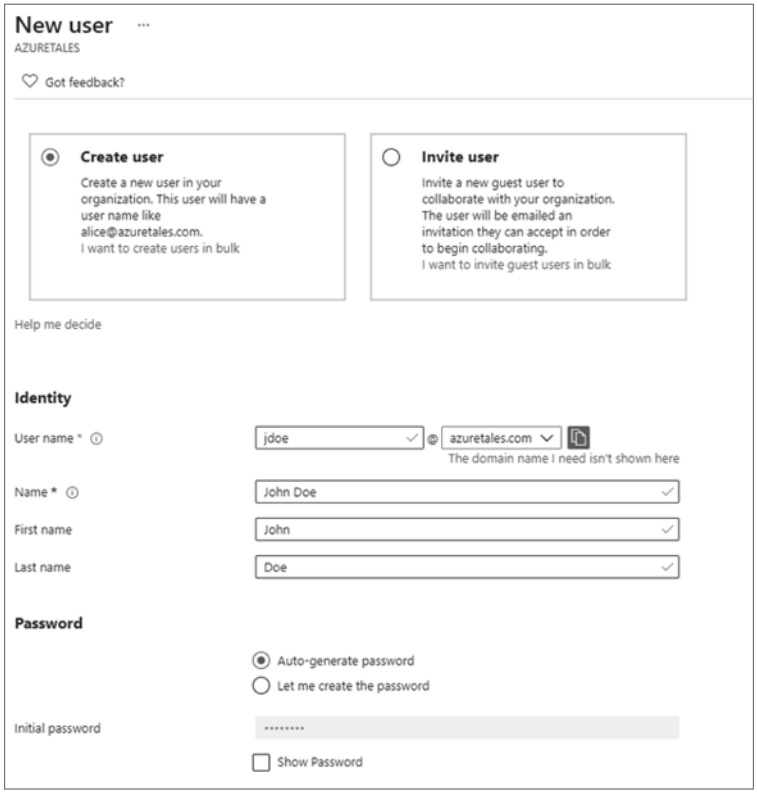
EXERCISE 1.2

Creating Users in Azure AD

1. Navigate to the All Users blade inside Azure Active Directory. You can follow the steps 1–5 of Exercise 1.1 to reach the All Users blade.
2. Once you are in the All Users blade, you can click the New User option.



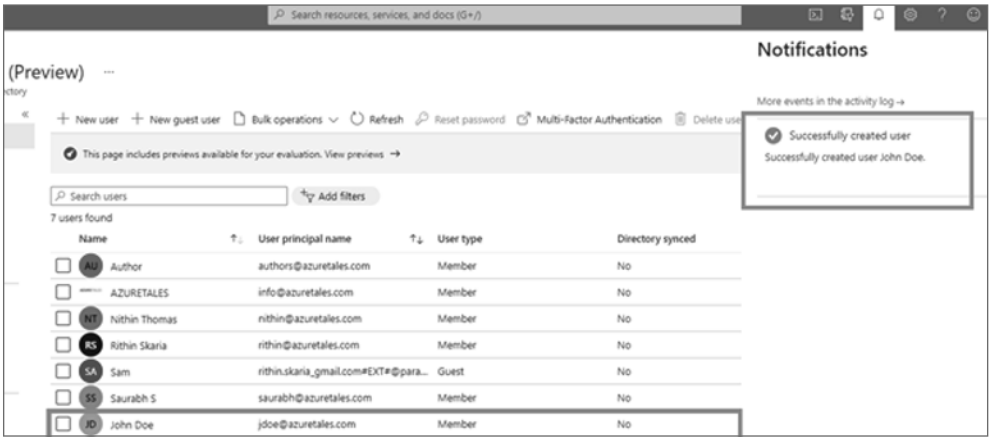
3. Selecting New User will display a window to input details of the new user you intend to create. You will be presented with two options, Create User and Invite User.



4. Selecting Create User will help you create a cloud identity that will exist only in Azure AD. On the other hand, if you select Invite User, you can invite a person from another Azure AD or a person who doesn't have an Azure AD account (Guest user) via an invitation process. In this exercise, we will choose Create User as our plan is to create a cloud identity user type.

5. Here the username, name, and password are the mandatory fields. You can fill in the fields First Name, Last Name, Department, Job Title, Contact Info, Profile Picture, etc., if you'd like; they are optional. In the previous graphic, you can see that we have left Password as "Auto-generate password," which means that the system will generate the password for the user. You can see the password by enabling the Show Password option.

6. Since we have filled the mandatory fields, we can click Create to provision the user. Within a couple of seconds, you will get a notification that the user is created, and the new user will be visible in your All Users blade.



You have successfully created a new user in the Azure AD. As of now, we have covered two exercises where you are viewing and adding users to Azure AD. As an administrator, your responsibility does not stop here; in your daily tasks you will be asked to delete users when someone leaves the organization, modify user attributes when they move to a different department, or change their location. To give you the idea of how to delete and modify users, let's head to the next section.

Deleting and Modifying Users

As mentioned in the previous section, whenever someone gets promoted, moves to a different department, or changes their work location, these details need to be updated on the user profile. Though these fields are not mandatory, they will be important in understanding more details about the user. Assume that there are two John Does in your organization—one works for HR and the other one works for IT. Adding department details here will help the administrator to perform the operations on the right user. In Exercise 1.3, we are going to modify the user we created in Exercise 1.2 and then delete the user.

EXERCISE 1.3

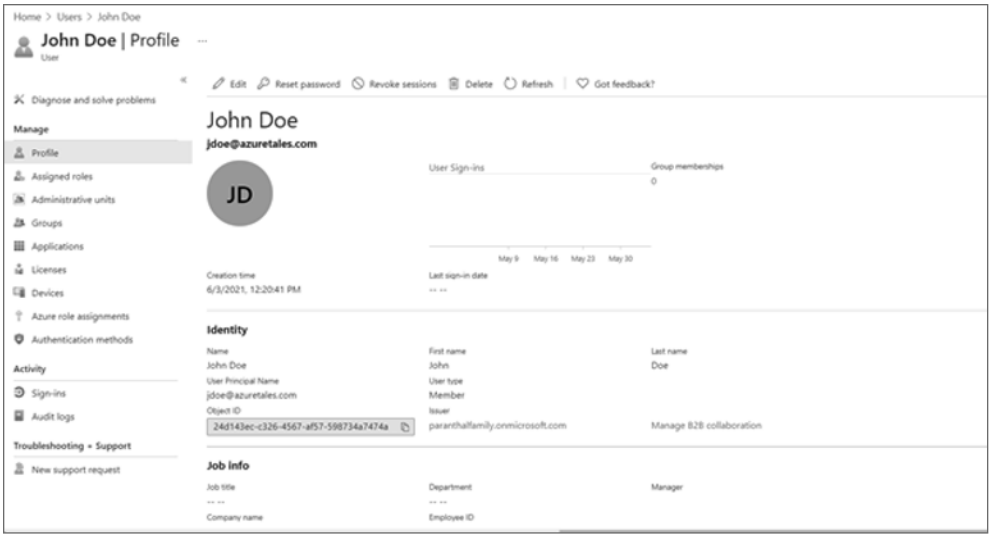
Modifying and Deleting Users

Let's perform the update process on the user we created in Exercise 1.2. The tasks we have here are as follows:

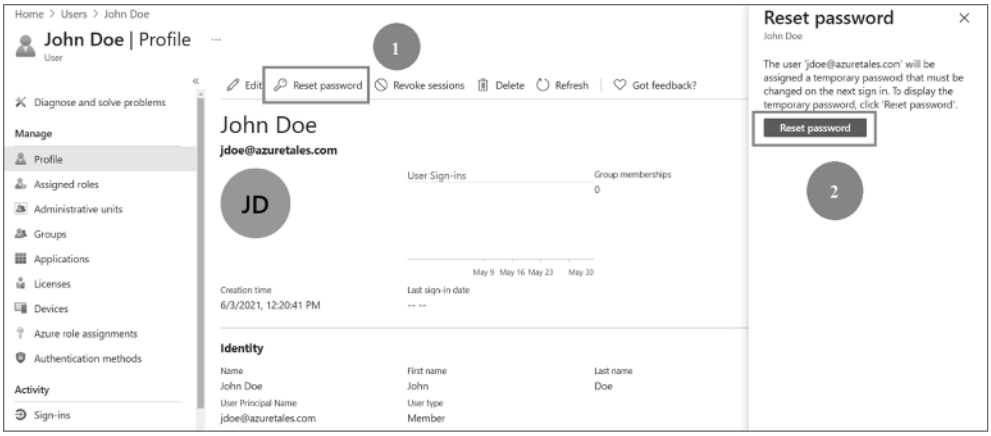
- Reset the password of the user to a new password.
- Change the department of the user to HR.
- Add the employee ID as 1322.
- Verify the user details.
- Delete the user.

The first step here is to navigate to the All Users blade as we have done in Exercise 1.1; you can follow these steps to update the user attributes:

1. From the All Users blade, select the user John Doe by clicking the name; that will take you to a screen similar to the following one.



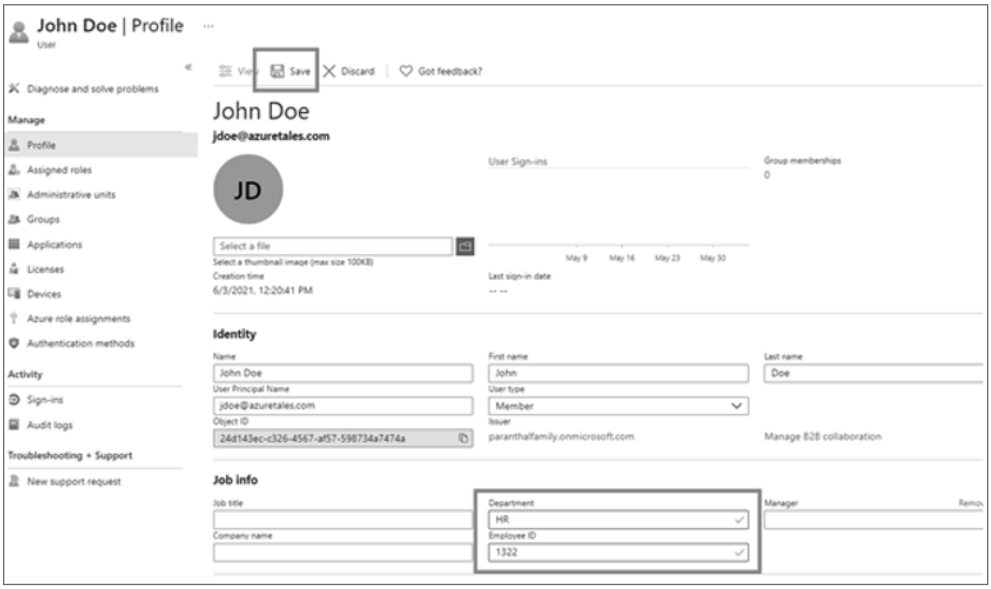
2. Since our first task here is to reset the password, you can click Reset Password, and you will be asked to confirm whether you want to proceed with the reset process. You must click again the Reset Password option, which will be visible in the right corner of the screen. To reset a user's password, you need to be the Global Administrator. User Administrators, Helpdesk Administrators, and Password Administrators can also reset the passwords of non-administrative accounts. However, User Administrators, Helpdesk Administrators, and Password Administrators cannot reset the password of a Global Administrator. Password reset of the Global Administrator can be done only by another Global Administrator.



3. Confirming the reset password option will display a temporary password on the screen. This needs to be changed on the first sign-in after the reset as this is a temporary password and an administrator is responsible for sending this password securely to the user.

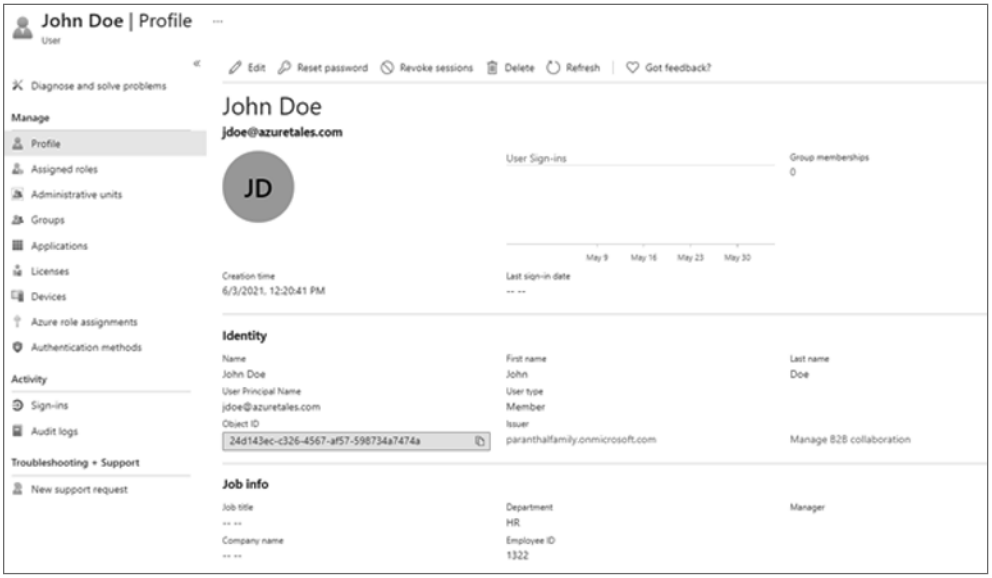
4. Now that you have reset the password, the next task is to update the department and employee ID. If you recall, we skipped these optional fields while creating the user, and it is time now to update them. To edit the user details, you can click the Edit button, which is on the left side of the Reset Password button.

5. Clicking the Edit button will enable all the text boxes. Once you have updated the information, you can click Save. You can update all information except the object ID, which is a unique ID assigned to every identity by Azure AD.



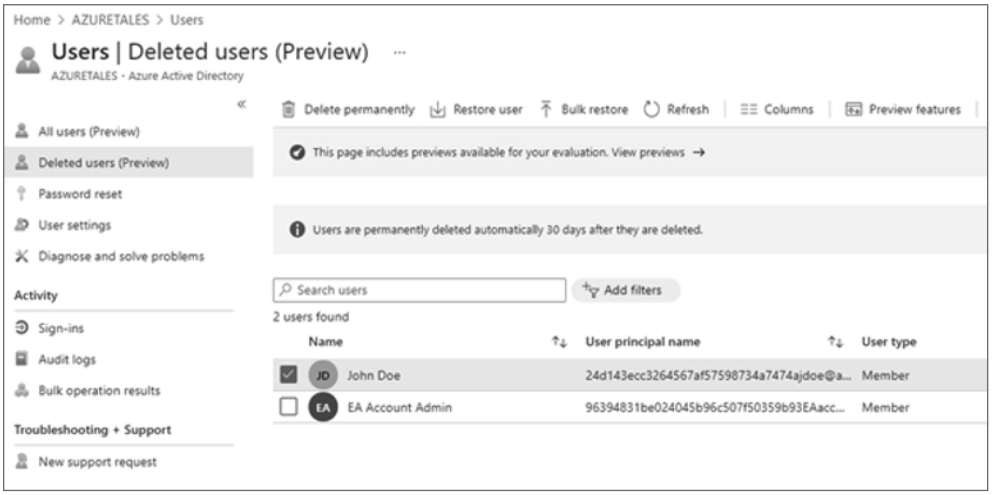
EXERCISE 1.3 *(continued)*

6. After saving the details, if you go back to user profile, you will be able to see that all the data you entered is populated to the user profile.



7. From this graphic, we confirmed that the department details and employee ID have been added to the user profile. The next task is to delete the user. Assume that John Doe is leaving the organization and you have to deprovision his account. In the graphic, you can see that there is a Delete button next to the Reset Password button. Clicking Delete will ask for your confirmation.

8. Click Yes, and John Doe's profile will be deleted. However, this is not a permanent delete action. All deleted users can be viewed from the Deleted Users blade.



9. You will have 30 days from the deletion date if you want to restore the user, using the Restore option. You can also delete the user immediately by selecting the Delete Permanently option instead of waiting for 30 days.

All these actions can be also performed from the Office 365 Admin panel, PowerShell, or CLI if required.

In Exercises 1.1, 1.2, and 1.3 you have seen how an administrator can view, add, modify, or delete users. Performing these tasks one by one from the portal is not a great idea if you have a large user base. All the actions that you have seen in the previous exercises can be performed in bulk. In the next section, you will learn how administrators can leverage bulk operations available for user accounts.

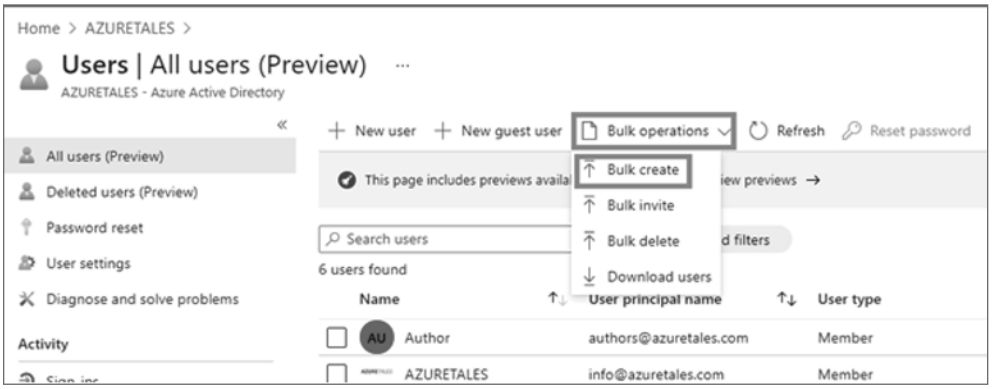
Bulk Operations

In an enterprise environment, new users are added, updated, or deleted in bulk. Performing these actions one by one for each user is a hectic task, and there is a higher chance of human error. You need to automate these tasks and should be able to perform these tasks in bulk. Azure AD provides bulk operations by which you can create, invite (for guest users), delete, and download users in your directory. These bulk actions are achieved via uploading a CSV file with the details. This file template will be available for download from Azure Portal itself. In the next exercise, you will use a bulk operation to create nine users (all Avengers characters) in a single shot, and once they are visible on the portal, you will perform a bulk delete operation. See Exercise 1.4.

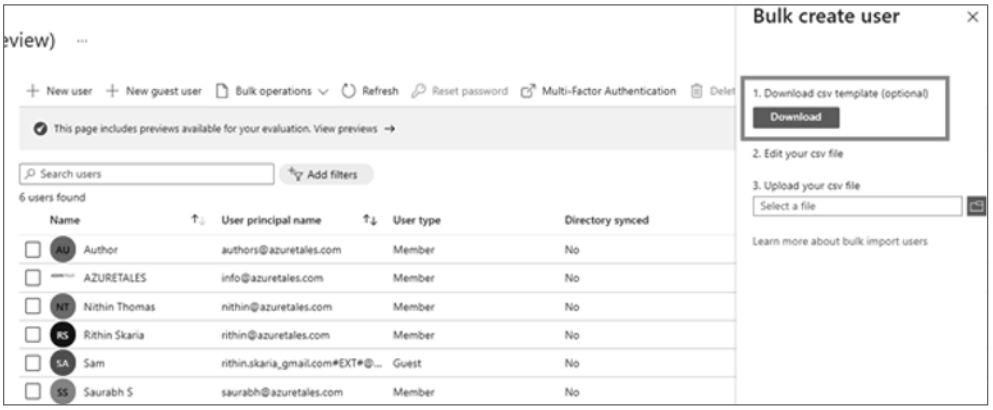
EXERCISE 1.4

Performing Bulk Operations

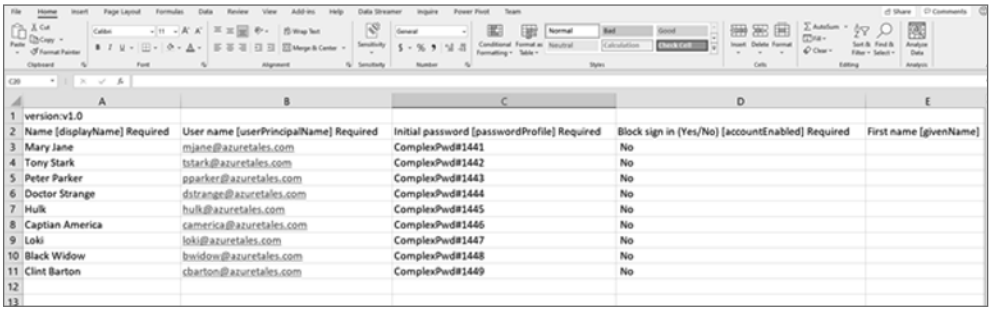
1. Navigate to the All Users blade. If you are not able to recall the steps to reach the All Users blade, please follow steps 1–5 of Exercise 1.1.
2. Select Bulk Operations and then select Bulk Create.



3. Selecting Bulk Create will let you download a CSV template. You need to download the template, fill in the details, and upload it to Azure AD for processing. Azure will prompt you with the steps.



4. Once the file is downloaded, you can open it in Microsoft Excel and fill in the details. The headers will be auto populated; some of them are required, while some are optional. The fields that are required will have a [Required] tag in the header. The required fields are Name, Username, Initial Password, and Block Sign In. Fill in the template, as shown here.



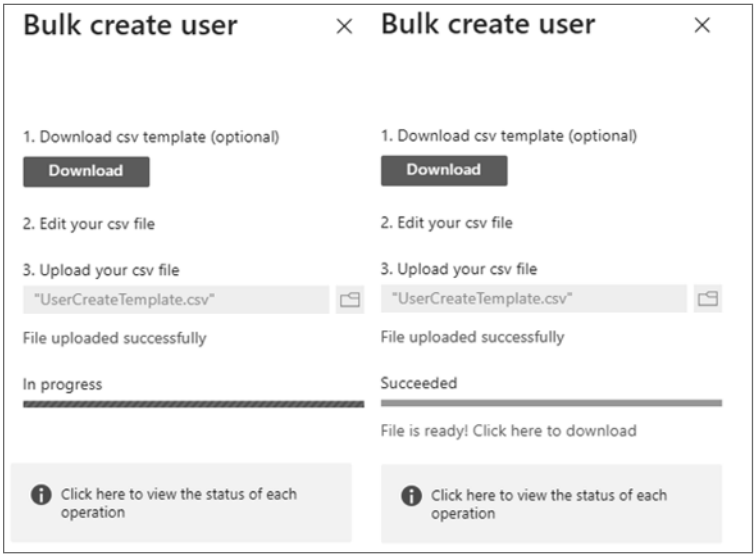
	A	B	C	D	E
1	version:v1.0				
2	Name [displayName] Required	User name [userPrincipalName] Required	Initial password [passwordProfile] Required	Block sign in (Yes/No) [accountEnabled] Required	First name [givenName]
3	Mary Jane	mjane@azuretales.com	ComplexPwd#1441	No	
4	Tony Stark	tstark@azuretales.com	ComplexPwd#1442	No	
5	Peter Parker	pparker@azuretales.com	ComplexPwd#1443	No	
6	Doctor Strange	dstrange@azuretales.com	ComplexPwd#1444	No	
7	Hulk	hulk@azuretales.com	ComplexPwd#1445	No	
8	Captian America	camerica@azuretales.com	ComplexPwd#1446	No	
9	Loki	loki@azuretales.com	ComplexPwd#1447	No	
10	Black Widow	bwidow@azuretales.com	ComplexPwd#1448	No	
11	Clint Barton	cbarton@azuretales.com	ComplexPwd#1449	No	
12					
13					

5. You can fill the optional details if required; however, it is mandatory to fill in the required fields; otherwise, the validation will fail.

6. Let's upload the file to Azure AD and see if we got it correct. You can use the upload option shown in step 3. If you closed the window after downloading the CSV file, you can click Bulk Operations ➢ Bulk Create and the upload window will be shown again. If the file is uploaded successfully, you will see a message on the screen. Once the file is uploaded, click Submit.

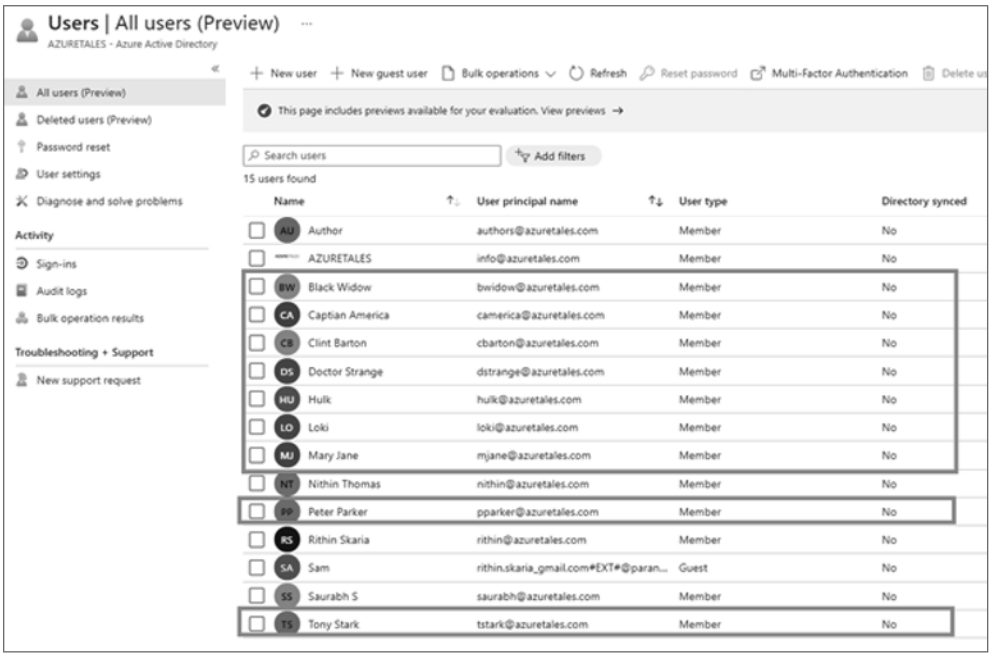
EXERCISE 1.4 *(continued)*

7. As soon as you click Submit, the status will change to "In Progress." If the format is correct, then you will get a "Succeeded" message.



8. You can also verify the status of any bulk operation by navigating to the Bulk Operation Results blade. You will be able to troubleshoot from this blade if you get an error during the bulk operation.

9. Since our bulk operation was successful, let's confirm if the users are visible in the All Users blade.



Similarly, you can perform bulk delete and bulk invite operations by downloading the corresponding CSV and uploading them back to Azure AD. Speaking about invitations, let's see how external users can be invited to your tenant for collaboration.

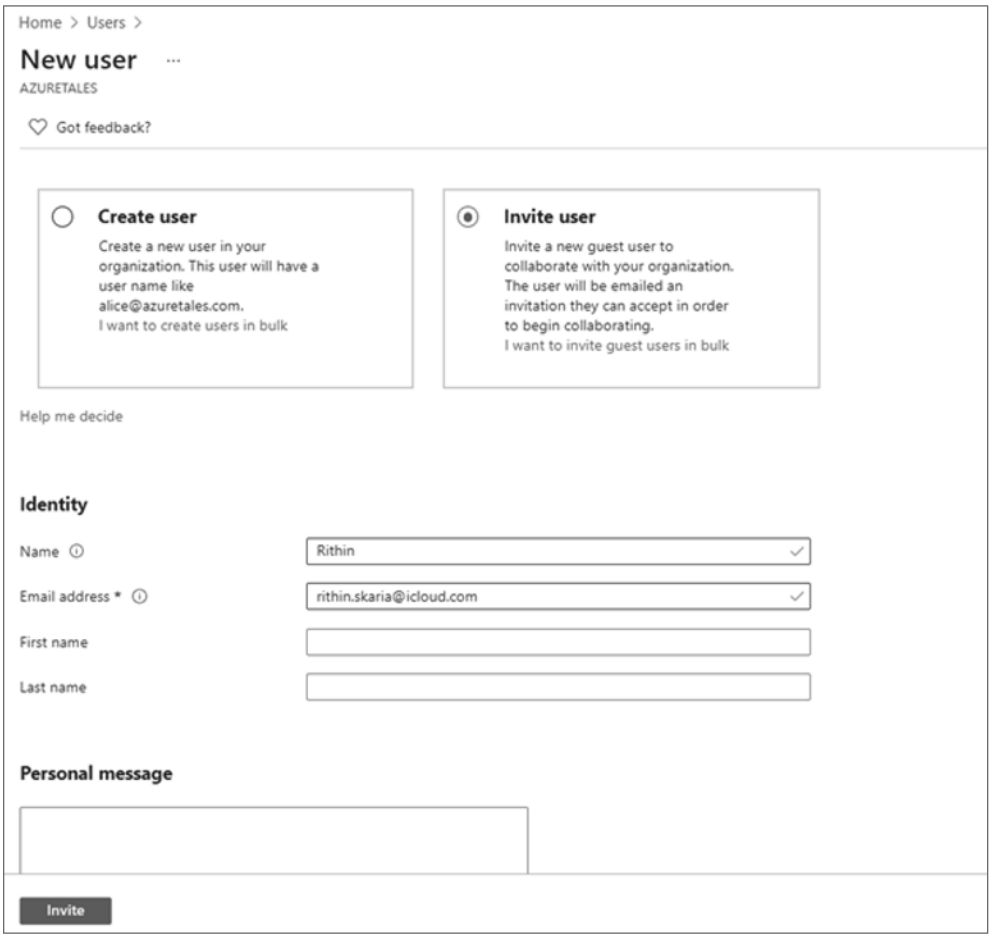
From the Deleted Users blade, you can perform bulk delete and restore operations if required.

Inviting Users

In the "Adding Users" section, we discussed several types of users. If you recall, we talked about Guest accounts (Microsoft accounts and users from external Azure ADs). These users need to be invited to your tenant. Recipients can redeem the invitation and join your tenant for collaboration.

In the All Users blade, you have an option to add a new Guest user. Clicking New Guest User will redirect you to a screen similar to Figure 1.2.

FIGURE 1.2 Inviting users



You can also add a guest user by clicking New User and then selecting the Invite User radio button instead of Create User.

The only email address is the mandatory field, and you can even customize the personalized message. By clicking Submit, this message will be appended to the email invitation, which will be triggered to the recipient, as shown in Figure 1.3.

A sample invitation has been added for your reference (refer to Figure 1.4).

These users can be easily spotted in the All Users blade by looking at the User Type column. You can further add a filter in the blade as shown in Figure 1.5 to list all the Guest users in your tenant.

FIGURE 1.3 Customizing the invite

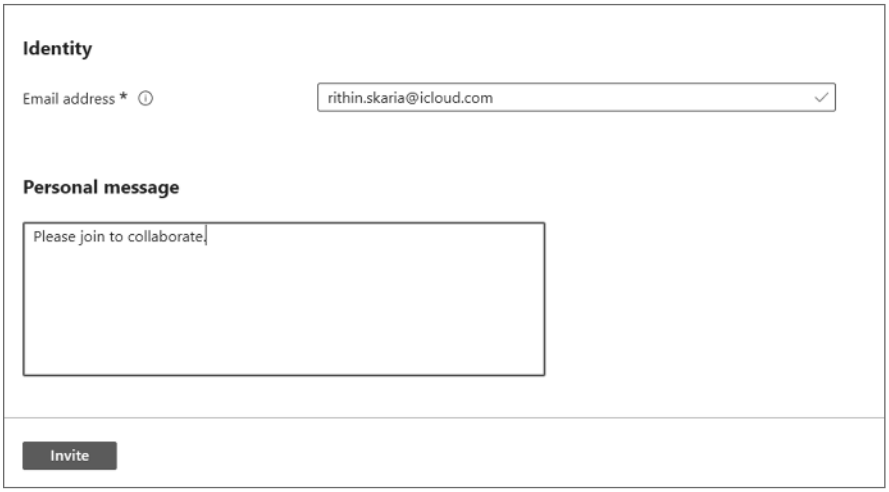


FIGURE 1.4 Invitation for Guest user

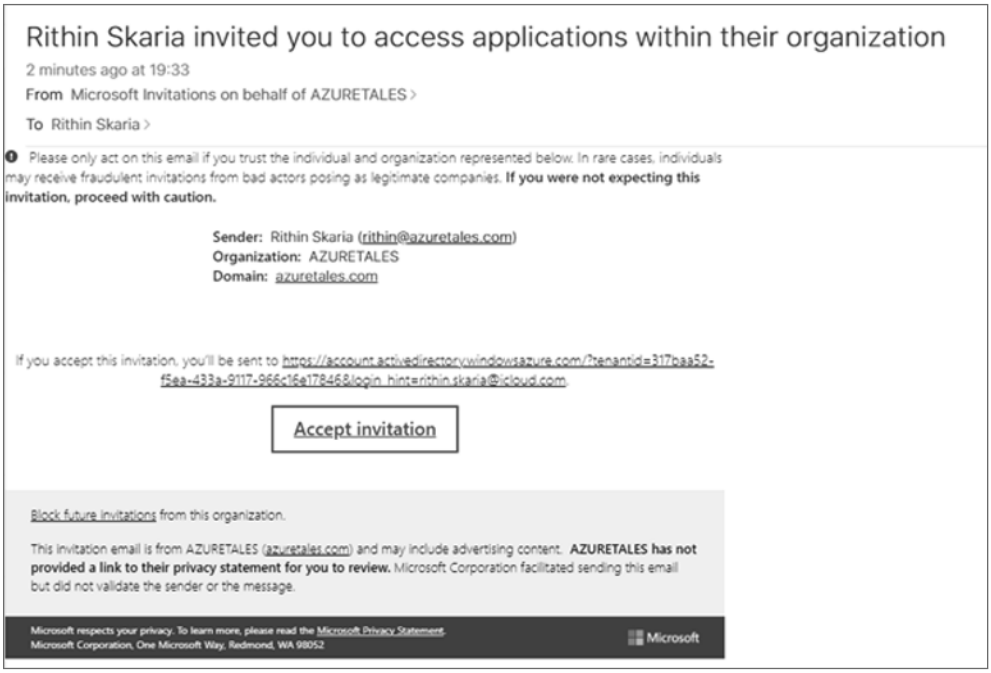
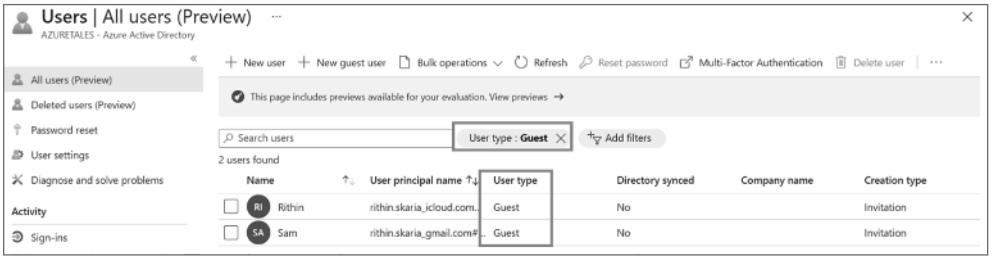


FIGURE 1.5 Filtering Guest users



So far, you have been working on user accounts and different operations that administrators can perform for managing users. Basic administrative tasks are limited not only to user management but can include group management as well. In the next section, we will talk about group accounts in Azure AD.

Group Accounts

When it comes to access management, applying permissions or roles to each user one by one is cumbersome, so to solve this complexity, we have groups in Azure AD. We can group users to create group accounts and then apply the permissions or roles to the group so that all members of the group get that access. Group accounts make access management easier. You can also synchronize groups from on-premises to the cloud, the same as with users.

Azure AD allows you to create two types of groups, security groups and Microsoft 365 Groups. Let's understand the differences between these types.

Security Groups Groups play an inevitable role in access management. Security groups can be used to control access to resources easily. For instance, you can create a security group called All HR and give access to all HR-related resources. As an administrator, the advantage here is you do not have to manage individual access; this can be controlled at the group level. Security groups require the Azure AD administrator to perform management actions.

Microsoft 365 Groups Microsoft 365 groups serve the same purpose as security groups; however, they provide additional capabilities such as access to a shared mailbox, shared calendar, SharePoint, and more. You can extend the collaboration and provide access to external users as well. Unlike security groups, both users and admins can use Microsoft 365 groups.

Another point to understand here is about membership to groups. You can add users as well as groups (nested groups) to a group as members. The rights can be accessed in three diverse ways, as follows:

Assigned This one is straightforward; this will let you add users (or groups) to the group as members. This type of addition is also known as *direct membership*.

Dynamic User Group memberships are controlled using member attributes; using them we can dynamically add or remove users from a group. For example, you can have a rule

like if the department of a user is HR, then that user should be added to the group All HR. Here Azure constantly reviews user attributes. If a new user is added with the department as HR, then Azure will add that user to the All HR group. Similarly, when someone leaves the department, Azure automatically removes the user from the group. This is especially useful for administrators, as they do not have to remove or add access whenever a new user is added or removed; but they must make sure that the attributes are added to the user correctly.

Dynamic Device This is applicable only in the case of security groups and is like the dynamic user concept. The primary difference is that instead of looking at the user attributes, here you are looking at the device attributes. You can register or join our devices to Azure AD, and based on the device attributes, the group membership can be controlled; we will cover AD Join later in this chapter.

Now that you are familiar with the membership types, let's go ahead and perform some hands-on tasks related to groups.

Viewing Groups

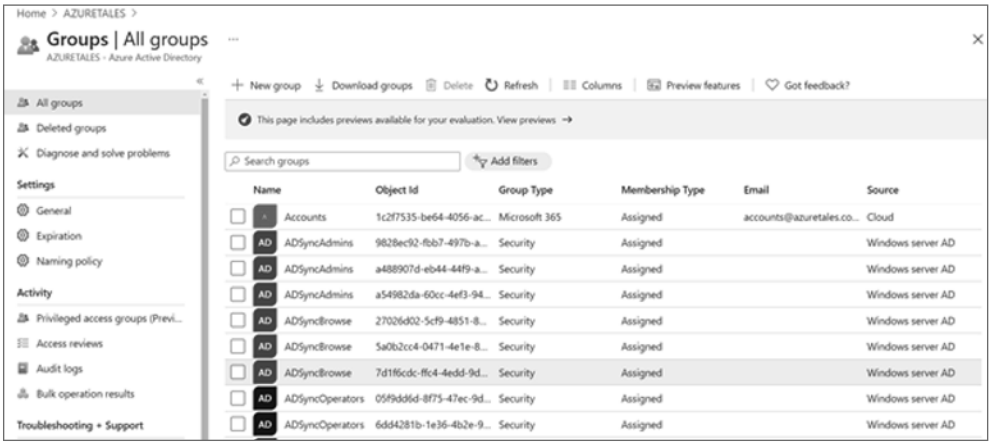
In Exercise 1.5, you will see how you can view groups in Azure AD.

If you are using a new setup, chances are you might not see any groups in your environment. This is fine; the purpose of the exercise is to make you understand how you can reach the Groups blade.

EXERCISE 1.5

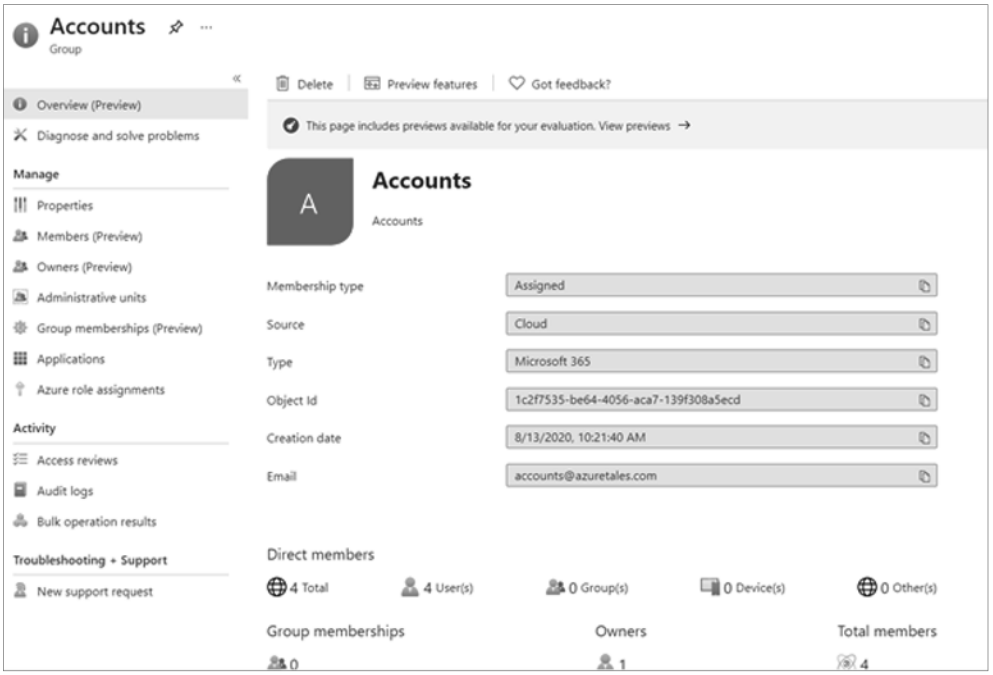
Viewing Groups in Azure AD

1. At this point, you should be familiar with the navigation in the Azure portal and how to reach the Azure Active Directory blade. Right below the Users option that you used earlier, you will be able to see Groups. Clicking Groups will take you to All Groups.



EXERCISE 1.5 *(continued)*

2. If you take a close look at the graphic, you can see that this list provides a lot of insights about the listed groups. For example, you can see the group type (Security Group or Microsoft 365 Group), membership type (Dynamic or Assigned), group email (shown only for Microsoft 365 as there will be a shared mailbox), and source (synchronized from Windows Server AD or the cloud). These details are extremely useful in managing the groups and in understanding the properties of a group.
3. Clicking any of the groups (you can skip this step if you do not have any groups in your environment) will give you a plethora of details about the group such as how many members are there, list of owners, group membership, device membership, etc.



Now that you know how to navigate to the Groups blade and find a group, let's move on and see how you can add a new group.

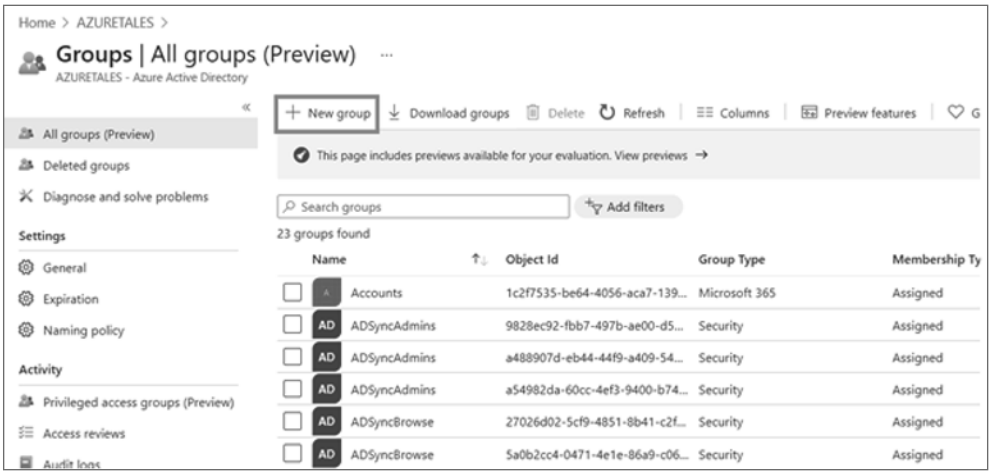
Adding Groups

In this section, we will cover how you can add a new security group and Microsoft 365 group. In addition, you will see how you can work with dynamic rules and direct membership to these groups. Especially in Exercise 1.6, you will create a security group called Avengers and add the users we created in Exercise 1.4 via direct membership.

EXERCISE 1.6

Adding Security Groups to Azure AD

1. Navigate to the Groups blade by following the steps mentioned in Exercise 1.5, and you will be able to see New Groups option.



2. Since our first task is to create a security group, you can see that we have selected the following options:

   a. **Group type:** Security (as we need to create a security group).

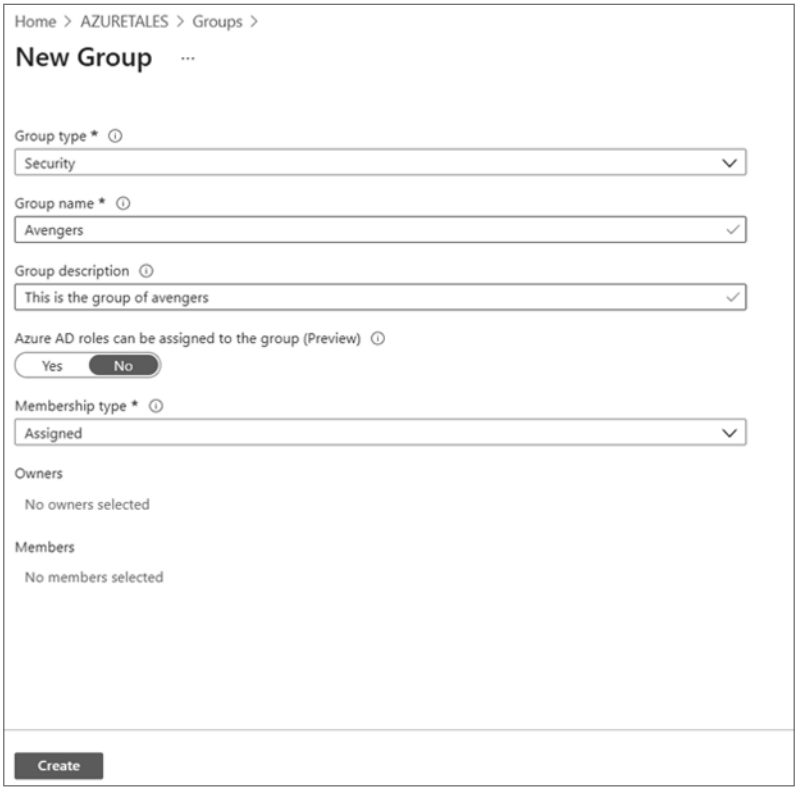
   b. **Group name:** Avengers (as we are going to add the Avengers users here).

   c. **Group description:** This field is optional; if you need to add a description about the group, feel free to add it.

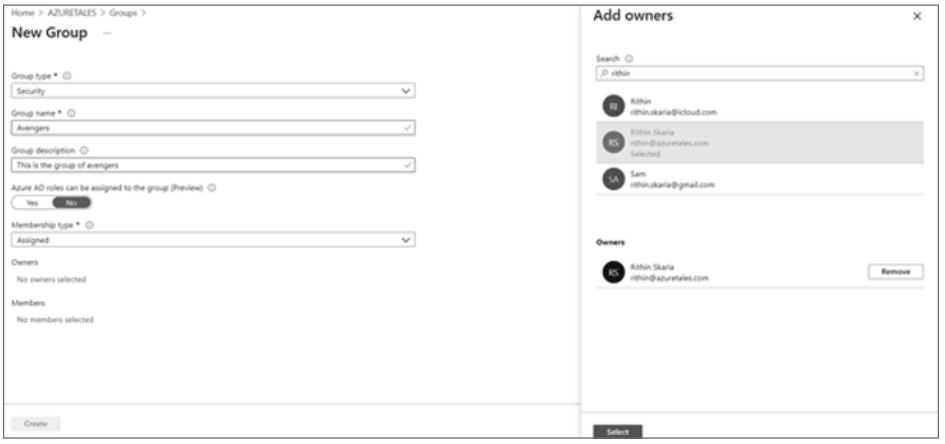
   d. **Azure AD roles can be assigned to this group:** Yes, this setting needs to be enabled if you plan to assign roles to this group from an access management perspective.

   e. **Membership type:** Assigned (as we are going to perform direct assignment).

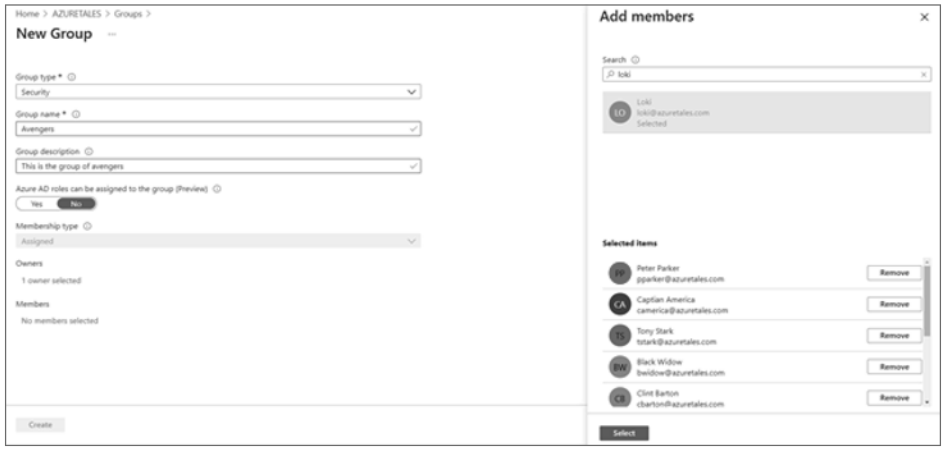
EXERCISE 1.6 *(continued)*



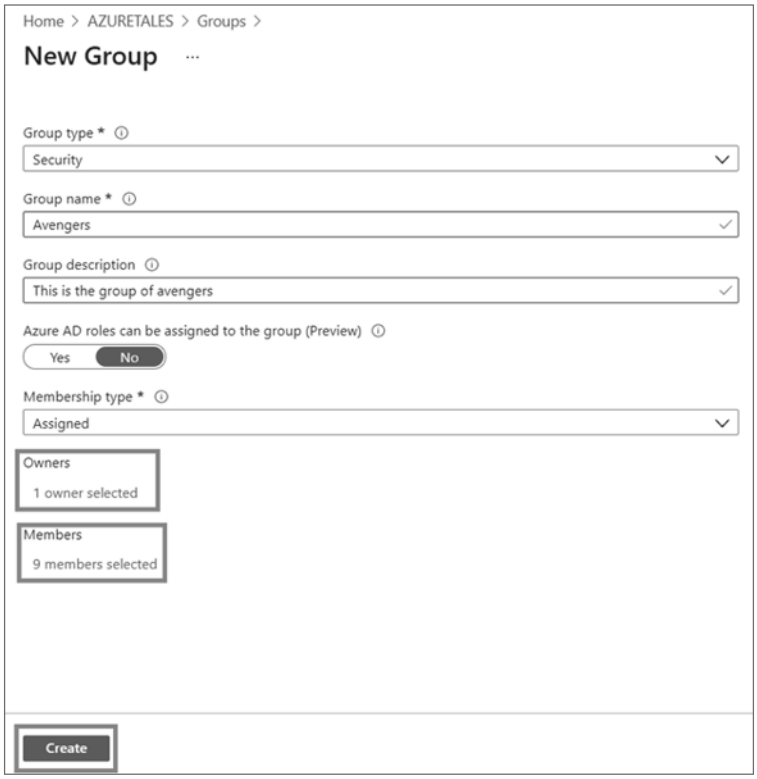
f. **Owners**: You can select the owners for the group. This set of users will manage the group such as adding or removing users. You can search users, and add once you are done, click Select.



g. **Members:** This is the set of users who will be part of the group; we will select all users that we need in the group. Once they are selected, click Select to add members to the group.



3. The new group window will now show the number of users you selected as owners and members. The next step is to click Create and create the group.



EXERCISE 1.6 *(continued)*

4. Navigate to All Groups and search for *Avengers*; you will be able to see the new group you created for our Avengers. Clicking the group name will reveal the properties of the group.

If you have followed these steps, then you have successfully completed the exercise to create a security group. Now let's focus on Microsoft 365 groups and dynamic users in Exercise 1.7.

Security groups can also be created with dynamic memberships supporting both dynamic users and devices; we are going to use Microsoft 365 and dynamic users for demonstration purposes only. You can apply the same logic with security groups and dynamic users, if needed.

EXERCISE 1.7

Adding Microsoft 365 Groups in Azure AD

In the previous exercise, we created security groups. It is time that we take the exercise to the next level by creating a Microsoft 365 group and adding users dynamically based on rules.

1. Before you create the group, you need to add some new users using the bulk create method. If you cannot recall the process, perform the steps in Exercise 1.4 to accomplish bulk creation. The following is a sample file used for creation and note that here we are using the usageLocation and department headers to add the usage location and department of the users. These attributes will later be used to build our dynamic rules. Upload the file and create the users before you create the group.

	A	B	C	D	H	I
1	version:v1.0					
2	Name [displayName] Required	User name [userPrincipalName] Require	Initial password [passwordProfile] Requ	Block sign in (Yes/No) [accountEnabled]	Department [department]	Usage location [usageLocation
3	Chris Ven	cven@azuretales.com	ComplexPwd#1441	No	HR	GB
4	John Peter	jpeter@azuretales.com	ComplexPwd#1442	No	Marketing	GB
5	Rick Case	rcase@azuretales.com	ComplexPwd#1443	No	HR	GB
6	Matt Philip	mphilip@azuretales.com	ComplexPwd#1444	No	Marketing	GB
7	David Ben	dben@azuretales.com	ComplexPwd#1445	No	HR	US
8	Jose Hender	jhender@azuretales.com	ComplexPwd#1446	No	HR	US
9	Sarah Phil	sphil@azuretales.com	ComplexPwd#1447	No	Finance	US
10	Eli Cin	ecin@azuretales.com	ComplexPwd#1448	No	Finance	US
11	Sinu Sam	ssam@azuretales.com	ComplexPwd#1449	No	Marketing	IN
12						
13						

2. As you performed in Exercise 1.6, you need to reach the New Group window and add properties as follows:

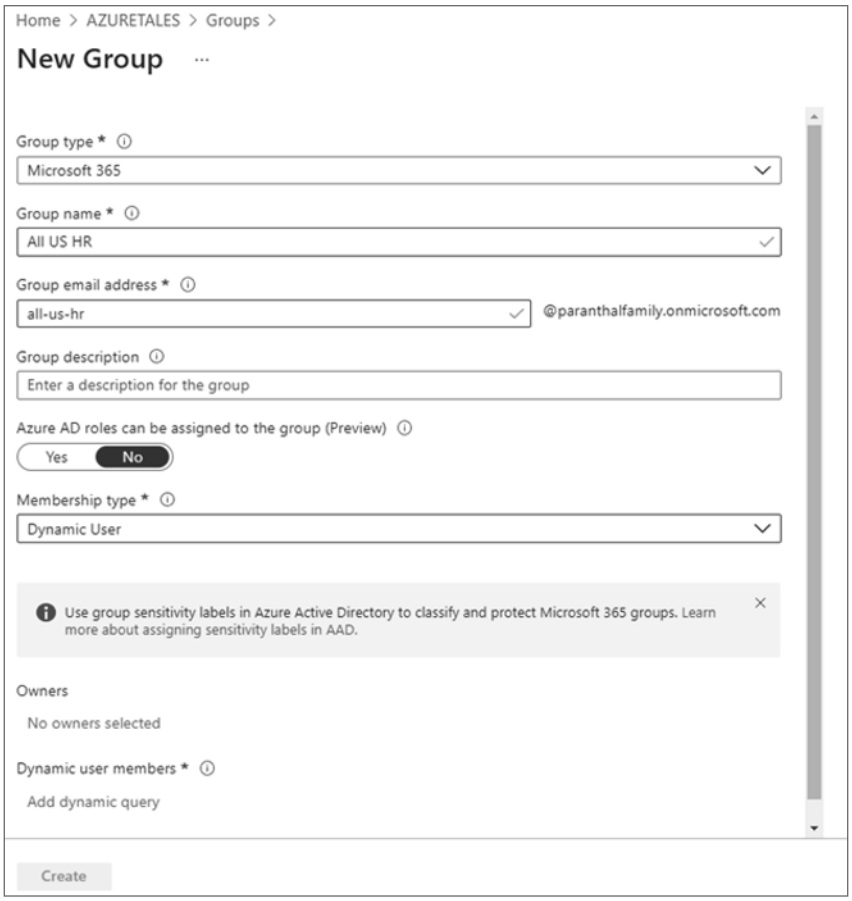
   a. **Group type:** Microsoft 365 (as we need to create a Microsoft 365 group).

   b. **Group name:** All HR (a group for all users whose department is HR).

c. **Group email address:** This is a required field as all Microsoft 365 groups should have an email address. You can add something like "all-hr" and the domain will be auto populated based on your tenant domain.

d. **Group description:** This field is optional; if you need to add a description about the group, feel free to add it.

e. **Membership type:** Dynamic User (as we are going to use dynamic queries to add users).



f. Owners can be selected in the same fashion as we did in the case of security groups (refer to Exercise 1.6 step 2.f).

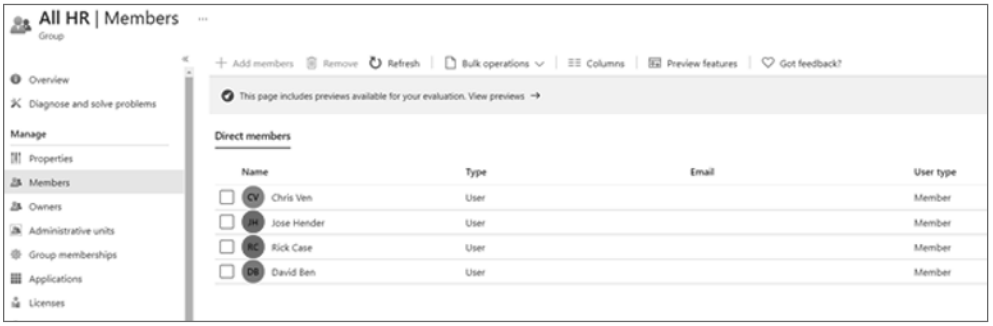
g. The next option is to define the dynamic query for the user. If you take a closer look at the previous graphic, at the bottom you can see there is an option to add a dynamic query. Click that, and you will be taken to the dynamic membership rules editor.

EXERCISE 1.7 *(continued)*

h. Based on the properties you are selecting, corresponding rules are created. In our example, we are adding the property "department" EQUALS "HR." We can add more expressions by clicking Add Expression.

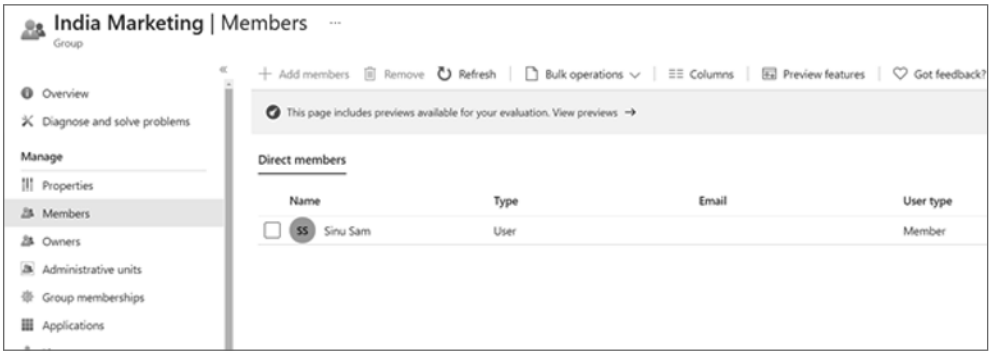
i. Azure Portal will automatically generate the rule syntax based on our selection. The rule syntax for what we selected here is user.department -eq "HR". Once you have verified the rules, click Save to save the rule.

3. Wait for a couple of minutes, and the members of the group will be automatically added based on the rule you configured.



4. Let's try to create another group called India Marketing where we will set up the rule using an additional expression. The final syntax will be (user.department -eq "Marketing") and (user.usageLocation -eq "IN"), as shown here.

5. You will see that the members matching the rule are added to the Members blade.



If you completed both the exercises, by now you know how to create security groups and Microsoft 365 groups. Now let's see how to delete or modify the existing groups.

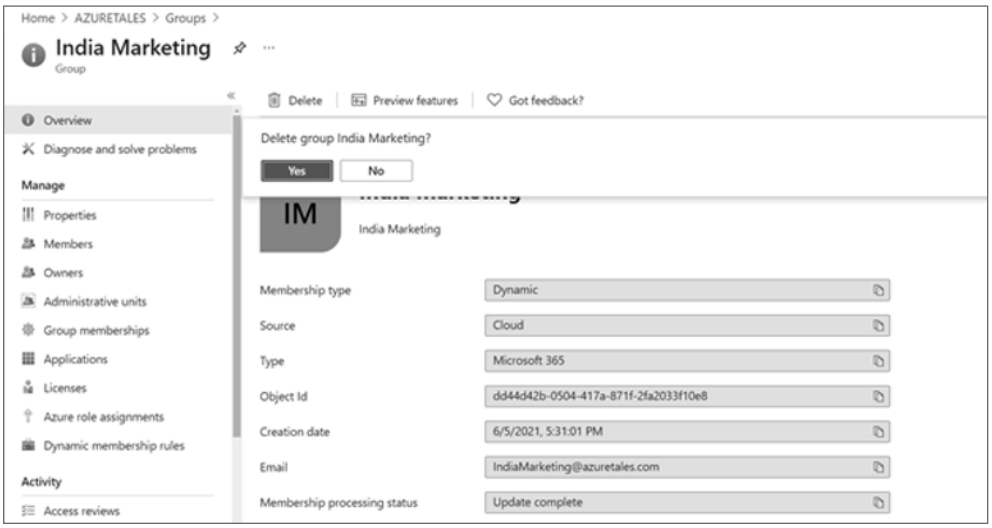
Deleting Groups

Deleting groups is a straightforward process; however, you need to perform this action with caution because deleting a group in production may cause serious repercussions on access management. Some scenarios where you will need to delete a group include the following:

- You selected the wrong group type while creating the group. This selection cannot be modified after creation; the only option is to delete the group and re-create the group with the right type.
- You have a duplicate group.
- You no longer need the group in your environment.

If you want to delete a group, you can navigate to Azure Active Directory ➢ Groups ➢ All Groups and open the group you want to delete. Clicking the Delete button as shown in Figure 1.6 will delete the group.

FIGURE 1.6 Deleting group



Updating details in a group is no different than updating the user properties. You can add or remove users any time from security groups or Microsoft 365 groups with an assigned membership type. However, in dynamic membership groups, you cannot manually add or remove users. The member management is completely managed by dynamic rules that you create. Azure gives you the option to modify the dynamic rules of your existing group without the need to re-create the group.

Now that are familiar with the user and group accounts in Azure AD, we will talk about the roles in Azure AD.

Azure AD Roles

Azure AD roles are used to manage the permissions that can be assigned to users. You can assign roles to users so they can perform certain actions such as resetting user passwords, assigning, or removing licenses, adding, or removing users, etc.

More than 50+ built-in roles are available in Azure AD so you can follow the principle of least privilege and assign users the permission that they need to complete the tasks given to them. Azure AD roles make sure that the users are not over-privileged or under-privileged with the permissions given to them. For example, if you want to give a user the permission to create/manage groups, create/manage groups settings such as naming and expiration policies, and view groups activity and audit reports, then Groups Administrator is the right role

that can be assigned to the user.

Here is the complete list of roles available in Azure AD:

`https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference`

You can assign roles to the users from the Users ➢ Assigned Roles blade. At the time of authoring this book, assigning roles to groups is in preview. If you would like to know more about this preview feature, refer to this document:

`https://docs.microsoft.com/en-us/azure/active-directory/roles/groups-concept`

We will cover more about Azure AD roles when we discuss role-based access control in Chapter 2, "Compliance and Cloud Governance."

We talked about managing users and groups and assigning roles to them. In an enterprise environment, not only users but devices used by users need to be managed and monitored. Azure AD Join helps you to make sure that the devices used by the users follow the organizational standards. Let's discuss Azure AD Join.

Azure AD Join

Single sign-on is one of the features offered by Azure AD. You can use SSO on devices, apps, and services from anywhere in the world. Joining devices to Azure AD assures the corporate devices are protected and that they follow the compliance standards set by the organization. Users can bring their own devices and join them to Azure AD, and administrators can make sure that these devices also follow the standards of your organization. Now, we will look at the benefits of Azure AD Join.

Benefits

Azure AD Join has the following benefits:

Single Sign-On This is the primary feature of AD Join; you can sign-in to any of your applications and services without a username and password prompt. The best part is it is not necessary to connect to the domain network to use SSO.

Enterprise Client Roaming The settings are synchronized across devices that are joined to Azure AD.

Microsoft Store for Business Joining your device and signing-in to the store with work or school accounts gives you a customized catalog of applications that are shared by your organization.

Windows Hello This provides you with biometric authentication using facial recognition or fingerprints to access corporate resources and sign-in to devices. The devices should have hardware that supports Windows Hello to use this feature.

Block Access Administrators can enforce policies and devices that do not meet the requirements can be easily blocked.

Let's see what connection options are offered by Azure AD Join.

Connection Options

You can connect your devices to Azure AD using the following options:

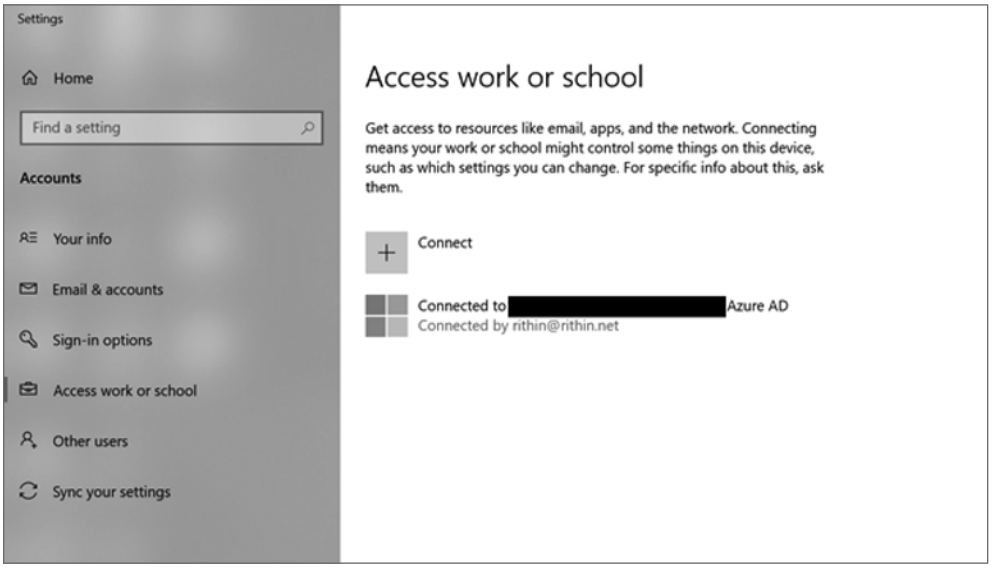
Register to Azure AD Registration creates an identity for the device, and this identity can be used for authentication. Whenever a user signs in, the identity of the device can be used for authentication. Administrators have the right to enable or disable this identity.

Join to Azure AD Joining to Azure AD provides the same features as registration and additionally changes the local state of the device. With a change of local state, users can sign in to their device using their work or school account. Joining is more like an extension to the registration process.

Combining the registration process with Microsoft Intune (it is a mobile device management [MDM] solution) will help you create conditional policies using the device attribute. Using this combo, you can block devices that do not follow the organizational compliance standards. For example, you could block all devices that are using Windows XP or Windows 7 and make Windows 10 the prerequisite for accessing corporate resources.

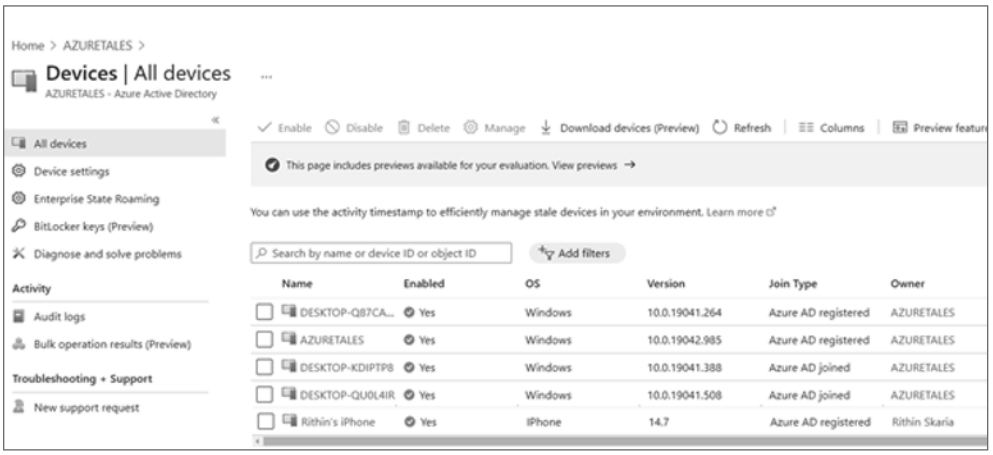
You could join your device to Azure AD by going to your Windows 10 Settings ➢ Accounts ➢ Access To Work Or School. Signing in with your work or school account will connect your device to the Azure AD domain, and you can sign in to corporate resources using SSO. Figure 1.7 shows how a connected device looks.

FIGURE 1.7 Connecting a device to Azure AD



All the devices that are connected to Azure AD can be explored from the Azure Active Directory ➢ Devices blade. This blade will show OS information, OS version, join type, and owner of the devices that are joined (refer to Figure 1.8).

FIGURE 1.8 Listing all devices connected to Azure AD



Now we will talk about a lifesaver for administrators: self-service password reset. Using self-serve options reduces the incoming requests to the IT help desk so administrators can utilize their time for more productive work.

Self-Service Password Reset

If you have worked at an IT help desk, you know most of the calls are for user password reset. Self-service password reset (SSPR) allows users to reset their passwords using a set of authentication methods set by the cloud administrators. Self-service password reset is always enabled to administrators to avoid lock-out scenarios. Admins need to use two authentication methods for password reset.

Enabling SSPR

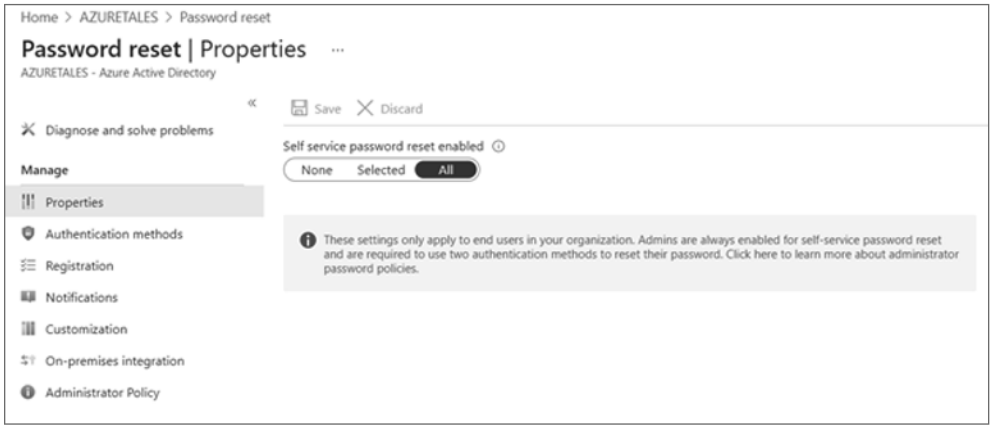
Cloud administrators need to enable SSPR options for users or groups as this option is not enabled by default. To enable this feature, you need to have the Global Administrator role in the tenant.

SSPR can be enabled from Azure Portal ➢ Azure Active Directory ➢ Password Reset. SSPR provides three options (refer Figure 1.9).

- **None**: SSPR is not enabled.
- **Selected**: SSPR is enabled for selected groups.
- **All**: SSPR is enabled for all users in the tenant.

Once SSPR is enabled, users need to register for SSPR. Azure will automatically redirect users to the registration page on first sign-in after SSPR is enabled. Users can always navigate to `https://aka.ms/ssprsetup` to set up their authentication methods or to change them in the future. For example, you might have registered with one phone number when you enrolled for SSPR, but you changed your phone number. In this case, you can change it by going to the SSPR setup page.

FIGURE 1.9 Enabling SSPR



Registered users can always reset the password from the sign-in page by clicking "Can't access your account?" as shown in the Figure 1.10.

It is not necessary that you navigate to Azure Portal to click "Can't access your account?"; you can navigate to any sign-in page that uses Azure AD login like Office 365, Dynamic 365, SharePoint, etc.

Users can also navigate to the reset page directly by going to `https://aka.ms/sspr`. This is an alias for the following:

`https://passwordreset.microsoftonline.com`

Now that you are familiar with SSPR setup, let's see what authentication methods are available for the users and how administrators can control these methods.

Authentication Methods

The administrator can choose the number of authentication methods required to reset the password and the number of methods available for users.

FIGURE 1.10 Initiating password reset

For a successful reset operation, you require at least one authentication method. Nevertheless, it is always better to have a secondary method. For example, if you set up SSPR with an email method, and if the user has no email access, then the user will not be able to reset the password. Here, it is better to have a second option like a mobile phone so that the user can receive the code as a text message and complete the authentication.

Methods available include the following:

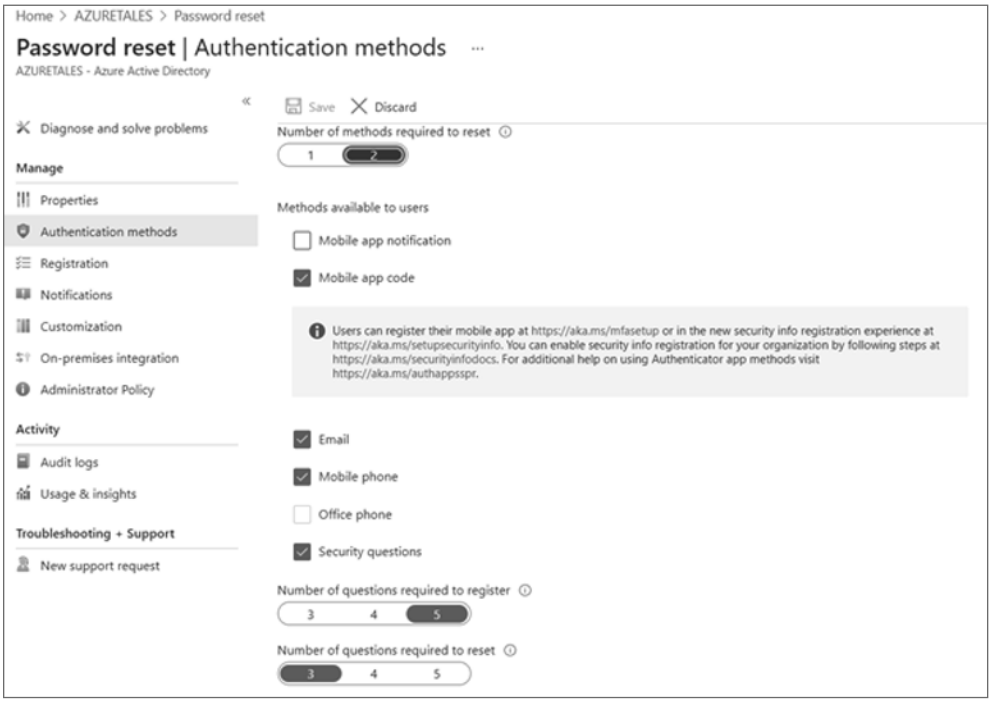
- Email notification
- Text message to mobile phone
- Text message to office phone
- Mobile app notification
- Mobile app code
- Security questions

In the case of security questions, the administrator can decide how many questions need to be registered and how many of them need to be answered to reset the password. Nonetheless, security questions are considered less secure as the answers to these questions can

be guessed if the intruder or hacker knows the user personally. Attackers can also collect answers for these questions via social engineering.

Authentication methods can be configured from Azure Portal ➢ Azure Active Directory ➢ Password Reset ➢ Authentication Methods (refer to Figure 1.11).

FIGURE 1.11 Configuring SSPR authentication methods



So far, we concentrated on a single-tenant environment; in real-world scenarios there will be different tenants, and admins are responsible for the management of these tenants. Let's see why we need multiple directories and what benefits it provides.

Managing Multiple Directories

Each tenant represents an organization, and it is a fully independent resource. Every tenant that you create is logically separated from other tenants that you manage in a multitenant environment. Even if you are the common administrator for all these tenants, there will not be any parent-child relationship between these tenants or directories. Resource independence, administrative independence, and synchronization independence are there between the tenants.

Resource independence is when you create or delete a resource in one tenant; this action will have no impact on any other resource in another tenant. However, there is a small exception that we discussed in the case of cloud identities from external AD. By default, Azure AD doesn't delete Guest users when they are deleted from their home tenant; however, we can set this up manually.

Administrative independence is when a non-admin user (say the user's name is John) of tenant A creates a new tenant, say tenant B.

- John will be the Global Administrator of the tenant B as he created the new tenant. The user will be added as a user from external AD. Here it says external AD, because John is not from tenant B but from tenant A.
- Administrators of tenant A have no control over tenant B. If the users of tenant A need to access or manage tenant B, then John must invite these users to tenant B and give the necessary role. One thing to note here is that if the admins of tenant A takeover John's account, they can access tenant B.
- Adding or removing an admin role in one tenant will not affect the role of the user in the other tenant. Here we're not removing the user; we are adding or removing the Azure AD roles, which will have no impact on the other tenant, and all roles the user has in the other tenant will be retained.

When it comes to synchronization independence, you can set up independent synchronization on each Azure AD.

With that, we have covered all the topics that are within the scope of the exam.

Summary

In this chapter, we talked about the identity and access management solution in Azure: Azure Active Directory. We started the chapter looking at the benefits of Azure AD, and then we examined how Azure AD is different from the traditional Windows Server Active Directory deployment.

As we progressed, we spoke about Azure AD licensing and how administrators can set up custom domains. After that, we learned about user accounts and group accounts. This is a major element of this chapter; understanding user and group management is crucial for cloud administrators. If you are not confident with identity and access management, there can be a chance of security flaws. Security issues are not something welcomed in an organization as they can cause damage to the reputation of the organization, especially when you are dealing with customer data. Along with the impact on the reputation, this can also lead to revenue loss. As an administrator, you should excel in the identity and access management field.

Then we spoke about Azure AD roles and how administrators should put emphasis on the principle of least privilege. Several other key ideas were reviewed including AD Join and SSPR. You learned about the advantages of incorporating these features in your environment.

Toward the end of the chapter, we covered multitenant environments and the independence they provide in terms of administration, resources, and synchronization.

Like with security, implementing governance and compliance is crucial in setting up the environment. In the next chapter, we will cover governance and compliance.

Exam Essentials

Understand Active Directory. Understand the purpose, benefits, and concepts related to Azure Active Directory. Along with that, recognize the key differences between different editions of Azure AD and the relevance of custom domains.

Know user and group management. Understand the different types of users who can be created in Azure AD. Know how these users can be viewed, updated, or deleted when required using portal and via bulk operations. Also, know how these users can be added to groups. In group management, focus on security groups and Microsoft 365 groups with dynamic users and assigned users.

Understand Azure AD Roles. Understand the relevance of Azure AD roles and how these are used to control the access and permissions of users and groups in Azure AD.

Know Azure AD Join. Recognize the differences between Azure AD Join and Azure AD register.

Understand SSPR. You need to understand how SSPR is configured for users and how the authentication methods are configured for users.

Understand a multitenant environment. Understand the independence provided by tenants while you are managing multiple directories.

Review Questions

1. Your users want to enable single sign-on to devices, apps, and services across all devices that are compliant with your organizational standards. Per your company, all devices should be protected, and users can use only their work or school account. Also, as an administrator, you should be able to disable their device in the case of a compromise. What should you do? (Select one.)
   - **A.** Join the device to Windows Active Directory
   - **B.** Install BitLocker and enable High Security Protocol
   - **C.** Register the device to Azure AD
   - **D.** Join the device to Azure AD
2. You are a user administrator, and one of the global administrators reached out to you to reset their password. Which of the two following ways can be used to reset the password of the global administrator?
   - **A.** User administrator can elevate access and reset password
   - **B.** Redirect the user to self-service options
   - **C.** Reset the password from the profile of the user and share via secured channel
   - **D.** Ask user to contact another global administrator
3. You are setting up self-service password reset for your users. Which of the following is not a validation method?
   - **A.** Fax to office number
   - **B.** A text or code to the office phone
   - **C.** Security questions
   - **D.** Email notification
4. Your organization would like to collaborate with a freelancer for project work. The project manager has sent the agreement to the freelancer, and they accepted it. As an administrator, you need to add this Microsoft account to the tenant for granting access. If you add this user to the tenant, which type of user will be created?
   - **A.** Cloud identity
   - **B.** Guest user
   - **C.** Directory synchronized identity
   - **D.** User-assigned managed identity
5. Which of the following facts about Azure AD is not correct?
   - **A.** Azure AD uses HTTP/HTTPS communication.
   - **B.** Azure AD has a flat hierarchy.
   - **C.** Azure AD can be queried through LDAP.
   - **D.** Federation Services is supported by Azure AD.

6. You are the Global Administrator of the tenant, and one of the users in the tenant who has a Compliance Administrator role creates a new tenant. What would be the role of the user who created the tenant in the new tenant?
   - **A.** Compliance Administrator
   - **B.** User role (no role will be assigned)
   - **C.** Cross Tenant Administrator
   - **D.** Global Administrator

7. You have an on-premises application, and you would like to give access to the application for cloud identities in your Azure AD. Your security team said that they cannot expose the application to the public Internet. How can you enable access in this case?
   - **A.** Use a load balancer and send to on-premises
   - **B.** Leverage Azure AD Application Proxy
   - **C.** Use conditional access
   - **D.** Enable PIM

8. You created a new tenant with the initial domain name `microteamengineering.onmicrosoft.com`. Your company already has a domain called `MTE.com`. When you create users, the usernames have the initial domain name. You decide to use the custom domain feature of Azure AD and add your domain. The domain stays unverified, and you cannot use the domain while creating users. What should have been done to use the domain in Azure AD?
   - **A.** Purchase a domain certificate before using the domain
   - **B.** Enroll in Intune services and register the domain
   - **C.** Work with your domain registrar and enable Azure AD integration
   - **D.** Add TXT/MX records given in Azure AD for proving the ownership of domain

9. You are the Global Administrator and trying to use the identity governance feature in Azure AD; however, the feature is grayed out. You are using a Premium P1 license. What could be the reason for this?
   - **A.** Purchase Premium P2 license
   - **B.** Contact Microsoft Support to enable this feature
   - **C.** Only Identity Governance Administrators can use this feature
   - **D.** Enroll your device to the identity governance program

10. You are editing the details of a user in your Azure AD. Which of the following fields cannot be changed?
    - **A.** Manager
    - **B.** Object ID
    - **C.** User Principal Name
    - **D.** Name

11. Your organization shared a list of 35 users to be deleted, and you want to delete users easily and in a trackable fashion. Which feature should you use?

A. Select the users and use the Delete Users option in the Users blade

B. Write an LDAP query and execute a bulk delete

C. Manually delete each user

D. Leverage a bulk delete operation

12. Deleted users from Azure AD can restored within _____ days.

A. 10

B. 90

C. 30

D. 180

13. You need to group devices in your environment based on device attributes. Which type of group and assignment should you choose?

A. Security group with dynamic devices

B. Microsoft 365 group with dynamic devices

C. Microsoft Device Management service

D. GPO in on-premises AD

14. You have the following users in your environment:

User 1: Marketing department and location is US

User 2: HR department and location is US

User 3: Marketing department and location is UK

User 4: HR department and location is India

You created a dynamic rule using this syntax: `(user.department -eq "HR" or user.usageLocation -eq "GB") and (user.usageLocation -ne "US")`. Which users will be part of the group?

A. User 1, User 2, User 3, and User 4

B. User 1, User 2, and User 4

C. User 2 and User 4

D. User 3 and User 4

15. You are planning to host a SharePoint site to share content only within the users of your environment. You need to set up a group for the admins to have a shared calendar and mailbox to collaborate. Which type of group should they go for?

A. Security group with mailbox enabled

B. Microsoft 365 group

C. Microsoft Exchange group

D. SharePoint mailbox group

16. You are the Office 365 administrator of your organization, and you created Microsoft 365 groups with dynamic users from the Office 365 Admin panel. You have been asked by your Azure AD Global Administrator to synchronize these groups with Azure AD for management purposes. How can you achieve this?
    - **A.** Use the Azure AD Connect tool and synchronize users and groups with Azure AD.
    - **B.** Use Office 365 connector for Azure AD and sync users.
    - **C.** All users and groups in Office 365 are automatically synchronized with Azure AD.
    - **D.** You cannot synchronize users; you need to re-create them on Azure AD.

17. After joining devices in your organization to Azure AD, you would like to enable facial recognition and biometric authentication for Windows 10 devices with supported hardware. Which feature of Windows 10 should be used for this?
    - **A.** Intune
    - **B.** Windows Hello for Business
    - **C.** Authenticator app for Windows 10
    - **D.** The Azure portal

18. You are assigning Azure AD roles. Which role will allow the user to manage all the groups in your tenant and be able to assign other administrator roles?
    - **A.** Global Administrator
    - **B.** Password Administrator
    - **C.** Security Administrator
    - **D.** Compliance Administrator

19. Identify which of the following statements about Azure AD is not correct.
    - **A.** Azure AD uses HTTP and HTTPS communications.
    - **B.** Azure AD uses Kerberos authentication.
    - **C.** There are no organizational units (OUs) or Group Policy objects (GPOs) in Azure AD.
    - **D.** Azure AD includes Federation Services.

20. You are Azure AD administrator, and your developers are asking you to block users from a certain country, and also if the users are from the United States, they require MFA before accessing the application. Which feature of Azure AD should you use to accomplish this?
    - **A.** Identity protection
    - **B.** Application Proxy secure endpoint
    - **C.** Privileged identity management
    - **D.** Conditional access