5

Section 5: Managing Identities

In this section, you will learn how to manage identities in Azure.

The following chapters will be covered in this section:

- `Chapter 14`, *Managing Azure Active Directory*
- `Chapter 15`, *Implementing and Managing Hybrid Identities*
- `Chapter 16`, *Implementing Multi-Factor Authentication*

14
Managing Azure Active Directory

In the previous chapter, we covered how to configure an internal and external load balancer using Azure Load Balancer. The main focus was on the features and capabilities of Azure Load Balancer, and also on how to create health probes and configure load balancing rules.

This chapter introduces the final objective of this book: the *Managing Identities* objective. In this chapter, we are going to cover how to create and manage users and groups in **Azure Active Directory** (**Azure AD**). You will learn how to manage this from the Azure portal and how to perform bulk updates inside your Azure AD tenant. You will learn how to configure self-service password reset for your users to reduce user management overhead. We are also going to cover Azure AD Join and how you can manage your devices that are registered or joined in Azure AD. To finish this chapter, we will add a custom domain to Azure AD.

The following topics will be covered in this chapter:

- Azure AD
- Creating and managing users and groups
- Adding and managing guest accounts
- Performing bulk user updates
- Configuring self-service password reset
- Azure AD Join
- Managing device settings
- Adding custom domains

Azure AD

Azure AD offers a directory and identity management solution from the cloud. It offers traditional username and password identity management, and roles and permissions management. On top of that, it offers more enterprise-grade solutions, such as **Multi-Factor Authentication** (**MFA**) and application monitoring, solution monitoring, and alerting. Azure AD can easily be integrated with your on-premises Active Directory to create a hybrid infrastructure.

Azure AD offers the following pricing plans:

- **Free**: This offers the most basic features, such as support for up to 500,000 objects, **single sign-on** (**SSO**), Azure B2B for external users, support for Azure AD Connect synchronization, self-service password change, groups, and standard security reports.
- **Basic**: This offers no object limit, a SLA of 99.9%, self-service password reset, company branding features, and support for the Application Proxy.
- **Premium P1**: This offers advanced reporting, MFA, conditional access, MDM auto-enrollment, cloud app discovery, and Azure AD Connect Health.
- **Premium P2**: This offers identity protection and Privileged Identity Management.

> For a detailed overview of the different pricing plans and all the features that are offered for each plan, you can refer to the following pricing page: `https://azure.microsoft.com/en-us/pricing/details/active-directory/`.
>
> Note that Azure AD Premium is part of the Enterprise Mobility and Security Suite.

In the next section, we are going to create and manage users and groups inside an Azure AD tenant.

Creating and managing users and groups

In this demonstration, we are going to create and manage users and groups in the Azure portal. You can also use PowerShell and CLI to create users.

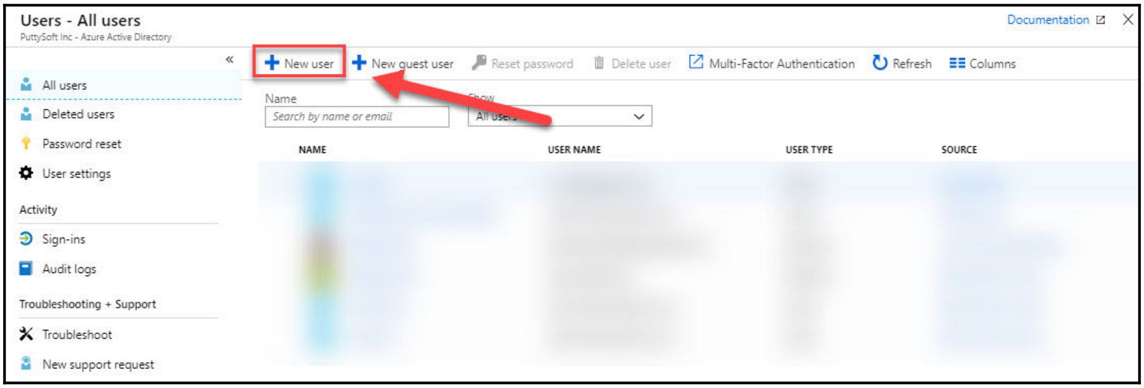
We are not going to create an Azure AD tenant in this demonstration. I assume that you already have one. If you need to create an Azure AD tenant, you can refer to the following tutorial: `https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-create-new-tenant`.

You can also create multiple Azure AD tenants in one subscription. These directories can be used for development and test purposes, for instance.

Creating users in Azure AD

We will begin by creating a couple of users in our Azure AD tenant from the Azure portal. Therefore, you have to take the following steps:

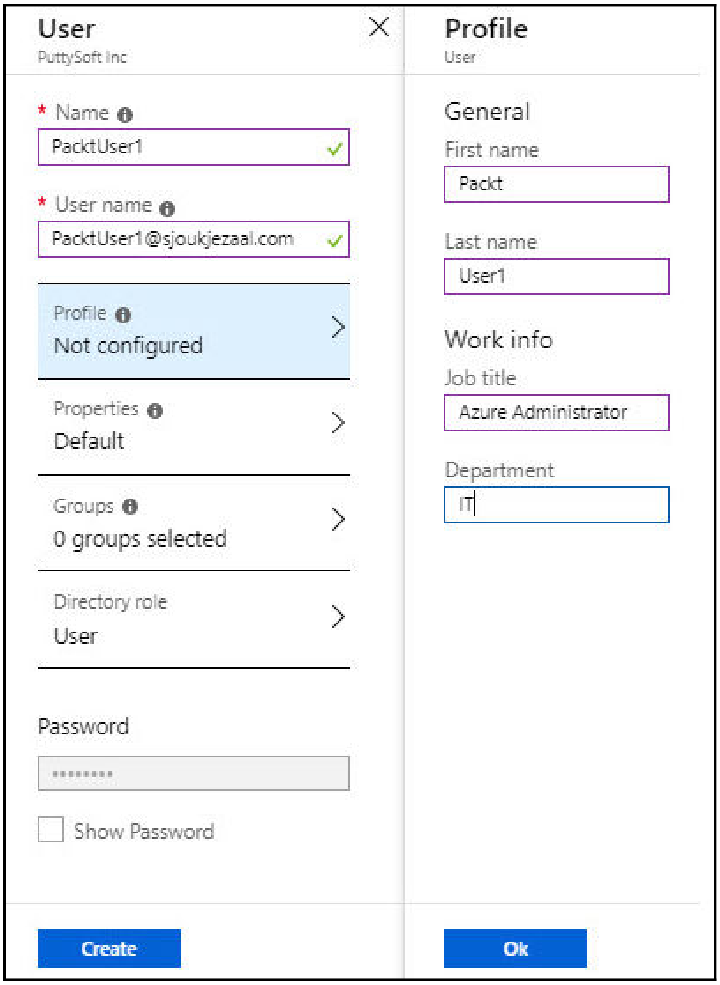
1. Navigate to the Azure portal by opening `https://portal.azure.com`.
2. In the left menu, select **Azure Active Directory**.
3. In the **Overview** blade of Azure AD, in the left menu, select **Users** | **All users**. Select **+ New user** from the top menu, as follows:



Creating a new user

4. We are going to create three users. Add the following values, which are shown in the following screenshot:
   - **Name**: `PacktUser1`.
   - **Username**: The username is the identifier that the user enters to sign in to Azure AD. Use your domain name that is configured and add this to the end of the username. In my case, this is `PacktUser1@sjoukjezaal.com`.

- **Profile**: Here, you can create a new profile for your user. Add the **First name**, **Last name**, **Job title**, and **Department**. After that, click **OK**, as follows:



User
PuttySoft Inc

* Name: PacktUser1 ✓

* User name: PacktUser1@sjoukjezaal.com ✓

Profile
Not configured

Properties
Default

Groups
0 groups selected

Directory role
User

Password: ••••••••

□ Show Password

Create

Profile
User

General

First name: Packt

Last name: User1

Work info

Job title: Azure Administrator

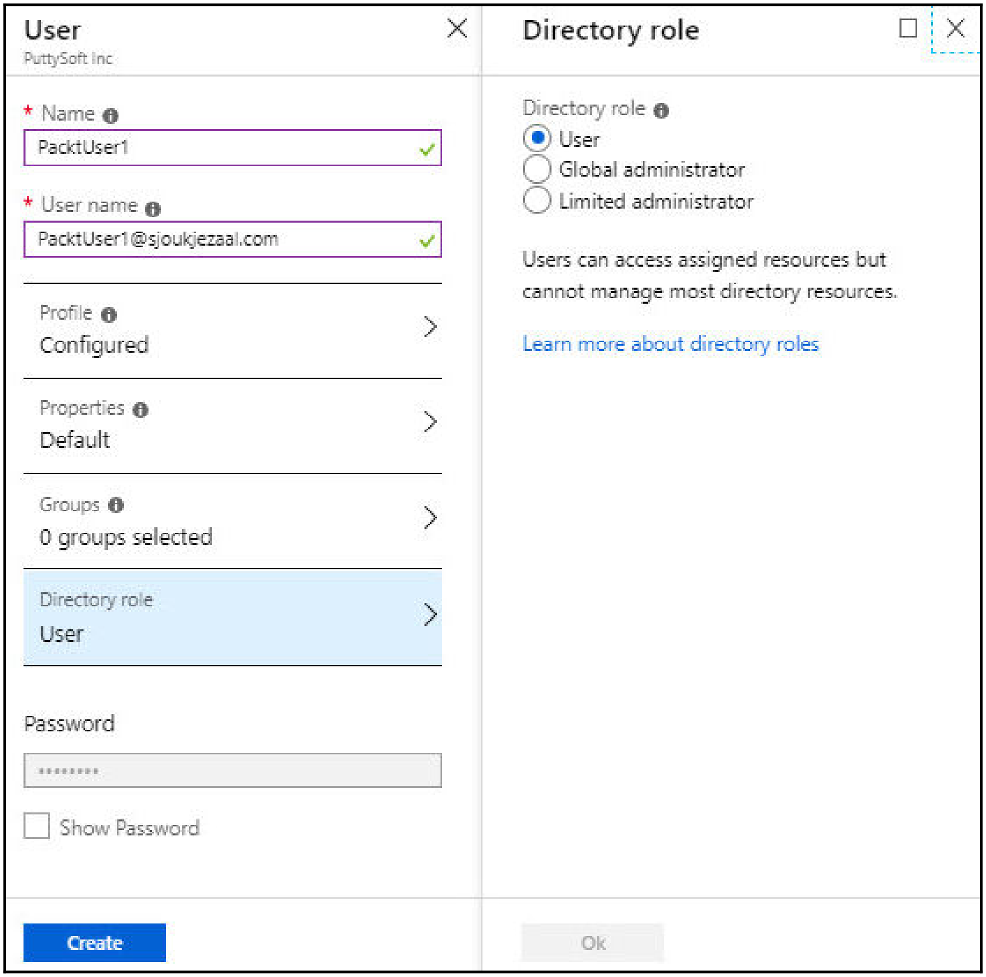
Department: IT

Ok

Creating a profile for your user

- **Group**: You can also add your user to a group from here. We are going to do this in the following demonstration, so you can skip this part for now.

- **Directory role**: Here, you can assign the user to the **User**, **Global administrator**, or **Limited administrator** role. Select **User**, as follows:



User
PuttySoft Inc

* Name
PacktUser1 ✓

* User name
PacktUser1@sjoukjezaal.com ✓

Profile
Configured

Properties
Default

Groups
0 groups selected

Directory role
User

Password
****

□ Show Password

Create

Directory role

Directory role
● User
○ Global administrator
○ Limited administrator

Users can access assigned resources but cannot manage most directory resources.

Learn more about directory roles

Ok

Selecting directory role

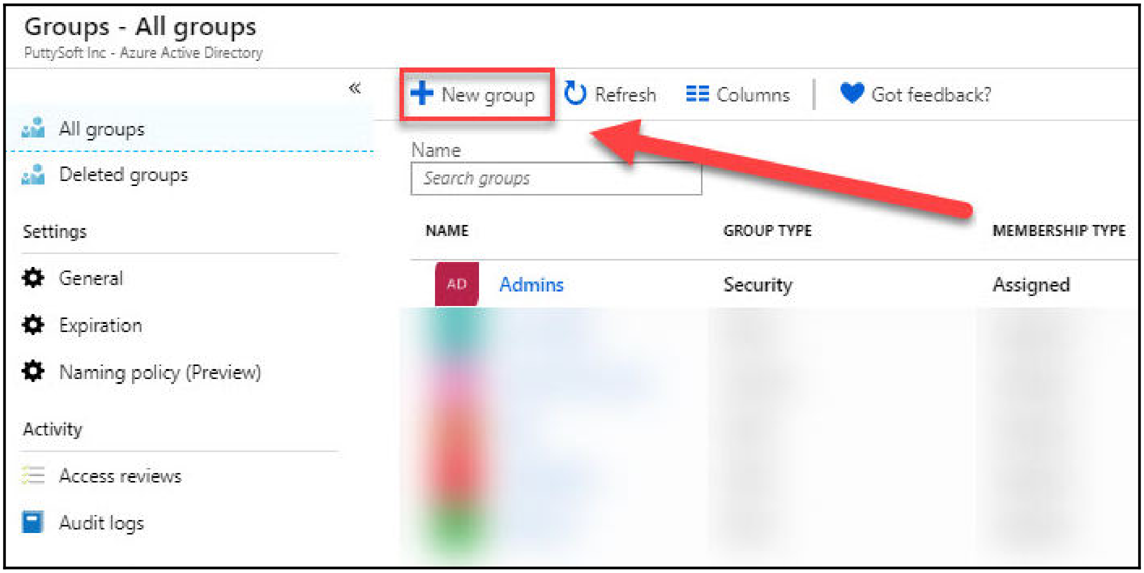
5. Click **Create**.
6. Repeat these steps and create `PackUser2` and `PacktUser3`.

Now that we have created a couple of users in our Azure AD tenant, we can add them to a group in Azure AD.

Creating groups in Azure AD

To create and manage groups from the Azure AD tenant in the Azure portal, you have to perform the following steps:

1. Navigate to the Azure portal by opening `https://portal.azure.com`.
2. In the left menu, select **Azure Active Directory.**
3. In the **Overview** blade of Azure AD, in the left menu, select **Groups** | **All groups**. Select **+ New group** from the top menu, as follows:



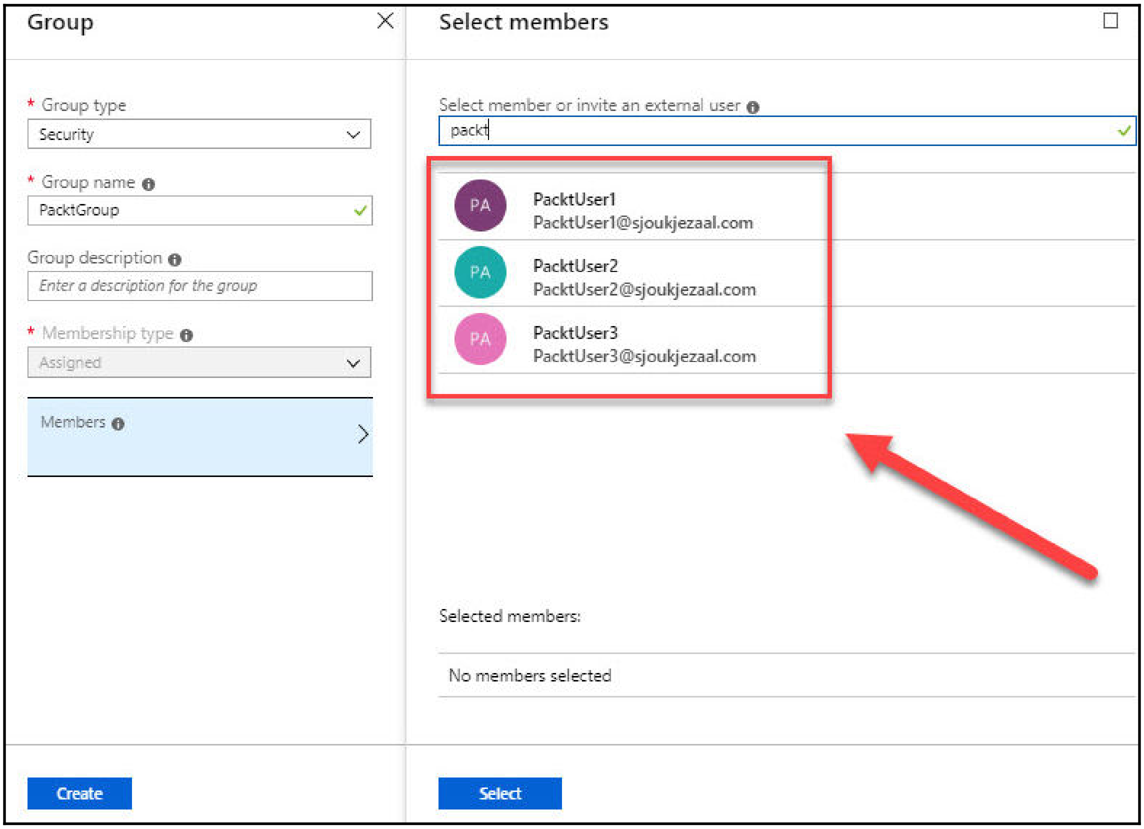
NAME	GROUP TYPE	MEMBERSHIP TYPE
AD Admins	Security	Assigned

Creating a new group

4. Add the following values to create the new group:
    - **Group type**: **Security.**
    - **Group name**: `PacktGroup`.

- **Membership type**: Here, you can choose between three different values. The first is **Assigned**, where you assign the members manually to the group; then, there's **Dynamic user**, where the group membership is determined based on certain user properties. Dynamic group membership eliminates the management overhead of adding and removing users. The last option is **Dynamic device**, and here the group membership is determined based on certain device properties. Select the first option: **Assigned.**

5. Click the **Members** tab to add members to this group. Select the three user accounts that we created in the previous demonstration, as follows:



* Group type: Security

* Group name: PacktGroup

Group description: Enter a description for the group

* Membership type: Assigned

Members

Select member or invite an external user: packt

PacktUser1 PacktUser1@sjoukjezaal.com

PacktUser2 PacktUser2@sjoukjezaal.com

PacktUser3 PacktUser3@sjoukjezaal.com

Selected members:

No members selected

Adding users to a group

6. Click **Select** to add the members, and then **Create** to create the group.

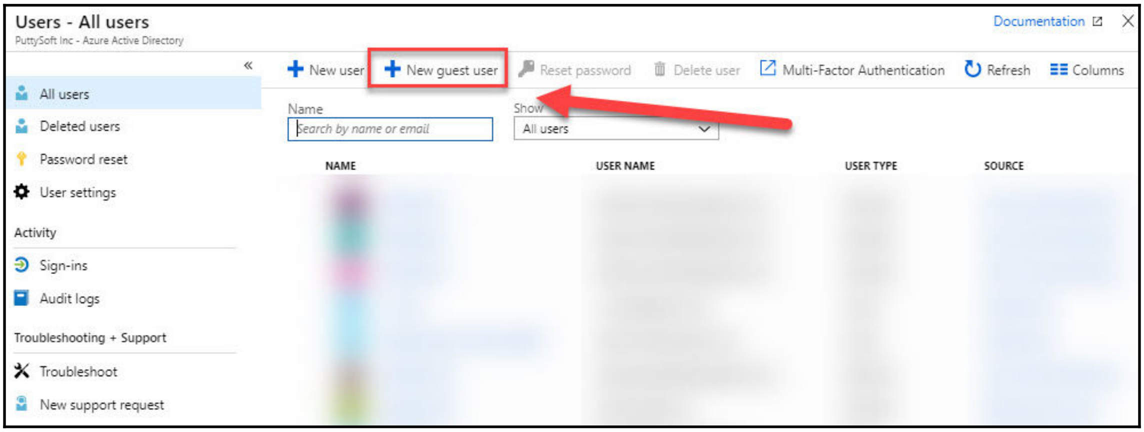
We have now created a new group inside Azure AD and added the user accounts to it that we created in the previous demonstration. In the next section, we are going to cover how to add and manage guest accounts.

Adding and managing guest accounts

You can also add guest accounts in Azure AD using Azure AD **business-to-business** (**B2B**). Azure AD B2B is a feature on top of Azure AD that allows organizations to work safely with external users. To be added to Azure B2B, external users don't need to have a Microsoft work or personal account that has been added to an existing Azure AD tenant. All sorts of accounts can be added to Azure B2B.

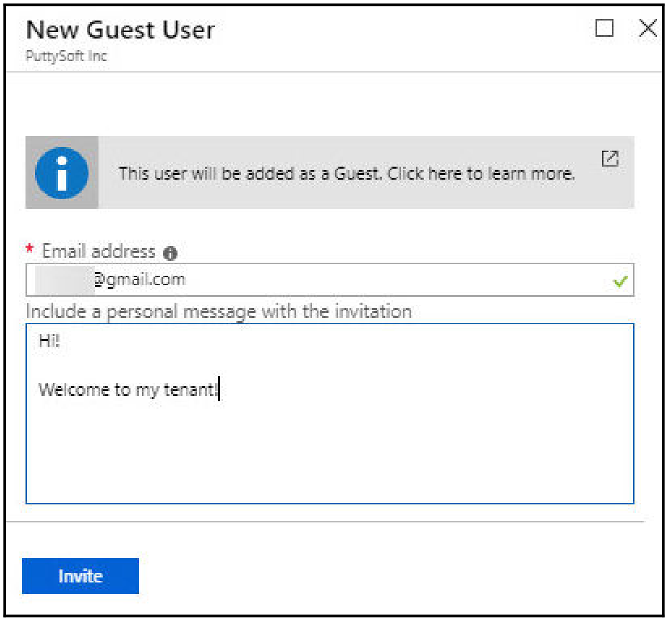
You don't have to configure anything in the Azure portal to use B2B; this feature is enabled by default for all Azure AD tenants. Perform the following steps:

1. Adding guest accounts to your Azure AD tenant is similar to adding internal users to your tenant. When you go to the users overview blade, you can choose **+ New guest user** in the top menu, as follows:



Adding a guest user

2. Then, you can provide an email address and a personal message, which is sent to the user's inbox. This personal message includes a link to log in to your tenant:



New Guest User

PuttySoft Inc

This user will be added as a Guest. Click here to learn more.

* Email address: [redacted]@gmail.com

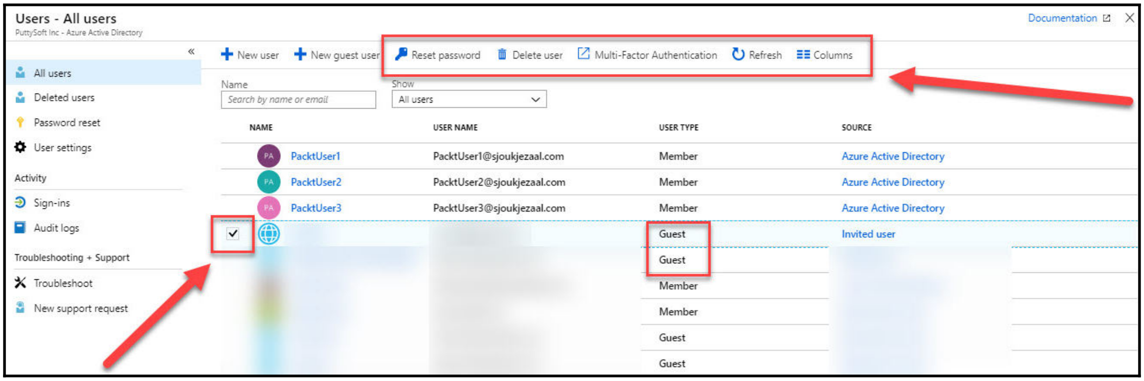
Include a personal message with the invitation:

Hi!

Welcome to my tenant!

External user properties

3. Click **Invite** to add the user to your Azure AD tenant and send out the invitation to the user's inbox.
4. To manage external users after creation, you can select them from the user overview blade. They will have a **USER TYPE**, which is named **Guest**. Simply select the user in the list and you will be able to manage the settings that are displayed in the top menu for this user, as follows:



Users - All users

PuttySoft Inc - Azure Active Directory

Name: Search by name or email

Show: All users

	NAME	USER NAME	USER TYPE	SOURCE
	PacktUser1	PacktUser1@sjoukjezaal.com	Member	Azure Active Directory
	PacktUser2	PacktUser2@sjoukjezaal.com	Member	Azure Active Directory
	PacktUser3	PacktUser3@sjoukjezaal.com	Member	Azure Active Directory
☑	[redacted]	[redacted]	Guest	Invited user
	[redacted]	[redacted]	Guest	[redacted]
	[redacted]	[redacted]	Member	[redacted]
	[redacted]	[redacted]	Member	[redacted]
	[redacted]	[redacted]	Guest	[redacted]
	[redacted]	[redacted]	Guest	[redacted]

Managing external users

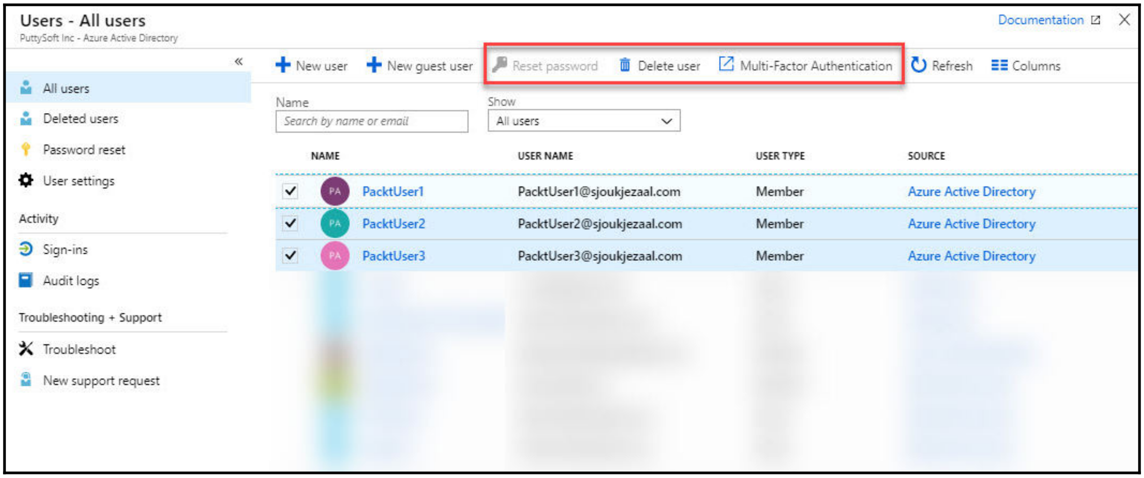
In the next section, we are going to cover how to perform bulk user updates from the Azure portal.

Performing bulk user updates

Performing bulk user updates is similar to managing single users (internal and guest). The only property that can't be set for multiple users is resetting the password. This has to be done for a single user.

To perform a bulk user update, you have to perform the following steps:

1. Go to the users overview blade again.
2. You can select multiple users in the overview blade. From the top menu, select the property that you want to configure, as follows:



Name: Search by name or email
Show: All users

	NAME	USER NAME	USER TYPE	SOURCE
✓	PA PacktUser1	PacktUser1@sjoukjezaal.com	Member	Azure Active Directory
✓	PA PacktUser2	PacktUser2@sjoukjezaal.com	Member	Azure Active Directory
✓	PA PacktUser3	PacktUser3@sjoukjezaal.com	Member	Azure Active Directory

Performing a bulk user update

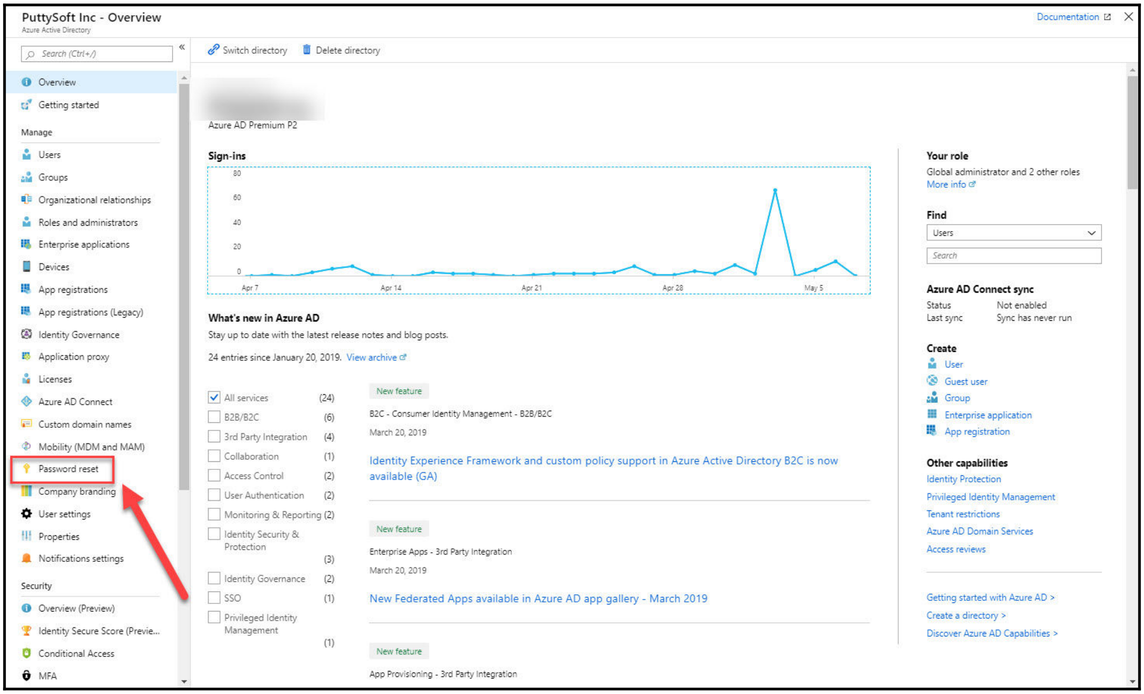
This concludes the demonstration for performing bulk user updates. In the next section, we are going to cover how you can configure self-service password reset for your users.

Configuring self-service password reset

By enabling self-service password for your users, they are able to change their passwords automatically, without calling the help desk. This eliminates management overhead significantly.

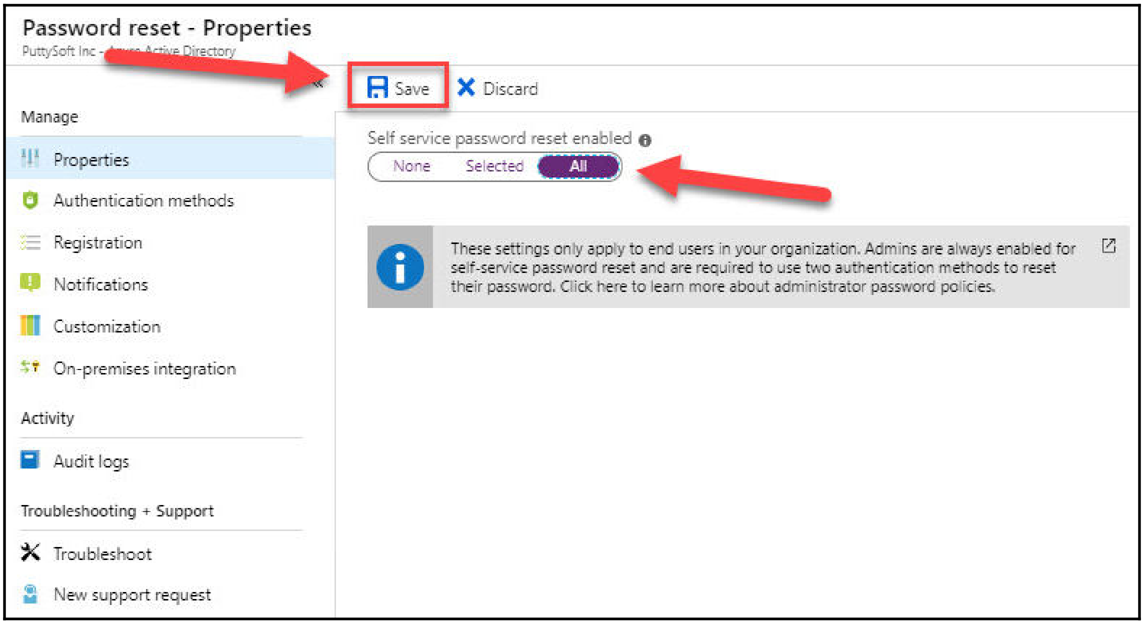
Self-service password reset can easily be enabled from the Azure portal. Therefore, you have to perform the following steps:

1. Navigate to the Azure portal by opening `https://portal.azure.com`.
2. In the left menu, select **Azure Active Directory**.
3. In the Azure AD overview blade, in the left menu, under **Manage**, select **Password reset**, as follows:



Selecting password reset

4. In the password reset overview blade, you can enable self-service password reset for all your users by selecting **All**, or for selected users and groups, by selecting **Selected**. For this demonstration, enable it for all users and click **Save** in the top menu, as follows:



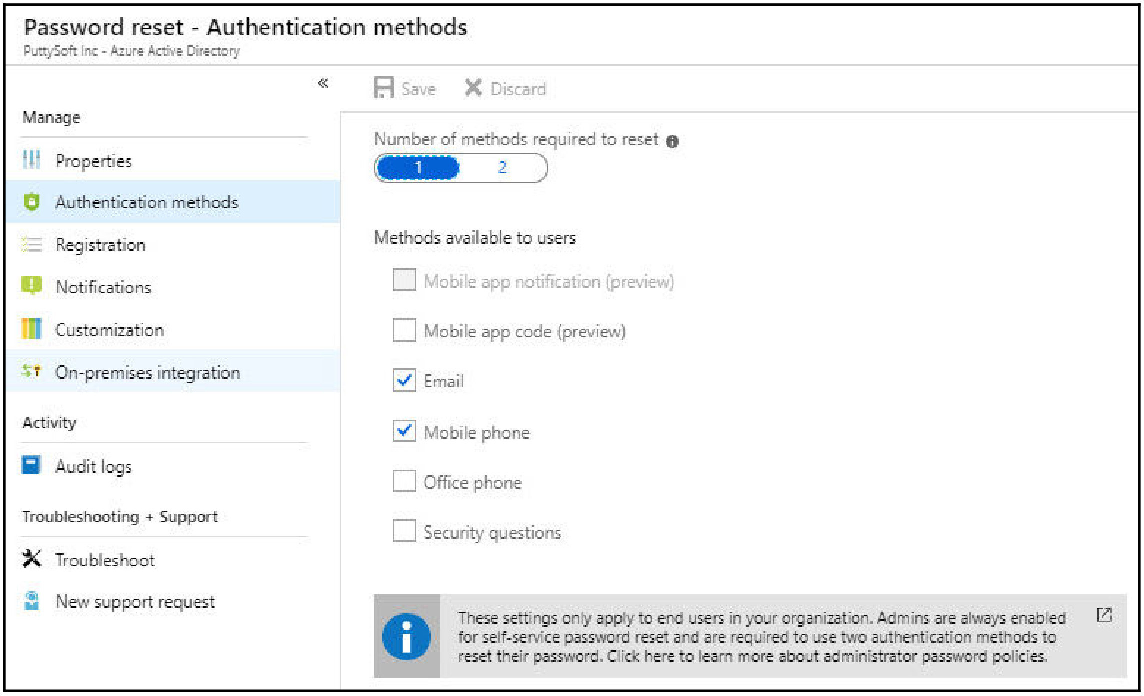
Self service password reset enabled
None Selected [✓ All]

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

Enabling self-service password reset for all users

5. Next, we need to set the different required authentication methods for your users. For this, under **Manage**, select **Authentication methods**.

6. In the next blade, we can set the number of authentication methods that are required to reset a password and what methods there are available for your users, as follows:



Number of methods required to reset
● 1 ○ 2

Methods available to users

□ Mobile app notification (preview)

□ Mobile app code (preview)

☑ Email

☑ Mobile phone

□ Office phone

□ Security questions

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

Different authentication methods

7. Make a selection and click **Save**.

If you want to test self-service password reset after configuration, make sure that you use a user account without administrator privileges.

We have now configured self-service password reset for all our users inside our Azure AD tenant. In the next section, we are going to manage device settings in Azure AD.

Azure AD Join

With Azure AD Join, you are able to join devices directly to Azure AD without the need to join your on-premises Active Directory in a hybrid environment. While hybrid Azure AD Join with an on-premises AD may still be preferred for some scenarios, Azure AD Join simplifies adding devices and modernizes device management for your organization. This can result in the reduction of device-related IT costs. Your users are getting access to the corporate assets through their devices. To protect these corporate assets, you want to control these devices. This allows your administrators to make sure that your users are accessing resources from devices that meet your standards for security and compliance.

Azure AD Join is a good solution when you want to manage devices with a cloud device management solution, modernize your application infrastructure, simplify device provisioning for geographically distributed users, and when your company is adopting Microsoft 365 as the productivity suite for your users.

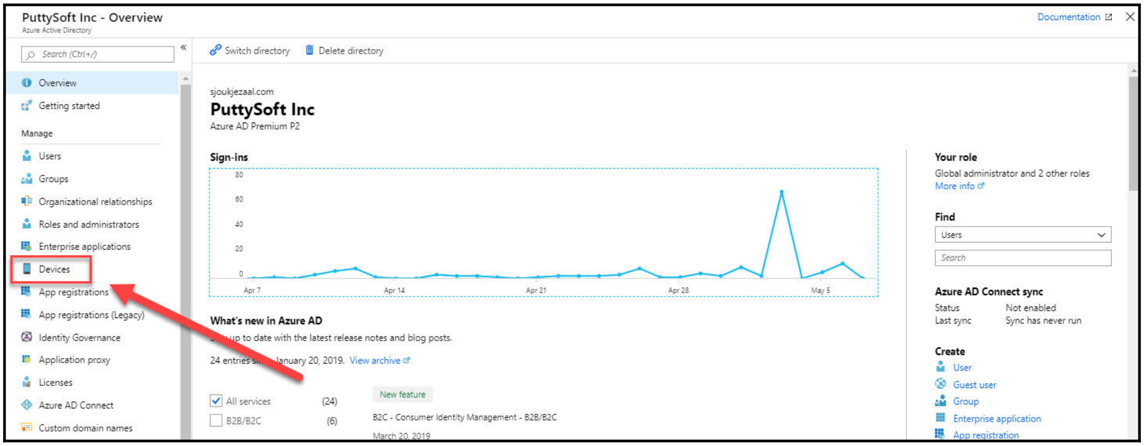
Managing device settings

Azure AD offers the ability to ensure that users are accessing Azure resources from devices that meet corporate security and compliance standards. Device management is the foundation for device-based conditional access, where you can ensure that access to your resources in your environment is only possible from managed devices.

Device settings can be managed from the Azure portal. To manage your device settings, your device needs to be registered or joined to Azure AD.

To manage the device settings from the Azure portal, you have to perform the following steps:

1. Navigate to the Azure portal by opening `https://portal.azure.com`.
2. In the left menu, select **Azure Active Directory**.
3. In the Azure AD overview blade, under **Manage**, select **Devices**, as follows:



sjoukjezaal.com

PuttySoft Inc

Azure AD Premium P2

What's new in Azure AD

up to date with the latest release notes and blog posts.

24 entries si January 20, 2019. View archive

☑ All services (24)

□ B2B/B2C (6)

B2C - Consumer Identity Management - B2B/B2C

March 20, 2019

Your role

Global administrator and 2 other roles

More info

Azure AD Connect sync

Status Not enabled

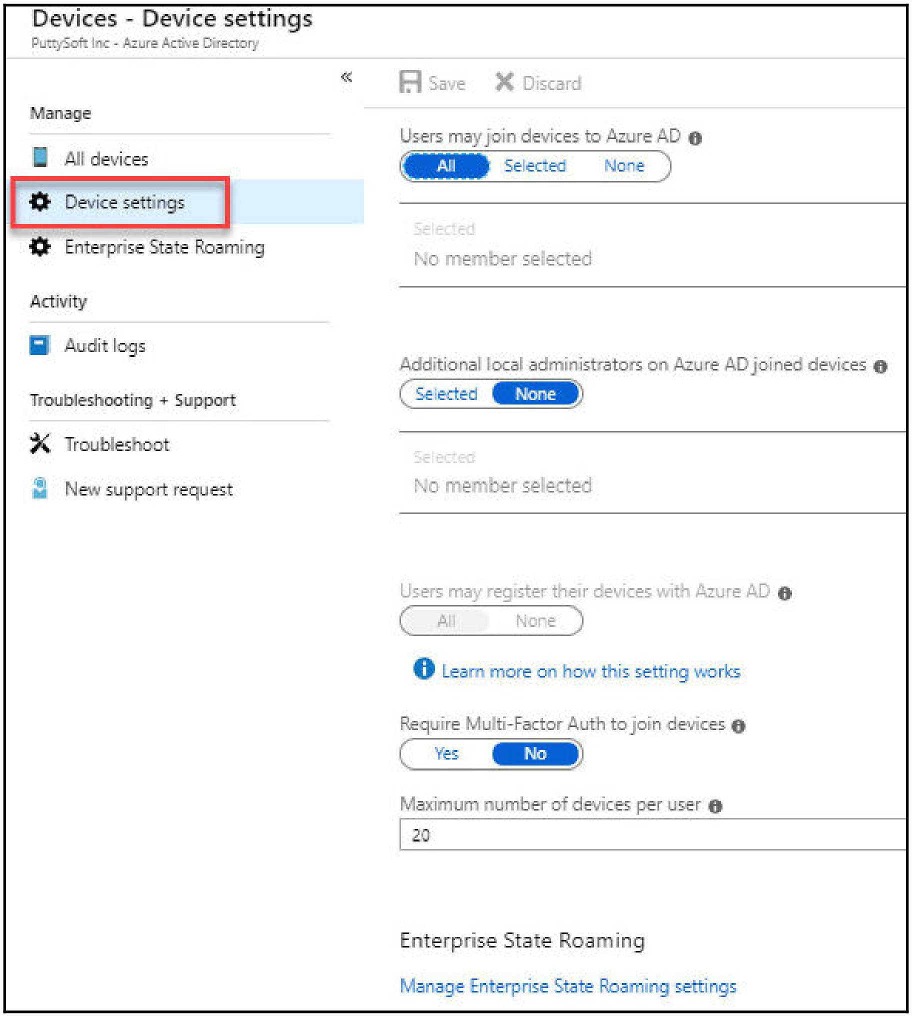
Last sync Sync has never run

Selecting Devices from the menu

4. The Device management blade will open. Here, you can configure your device management settings, locate your devices, perform device management tasks, and review the device management-related audit logs.

5. To configure device settings, select **Device settings** from the left menu. In here, you can configure the following settings, which are shown in the following screenshot:
    - **Users may join devices to Azure AD**: Here, you can set which users can join their devices to Azure AD. This setting is only applicable to Azure AD Join on Windows 10.
    - **Additional local administrators on Azure AD joined devices**: Here, you can select the users that are granted local administrator permissions on a device. The users that are selected here are automatically added to the device administrator's role in Azure AD. Global administrators in Azure AD and device owners are granted local administrator rights by default (this is an Azure AD Premium option).
    - **Users may register their devices with Azure AD**: This setting needs to be configured to allow devices to be registered with Azure AD. There are two options here: **None**, that is, devices are not allowed to register when they are not Azure AD joined or hybrid Azure AD joined, and **All**, that is, all devices are allowed to register. Enrolment with Microsoft Intune or **Mobile Device Management** (**MDM**) for Office 365 requires registration. If you have configured either of these services, **All** is selected and **None** is not available.
    - **Require Multi-Factor Auth to join devices**: Here, you can set that users are required to perform multi-factor authentication when registering a device. Before you can enable this setting, MFA needs to be configured for the users that register their devices.

- **Maximum number of devices**: This setting allows you to select the maximum number of devices that a user can have in Azure AD:



Devices - Device settings
PuttySoft Inc - Azure Active Directory

Users may join devices to Azure AD: [✓ All] Selected None

Selected
No member selected

Additional local administrators on Azure AD joined devices: Selected [✓ None]

Selected
No member selected

Users may register their devices with Azure AD: All None

Learn more on how this setting works

Require Multi-Factor Auth to join devices: Yes [✓ No]

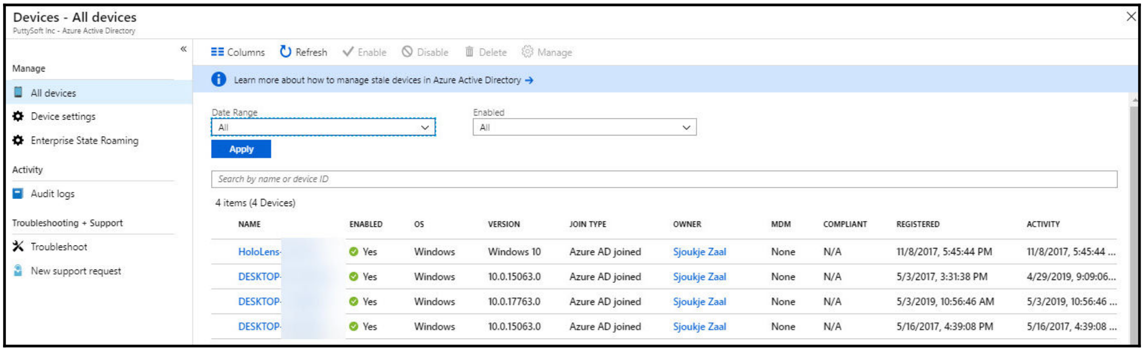
Maximum number of devices per user: 20

Enterprise State Roaming

Manage Enterprise State Roaming settings

Device settings overview

6. To locate your devices, under **Manage**, select **All devices**. In this overview, you will see all the joined and registered devices, as follows:



Devices - All devices
PuttySoft Inc - Azure Active Directory

Learn more about how to manage stale devices in Azure Active Directory →

Date Range: All

Enabled: All

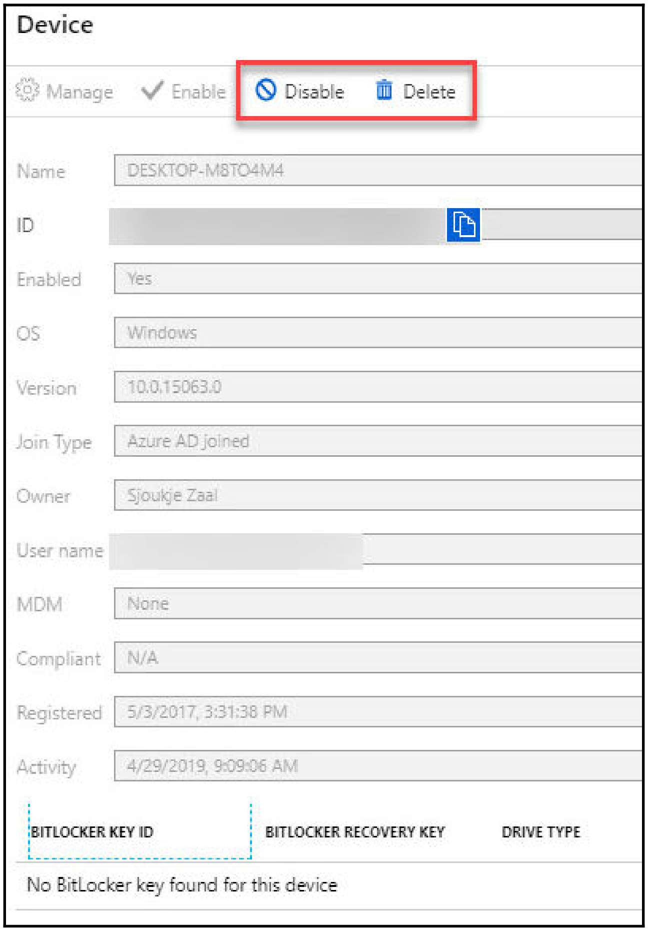
Search by name or device ID

4 items (4 Devices)

NAME	ENABLED	OS	VERSION	JOIN TYPE	OWNER	MDM	COMPLIANT	REGISTERED	ACTIVITY
HoloLens-[redacted]	✓ Yes	Windows	Windows 10	Azure AD joined	Sjoukje Zaal	None	N/A	11/8/2017, 5:45:44 PM	11/8/2017, 5:45:44 ...
DESKTOP-[redacted]	✓ Yes	Windows	10.0.15063.0	Azure AD joined	Sjoukje Zaal	None	N/A	5/3/2017, 3:31:38 PM	4/29/2019, 9:09:06...
DESKTOP-[redacted]	✓ Yes	Windows	10.0.17763.0	Azure AD joined	Sjoukje Zaal	None	N/A	5/3/2019, 10:56:46 AM	5/3/2019, 10:56:46 ...
DESKTOP-[redacted]	✓ Yes	Windows	10.0.15063.0	Azure AD joined	Sjoukje Zaal	None	N/A	5/16/2017, 4:39:08 PM	5/16/2017, 4:39:08 ...

Located devices

7. You can also select the different devices from the list to get more detailed information about the device. In here, global administrators and cloud device administrators can **Disable** or **Delete** the device, as follows:

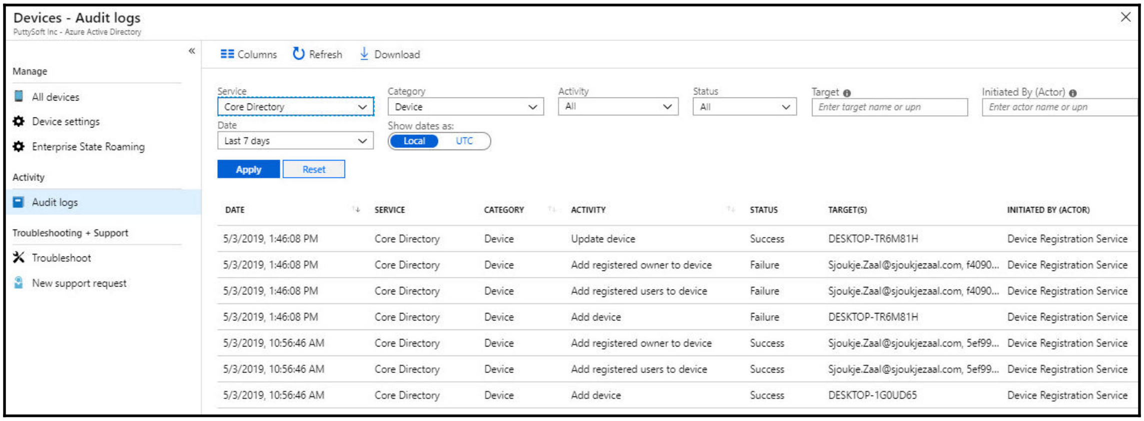


Name	DESKTOP-M8TO4M4
ID	[redacted]
Enabled	Yes
OS	Windows
Version	10.0.15063.0
Join Type	Azure AD joined
Owner	Sjoukje Zaal
User name	[redacted]
MDM	None
Compliant	N/A
Registered	5/3/2017, 3:31:38 PM
Activity	4/29/2019, 9:09:06 AM

BITLOCKER KEY ID	BITLOCKER RECOVERY KEY	DRIVE TYPE
No BitLocker key found for this device		

Device information

8. For audit logs, under **Activity**, select **Audit logs**. From here, you can view and download the different log files. You can also create filters to search through the logs, as follows:



Devices - Audit logs
PuttySoft Inc - Azure Active Directory

Service: Core Directory
Category: Device
Activity: All
Status: All
Target: Enter target name or upn
Initiated By (Actor): Enter actor name or upn
Date: Last 7 days
Show dates as: Local UTC

DATE	SERVICE	CATEGORY	ACTIVITY	STATUS	TARGET(S)	INITIATED BY (ACTOR)
5/3/2019, 1:46:08 PM	Core Directory	Device	Update device	Success	DESKTOP-TR6M81H	Device Registration Service
5/3/2019, 1:46:08 PM	Core Directory	Device	Add registered owner to device	Failure	Sjoukje.Zaal@sjoukjezaal.com, f4090...	Device Registration Service
5/3/2019, 1:46:08 PM	Core Directory	Device	Add registered users to device	Failure	Sjoukje.Zaal@sjoukjezaal.com, f4090...	Device Registration Service
5/3/2019, 1:46:08 PM	Core Directory	Device	Add device	Failure	DESKTOP-TR6M81H	Device Registration Service
5/3/2019, 10:56:46 AM	Core Directory	Device	Add registered owner to device	Success	Sjoukje.Zaal@sjoukjezaal.com, 5ef99...	Device Registration Service
5/3/2019, 10:56:46 AM	Core Directory	Device	Add registered users to device	Success	Sjoukje.Zaal@sjoukjezaal.com, 5ef99...	Device Registration Service
5/3/2019, 10:56:46 AM	Core Directory	Device	Add device	Success	DESKTOP-1G0UD65	Device Registration Service

Audit logs

We have now looked at all the different management and configuration options for devices that are registered or joined to Azure AD. In the next section, we are going to cover how you can add custom domains to Azure AD.

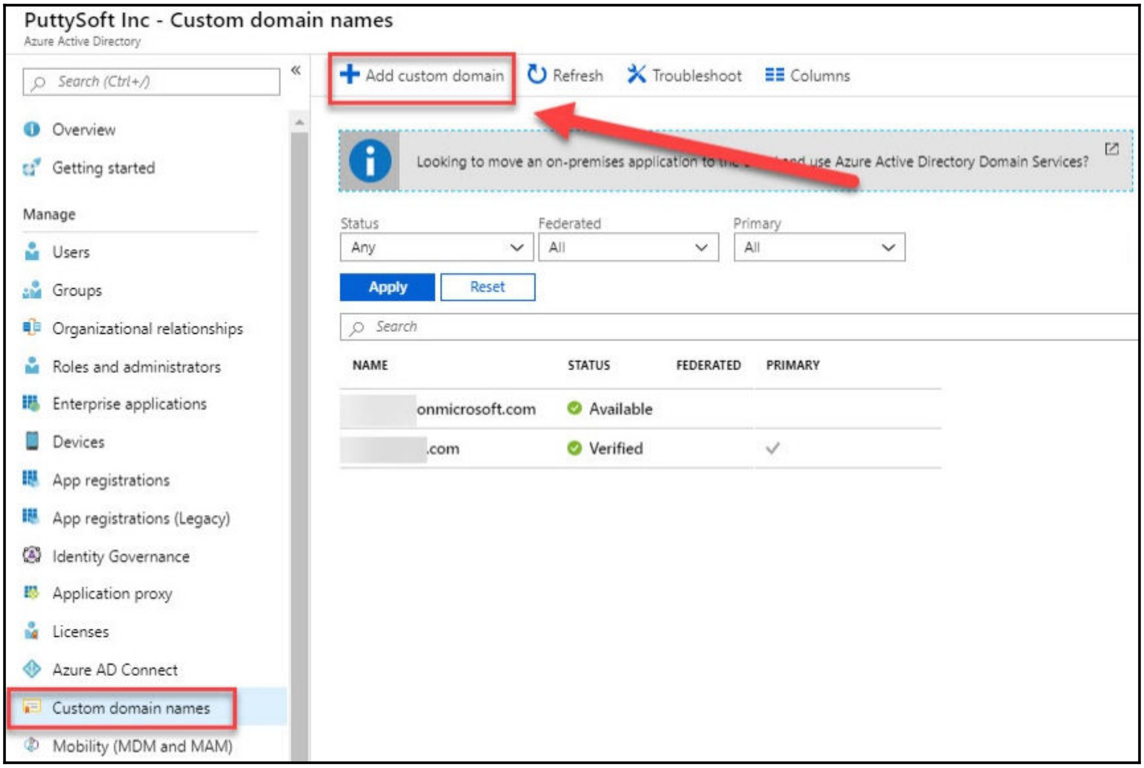
Adding custom domains

Azure creates an initial domain for every Azure AD tenant that is created in a subscription. This domain name consists of the tenant name, followed by `onmicrosoft.com` (`packtpub.onmicrosoft.com`). You cannot change or delete the initial domain name, but you can add custom domains to your Azure AD tenant.

This custom domain name can be registered at a third-party domain registrar and, after registration, you can add it to the Azure AD tenant.

To add a custom domain to Azure AD from the Azure portal, you have to perform the following steps:

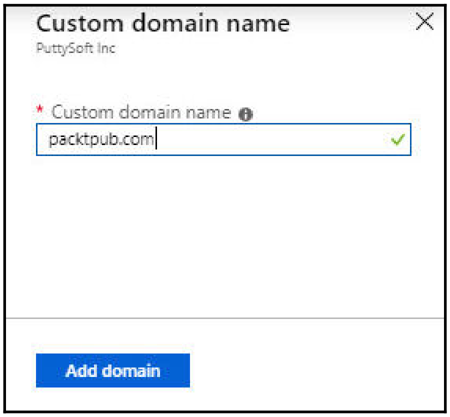
1. Navigate to the Azure portal by opening `https://portal.azure.com`.
2. In the left menu, select **Azure Active Directory**.
3. In the Azure AD overview blade, under **Manage**, select **Custom domain names**. To add a custom domain, select the **+ Add custom domain** button in the top menu, as follows:



NAME	STATUS	FEDERATED	PRIMARY
onmicrosoft.com	Available		
.com	Verified		✓

Adding a custom domain

4. Type the custom domain name in the **Custom domain name** field (for example, `packtpub.com`) and select **Add domain**, as follows:



Custom domain name

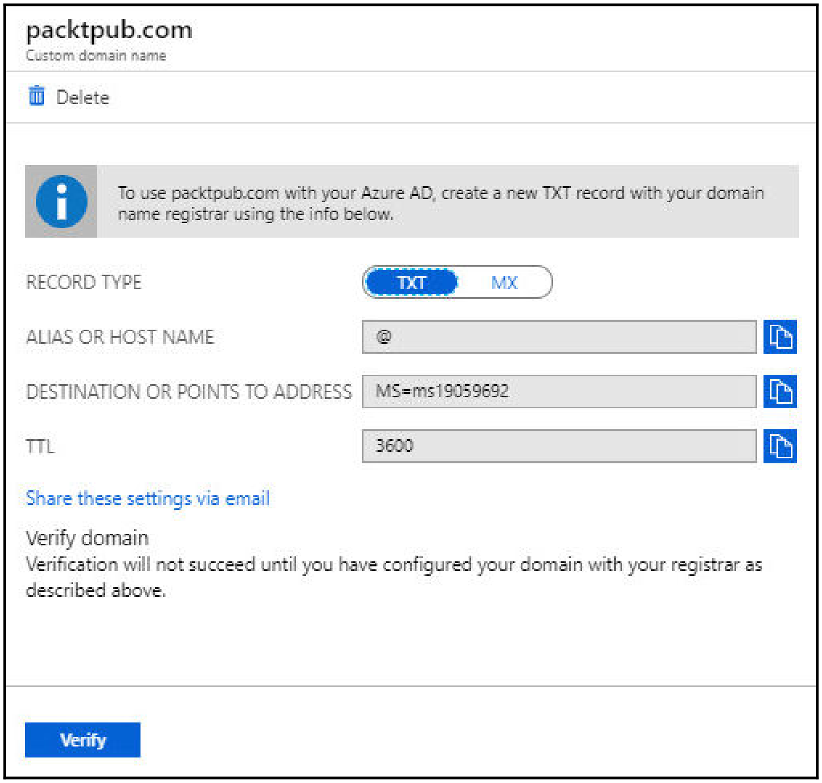
PuttySoft Inc

* Custom domain name

packtpub.com

Providing a custom domain name

5. After you add your custom domain name to Azure AD, you need to create a **TXT** record inside the DNS settings of your domain registrar. Go to your domain registrar and add the Azure AD DNS information from your copied TXT file. Creating this TXT record for your domain *verifies* ownership of your domain name. After creating the TXT file, click **Verify**, as follows:


packtpub.com
Custom domain name

To use packtpub.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

RECORD TYPE: TXT | MX

ALIAS OR HOST NAME: @

DESTINATION OR POINTS TO ADDRESS: MS=ms19059692

TTL: 3600

Share these settings via email

Verify domain
Verification will not succeed until you have configured your domain with your registrar as described above.

Verifying the ownership of the domain

6. After you've verified your custom domain name, you can delete your verification TXT or MX file.

We have now configured a custom domain for our Azure AD tenant. Your users can now use this domain name to log in to the various Azure resources they have access to.

Summary

In this chapter, we covered the first part of the *Managing Identities* objective. We covered the various aspects of Azure AD. You've learned how to add users and groups, how to add guest users, and how to manage your devices in Azure AD. We also covered how to add custom domain names to our Azure AD tenant from the Azure portal.

In the next chapter, we will cover the second part of this exam objective. In this chapter, we will cover how to implement and manage hybrid identities.

Questions

Answer the following questions to test your knowledge of the information in this chapter. You can find the answers in the *Assessments* section at the end of this book:

1. If you want to create a guest user using PowerShell, you have to use the `New-AzureADMSInvitation` cmdlet.
    - Yes
    - No
2. If you want to use Azure AD Join for your devices, you first need to configure your on-premises AD environment in a hybrid environment, together with Azure AD.
    - Yes
    - No
3. When you add a custom domain to Azure AD, you need to verify it by adding a TXT record to the DNS settings of your domain registrar.
    - Yes
    - No

Further reading

You can check out the following links for more information about the topics that were covered in this chapter:

- *Azure Active Directory Documentation:* `https://docs.microsoft.com/en-us/azure/active-directory/`
- *Add or delete users using Azure Active Directory:* `https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory`
- *Azure Active Directory version 2 cmdlets for group management:* `https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-settings-v2-cmdlets`
- *Quickstart: Add a guest user with PowerShell:* `https://docs.microsoft.com/en-us/azure/active-directory/b2b/b2b-quickstart-invite-powershell`
- *Quickstart: Self-service password reset:* `https://docs.microsoft.com/en-us/azure/active-directory/authentication/quickstart-sspr`
- *How to: Plan your Azure Active Directory join implementation*: `https://docs.microsoft.com/en-us/azure/active-directory/devices/azureadjoin-plan`
- *What is device management in Azure Active Directory?:* `https://docs.microsoft.com/en-us/azure/active-directory/devices/overview`
- *Add your custom domain name using the Azure Active Directory portal:* `https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain`

15
Implementing and Managing Hybrid Identities

In the previous chapter, we've covered how to manage **Azure Active Directory** (**Azure AD**). This chapter proceeds with the *Managing Identities* objective. In this chapter, we are going to cover how to implement and manage hybrid identities. We are going to install and configure Azure AD Connect to synchronize the identities from your on-premises Active Directory to Azure AD. Then you will learn how to manage Azure AD Connect. In the last part of this chapter, we will dive into password sync and password writeback. You will learn how to enable password sync in Azure AD Connect and the Azure portal. At lastly, you will learn how to manage password sync.

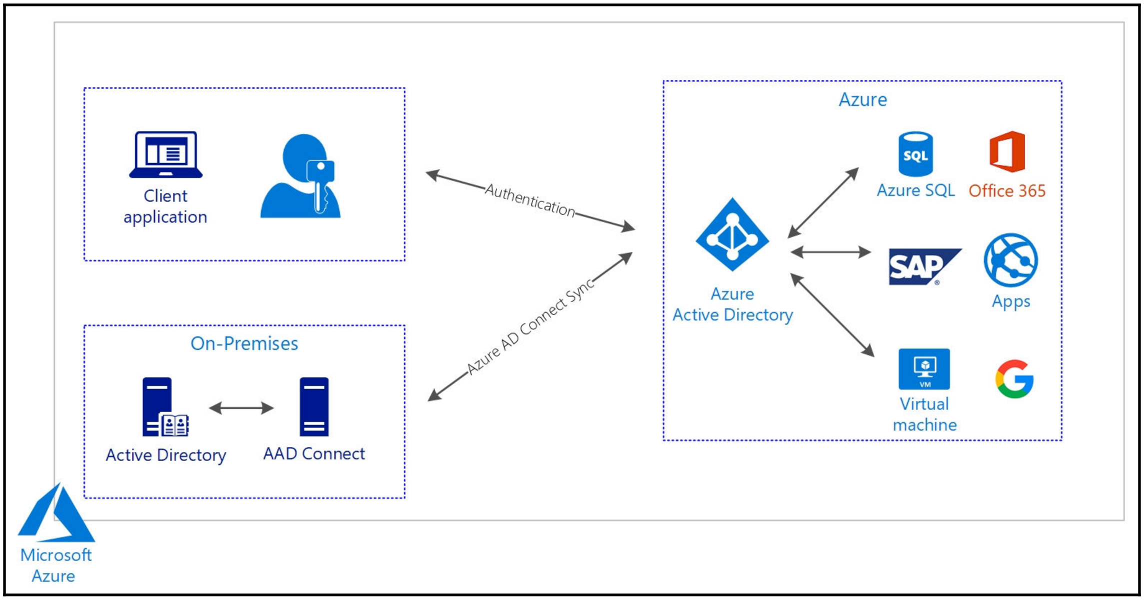
The following topics will be covered in this chapter:

- Azure AD Connect
- Installing Azure AD Connect
- Managing Azure AD Connect
- Managing password sync and password writeback

Azure AD Connect

Azure AD Connect is a service that you can use to synchronize your on-premises Active Directory identities with Azure. This way, you can use the same identities for authentication on your on-premises environment as well as in the cloud, and other **software as a service** (**SaaS**) applications.

The Azure AD Connect sync service consists of two parts, the Azure AD Connect sync component, which is a tool that is installed on a separate server inside your on-premises environment, and the Azure AD Connect sync service, which is part of Azure AD. The sync component can sync data from Active Directory and SQL Servers to Azure. There is also a third component named the **Active Directory Federation Services** (**ADFS**) component, which can be used in a scenario where ADFS is involved. To monitor the on-premises identity infrastructure and the different Azure AD components, you can use a tool named Azure AD Connect Health. The following diagram illustrates the architecture of Azure AD Connect:



Azure AD Connect architecture

Azure AD Connect offers support for your users to sign in with the same passwords to both on-premises and cloud resources. It provides three different authentication methods for this, the password hash synchronization method, the pass-through authentication method, and the Federated SSO method (in conjunction with ADFS).

Azure AD password hash synchronization

Most organizations only have a requirement to enable user sign in to Office 365, SaaS applications, and other Azure AD-based resources. The password hash synchronization method is well suitable for those scenarios.

Using this method, hashes of the user's password are synced between the on-premises Active Directory and Azure AD. When there are any changes to the user's password, the password is synced immediately, so users can always log in with the same credentials on-premises as well as in Azure.

This authentication method also provides Azure AD Seamless **Single Sign-On** (**SSO**). This way, users are automatically signed in when they are using a domain-joined device on the corporate network. Users only have to enter their username when using Seamless SSO. To use Seamless SSO, you don't have to install additional software or components on the on-premises network. You can push this capability to your users using group policies.

Azure AD pass-through authentication

Azure AD pass-through authentication offers the same capability as Azure AD password hash synchronization. Users can log in to their Azure resources as well as on-premises resources using the same credentials. The difference is that the passwords don't sync with Azure AD using pass-through authentication. The passwords are validated using the on-premises Active Directory and are not stored in the Azure AD at all.

This method is suitable for organizations that have security and compliance restrictions and aren't allowed to send usernames and passwords outside the on-premises network. Pass-through authentication requires an agent to be installed on a domain-joined Windows server that resides inside the on-premises environment. This agent then listens for password validation requests and only makes an outbound connection from within your network. It also offers support for **Multi-Factor Authentication** (**MFA**) and Azure AD conditional access policies.

Azure AD pass-through authentication offers Azure AD Seamless SSO as well.

In the next section, we are going to install Azure AD Connect and synchronize some on-premises users to Azure.

Installing Azure AD Connect

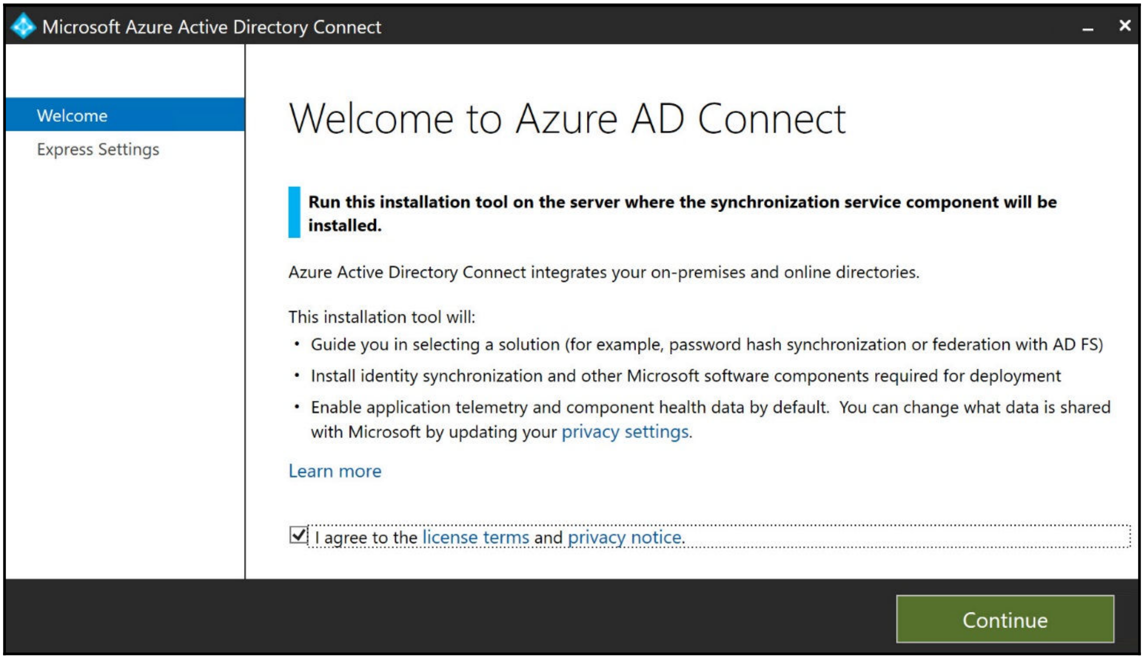
Azure AD Connect is installed on an on-premises server with Active Directory installed and configured on it. The first step is to download Azure AD Connect. After downloading, we can install it on a domain controller.

> For this demonstration, I have already deployed a Windows Server 2016 virtual machine in Azure and installed and configured Active Directory on it. Configuring Active Directory is beyond the scope of the exam and this book. Make sure that when you configure Active Directory Domain Services, the Forest name matches one of the existing verified custom domains in Azure AD. Otherwise, you will receive a warning message when you install Azure AD Connect on your domain controller, that SSO is not enabled for your users. For installing Active Directory on a Windows Server 2016 machine, you can refer to the following website: `https://blogs.technet.microsoft.com/canitpro/2017/02/22/step-by-step-setting-up-active-directory-in-windows-server-2016/`.

Therefore, take the following steps:

1. Before downloading Azure AD Connect, add at least one user to your on-premises Active Directory.
2. To download Azure AD Connect, you can refer to the following website: `https://www.microsoft.com/en-us/download/details.aspx?id=47594`. Store it on a local drive on your domain controller and run `AzureADConnect.msi` after downloading.

3. The installation wizard starts with the welcome screen. Select the checkbox to agree with the license terms:



Welcome to Azure AD Connect

Run this installation tool on the server where the synchronization service component will be installed.

Azure Active Directory Connect integrates your on-premises and online directories.

This installation tool will:

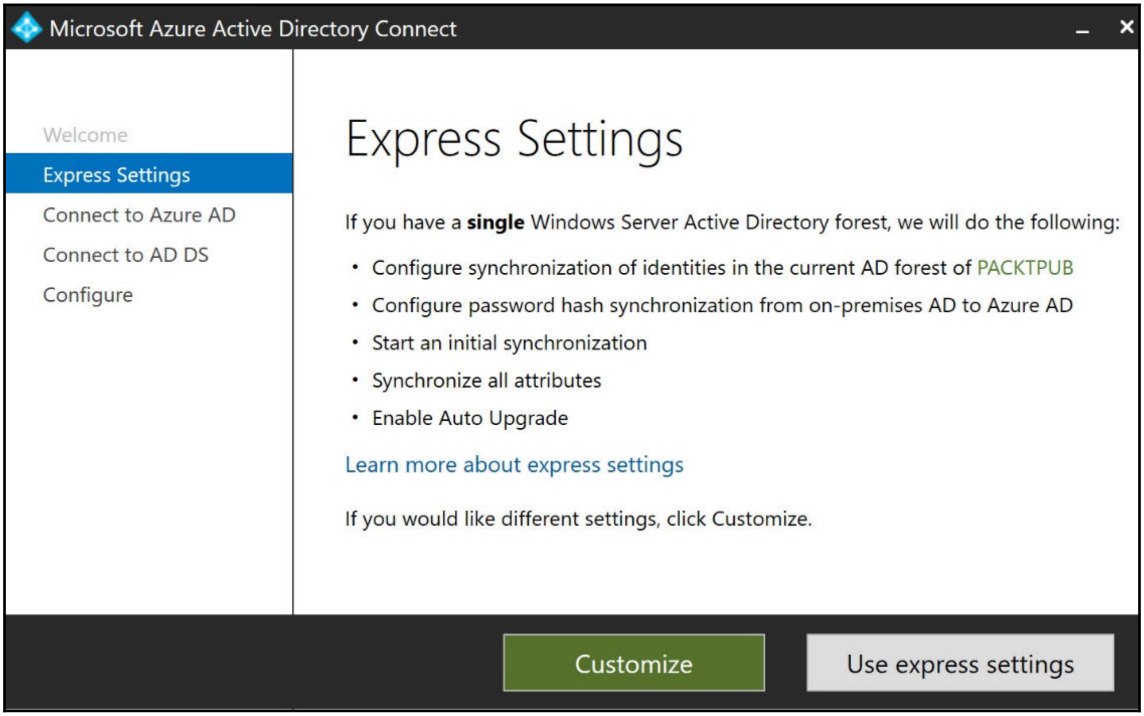
- Guide you in selecting a solution (for example, password hash synchronization or federation with AD FS)
- Install identity synchronization and other Microsoft software components required for deployment
- Enable application telemetry and component health data by default. You can change what data is shared with Microsoft by updating your privacy settings.

Learn more

☑ I agree to the license terms and privacy notice.

Azure AD Connect welcome screen

4. Select **Use express settings** in the next screen:



Express Settings

If you have a **single** Windows Server Active Directory forest, we will do the following:

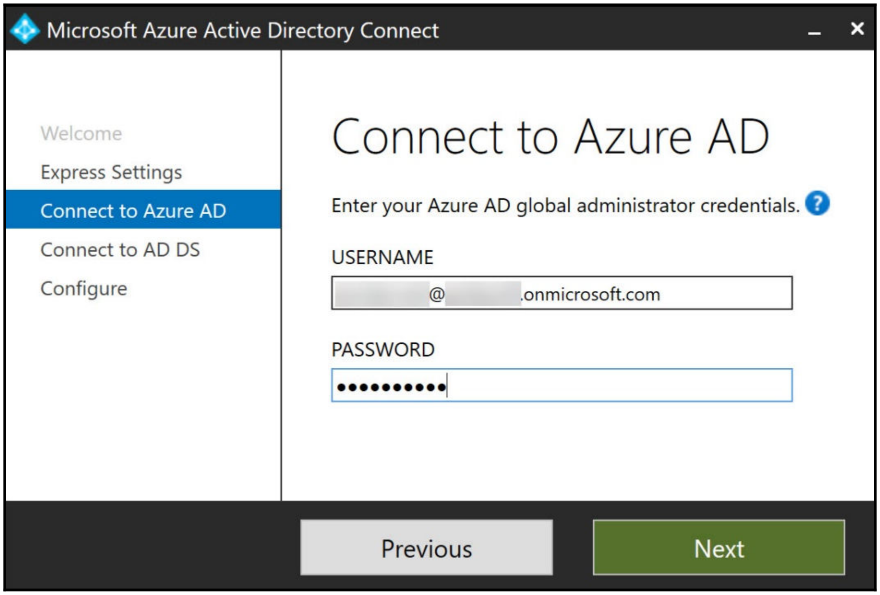
- Configure synchronization of identities in the current AD forest of PACKTPUB
- Configure password hash synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

Learn more about express settings

If you would like different settings, click Customize.

Installing Azure AD Connect using express settings

5. On the next screen, provide the username and password of a global administrator account (This account must be a school or organization account and cannot be a Microsoft account or any other type of account) for your Azure AD and click **Next**:



Connect to Azure AD

Enter your Azure AD global administrator credentials.

USERNAME

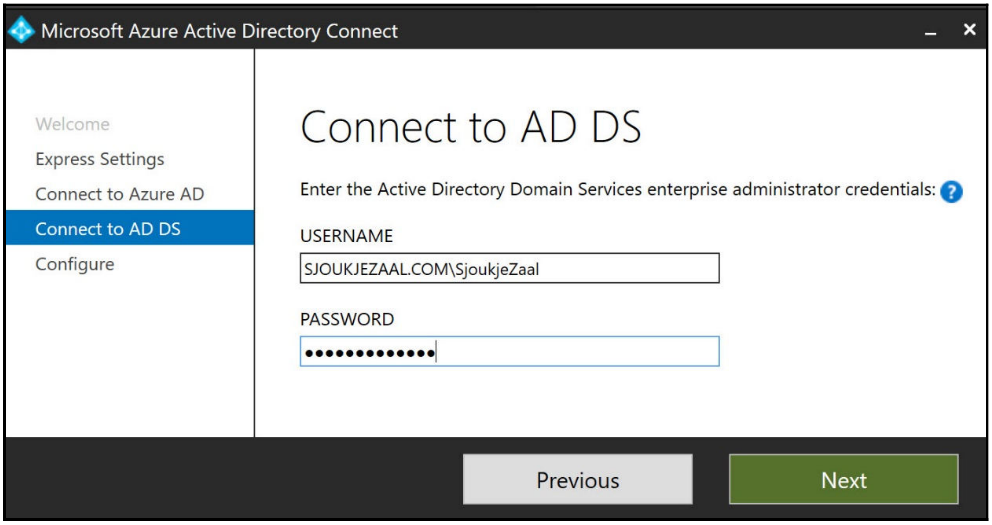
[redacted]@[redacted].onmicrosoft.com

PASSWORD

••••••••••

Provide global administrator credentials

6. On the **Connect to AD DS** screen, enter the username and password for an enterprise administrator account and click **Next** as follows:



Connect to AD DS

Enter the Active Directory Domain Services enterprise administrator credentials:

USERNAME

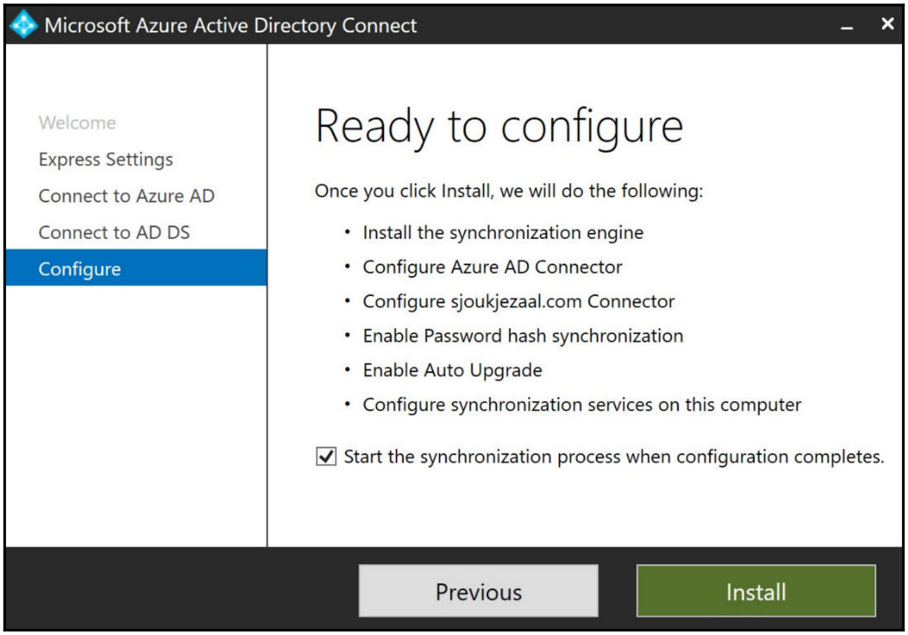
SJOUKJEZAAL.COM\SjoukjeZaal

PASSWORD

•••••••••••••

Enter enterprise administrator account

The last screen will give an overview of what is going to be installed, as follows:



Ready to configure

Once you click Install, we will do the following:

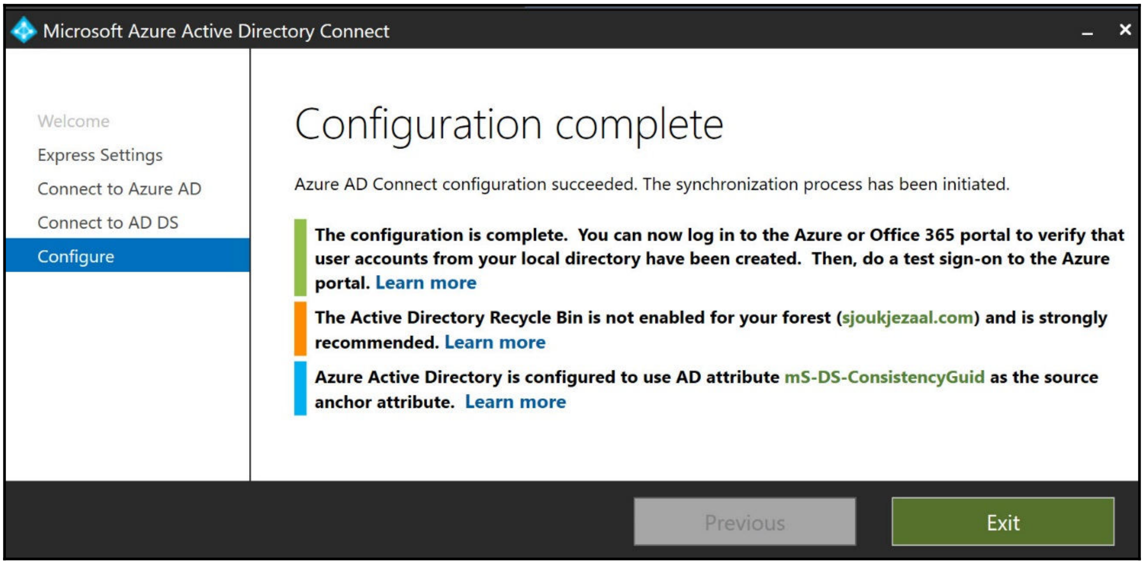
- Install the synchronization engine
- Configure Azure AD Connector
- Configure sjoukjezaal.com Connector
- Enable Password hash synchronization
- Enable Auto Upgrade
- Configure synchronization services on this computer

☑ Start the synchronization process when configuration completes.

Ready to configure

7. Click **Install.**
8. This will install Azure AD Connect on your domain controller. The synchronization process of user accounts to Azure AD will automatically be started after configuration.

9. After successful configuration, you will see the following outcome:



Configuration complete

Azure AD Connect configuration succeeded. The synchronization process has been initiated.

The configuration is complete. You can now log in to the Azure or Office 365 portal to verify that user accounts from your local directory have been created. Then, do a test sign-on to the Azure portal. Learn more

The Active Directory Recycle Bin is not enabled for your forest (sjoukjezaal.com) and is strongly recommended. Learn more

Azure Active Directory is configured to use AD attribute mS-DS-ConsistencyGuid as the source anchor attribute. Learn more

Configuration complete

10. Click **Exit** to close the installer.

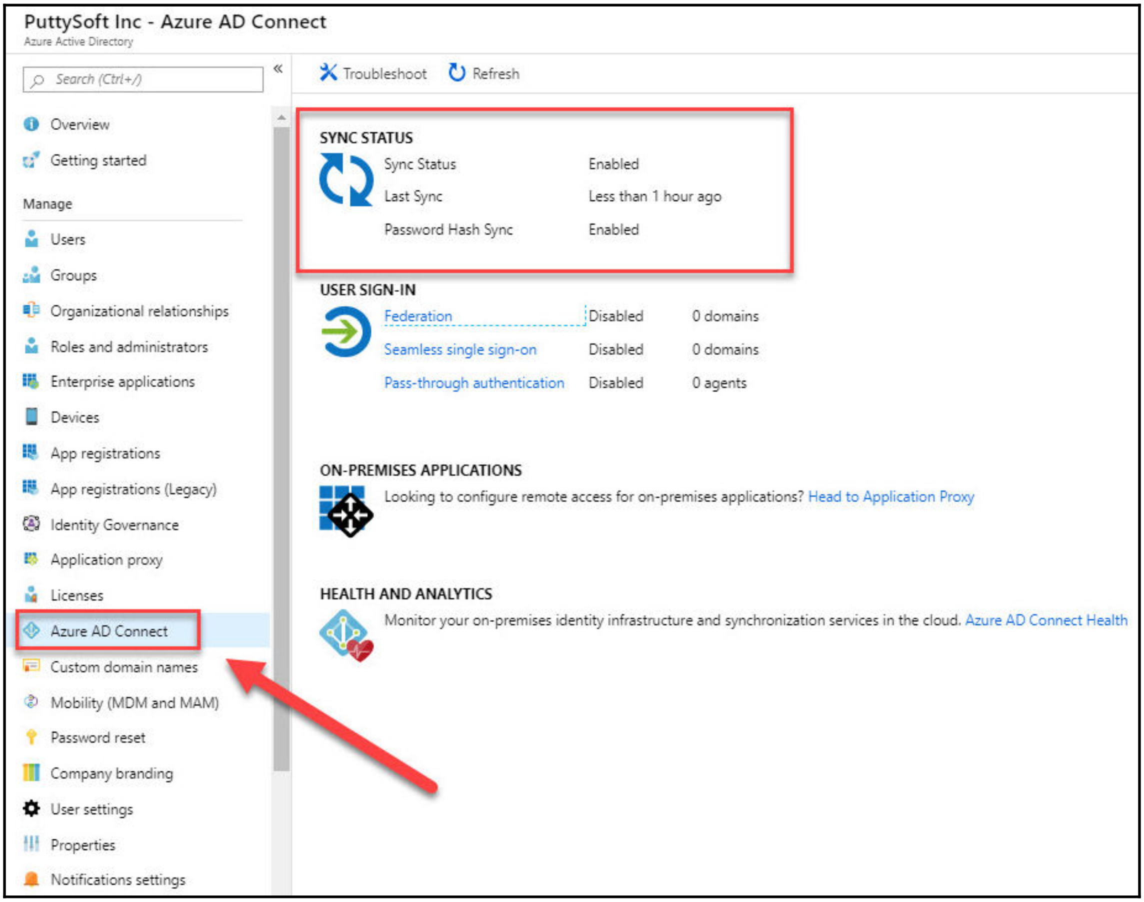
In this demonstration, we installed Azure AD Connect on an on-premises domain controller. In the next section, we are going to manage it from the Azure portal.

Managing Azure AD Connect

Azure AD Connect can be managed from the Azure portal after installation and configuration on the on-premises domain controller. To manage it, you have to take the following steps:

1. Navigate to the Azure portal by opening `https://portal.azure.com`.
2. In the left menu, select **Azure Active Directory**.

3. Under **Manage**, select **Azure AD Connect**. In the **Azure AD Connect** blade, as shown in the following screenshot, you can see that sync is enabled, that the last sync was less than an hour ago, and that **Password Hash Sync** is enabled:



PuttySoft Inc - Azure AD Connect
Azure Active Directory

SYNC STATUS

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Disabled	0 agents

ON-PREMISES APPLICATIONS

Looking to configure remote access for on-premises applications? Head to Application Proxy

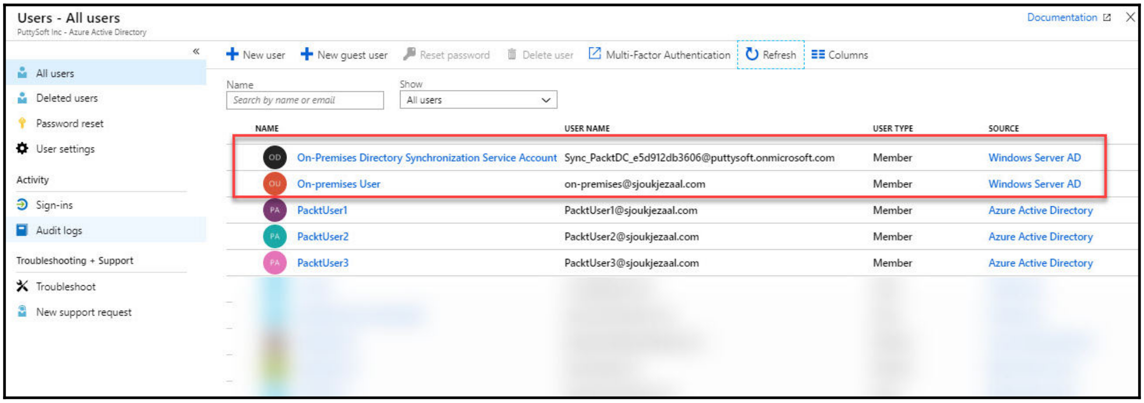
HEALTH AND ANALYTICS

Monitor your on-premises identity infrastructure and synchronization services in the cloud. Azure AD Connect Health

Azure AD Connect settings

4. You can also set the three authentication methods under **USER SIGN-IN**. Here, you can set the authentication method to **Federation, Seamless single sign-on**, or **Pass-through authentication**. You can monitor the health of your on-premises infrastructure and synchronization services under **Health and Analytics**.

5. To check if the users are synced, you can go to the **user overview** blade. Here, you will find your synced users, as in the following screenshot:



NAME	USER NAME	USER TYPE	SOURCE
OD On-Premises Directory Synchronization Service Account	Sync_PacktDC_e5d912db3606@puttysoft.onmicrosoft.com	Member	Windows Server AD
OU On-premises User	on-premises@sjoukjezaal.com	Member	Windows Server AD
PA PacktUser1	PacktUser1@sjoukjezaal.com	Member	Azure Active Directory
PA PacktUser2	PacktUser2@sjoukjezaal.com	Member	Azure Active Directory
PA PacktUser3	PacktUser3@sjoukjezaal.com	Member	Azure Active Directory

Synced users

Azure AD Connect sync synchronizes changes in your on-premises directory using a scheduler. There are two scheduler processes, one for password sync and another for object/attribute sync and maintenance tasks. For more information on how to configure this or creating a custom scheduler using PowerShell, you can refer to the following tutorial: `https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-feature-scheduler`.

In this demonstration, we managed Azure AD Connect from the Azure portal. In the next section, we are going to cover how to manage password writeback in more detail.

Password writeback

Password writeback is used for synchronizing password changes in Azure AD back to your on-premises Active Directory environment. This setting is enabled as part of Azure AD Connect, and it provides a secure mechanism to send password changes from Azure AD back to an on-premises Active Directory.

It provides the following features and capabilities:

- **Enforcement of on-premises Active Directory password policies**: When a user resets their password, the on-premises Active Directory policy is checked to ensure it meets the password requirements before it gets committed to the directory. It checks the password complexity, history, password filters, age, and other password restrictions that are defined in the on-premises Active Directory.
- **Zero-delay feedback**: Users are notified immediately after changing their password, if their password doesn't meet the on-premises Active Directory policy requirements. This is a synchronous operation.
- **Supports password writeback when an administrator resets them from the Azure portal**: When an administrator resets the password in the Azure portal, the password is written back to the on-premises Active Directory (when a user is federated or password hash synchronized). This functionality doesn't work from the Office admin portal.
- **Doesn't require any inbound firewall rules**: Password writeback uses the Azure Service Bus for communicating with the on-premises Active Directory, so there is no need to open the firewall. All communication is outbound and goes over port `443`.
- **Supports password changes from the access panel and Office 365**: When federated or password hash synchronized users change their password, those passwords are written back to your on-premises Active Directory as well.

In the next demonstration, we are going to enable password writeback.

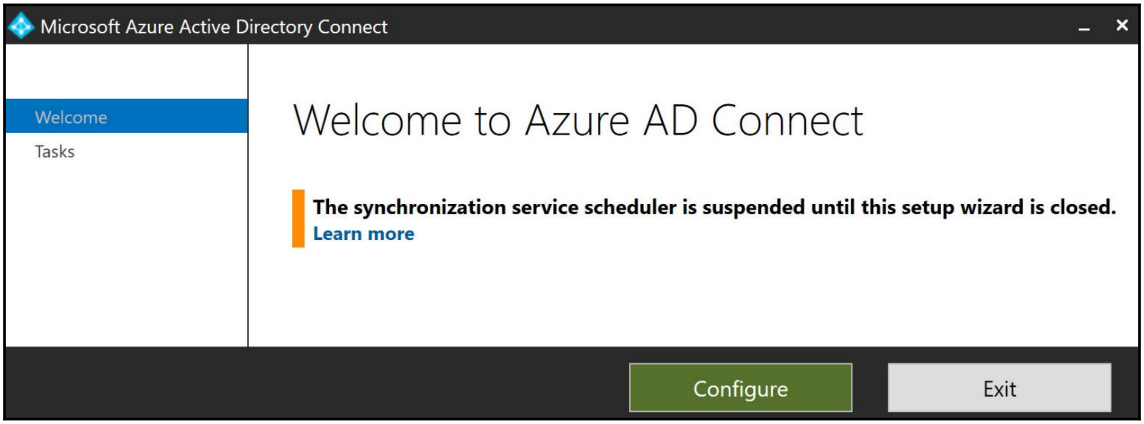
Managing password writeback

To enable password writeback, we need to make some changes to both the configuration of Azure AD Connect on the on-premises domain controller, and from the Azure portal.

Enabling password writeback in Azure AD Connect

To enable password writeback in Azure AD Connect, we have to take the following steps:

1. Log in to your on-premises domain controller using **Remote Desktop** (**RDP**) and start the Azure AD Connect wizard again.
2. On the **Welcome to Azure AD Connect** page, select **Configure** as follows:

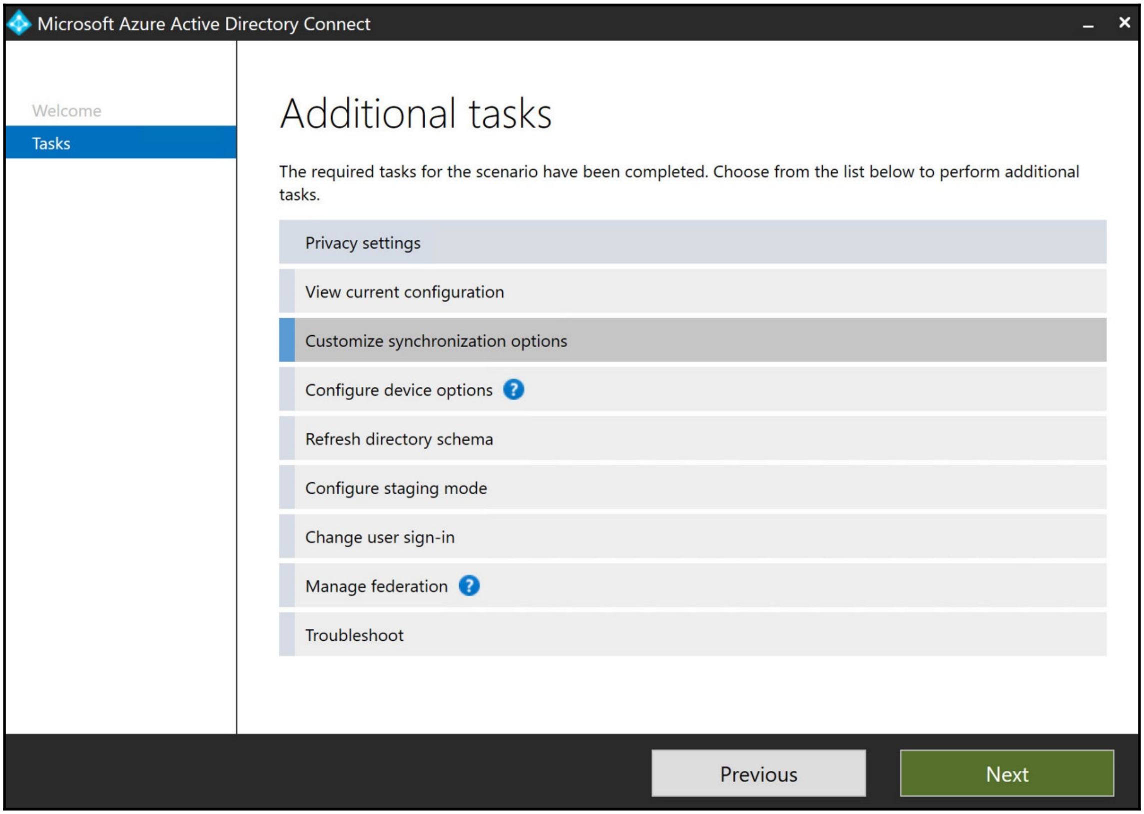


Welcome to Azure AD Connect

The synchronization service scheduler is suspended until this setup wizard is closed.
Learn more

Welcome screen

3. In the **Additional tasks** screen, select **Customize synchronization options**, and select **Next** as follows:



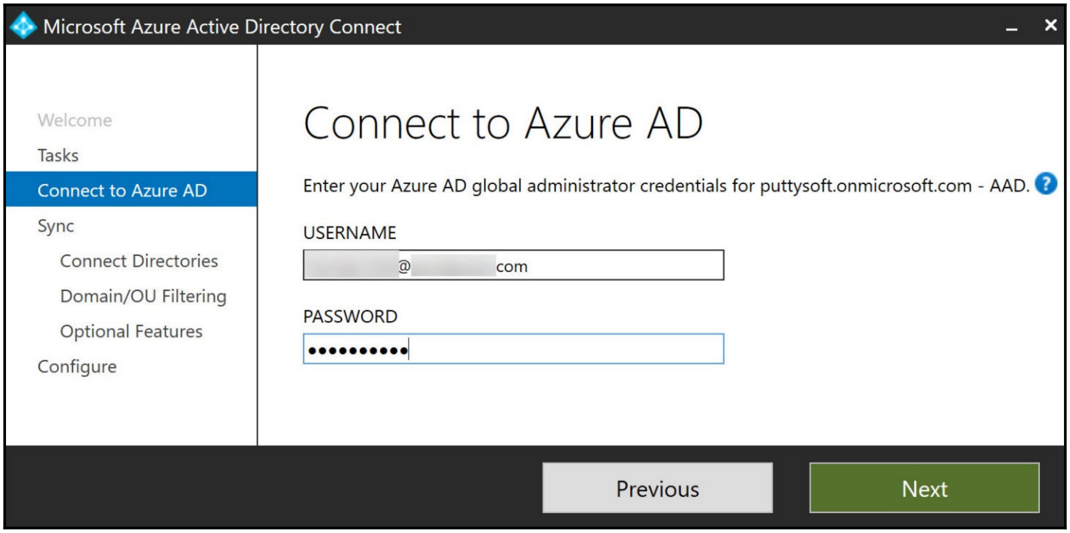
Microsoft Azure Active Directory Connect

Additional tasks

The required tasks for the scenario have been completed. Choose from the list below to perform additional tasks.

Additional tasks screen

4. Provide Azure AD global administrator credentials and select **Next** as follows:



Connect to Azure AD

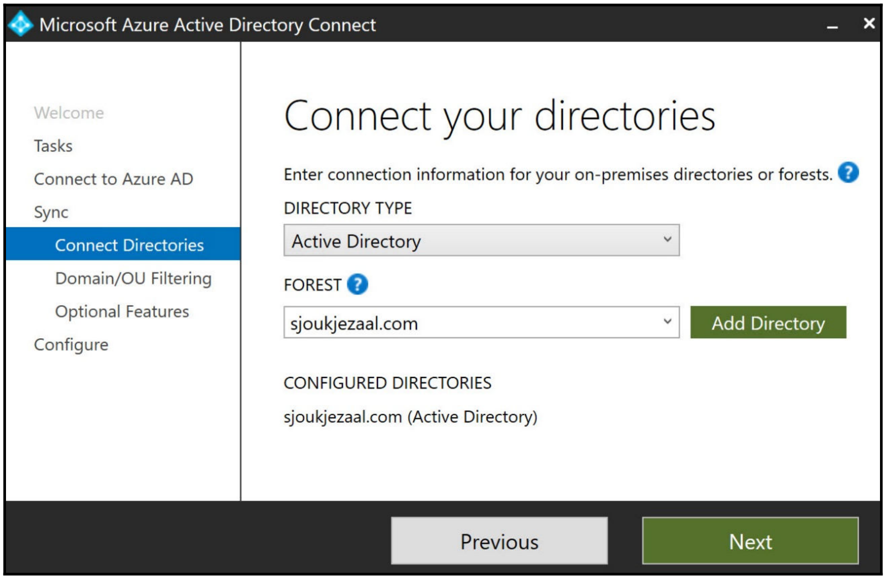
Enter your Azure AD global administrator credentials for puttysoft.onmicrosoft.com - AAD.

USERNAME: [redacted]@[redacted]com

PASSWORD: ●●●●●●●●●●●

Providing administrator credentials

5. On the **Connect your directories** screen, select **Next** as follows:



Connect your directories

Enter connection information for your on-premises directories or forests.

DIRECTORY TYPE: Active Directory

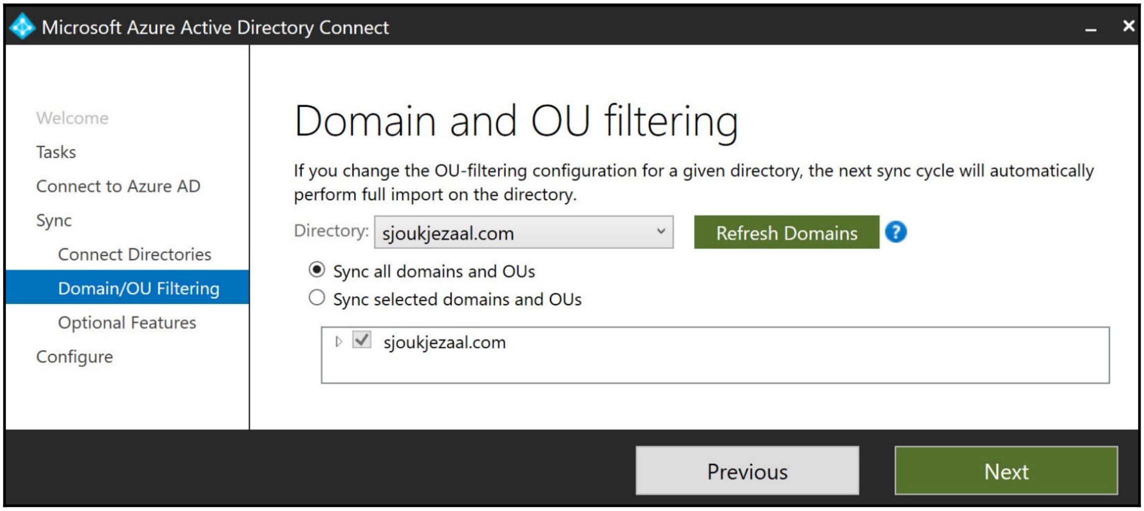
FOREST: sjoukjezaal.com

CONFIGURED DIRECTORIES

sjoukjezaal.com (Active Directory)

Connecting your directories

6. On the **Domain and OU filtering** screen, select **Next** again as follows:



Domain and OU filtering

If you change the OU-filtering configuration for a given directory, the next sync cycle will automatically perform full import on the directory.

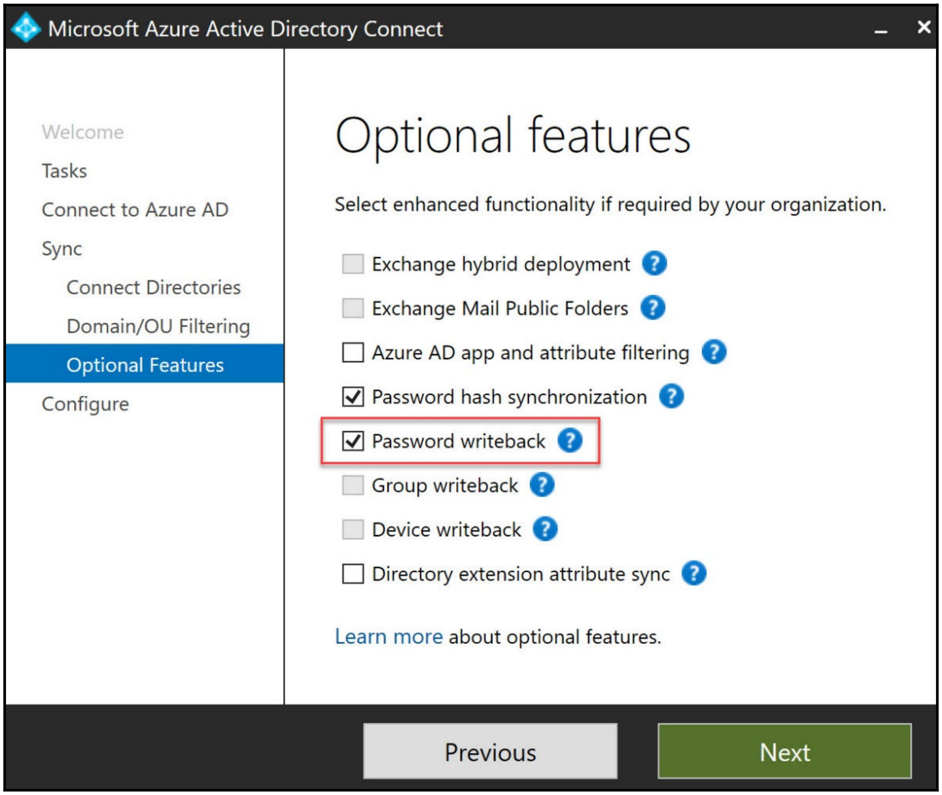
Directory: sjoukjezaal.com

● Sync all domains and OUs
○ Sync selected domains and OUs

☑ sjoukjezaal.com

Domain and OU filtering screen

7. On the **Optional features** screen, select the box next to **Password writeback** and select **Next** as follows:



Microsoft Azure Active Directory Connect

Optional features

Select enhanced functionality if required by your organization.

□ Exchange hybrid deployment
□ Exchange Mail Public Folders
□ Azure AD app and attribute filtering
☑ Password hash synchronization
☑ Password writeback
□ Group writeback
□ Device writeback
□ Directory extension attribute sync

Learn more about optional features.

Enabling password writeback

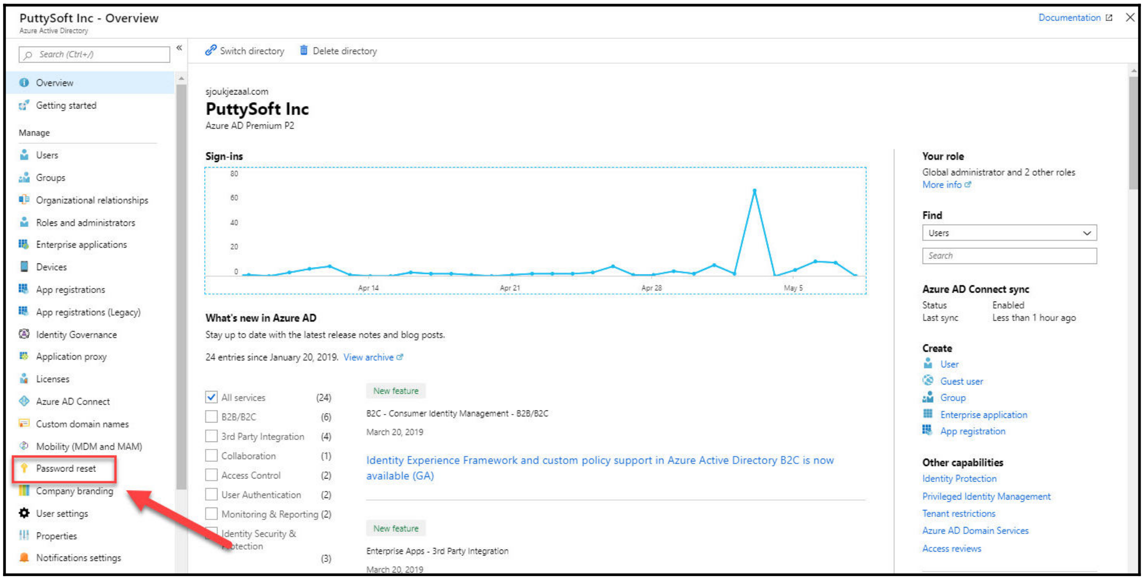
8. On the **Ready to configure** page, select **Configure**.
9. When the configuration is finished, select **Exit**.

We have now enabled password writeback on the domain controller. In the next section, we are going to enable it in the Azure portal as well.

Enabling password writeback in the Azure portal

To enable password writeback in the Azure portal, we have to take the following steps:

1. Navigate to the Azure portal by opening `https://portal.azure.com`.
2. In the left menu, select **Azure Active Directory**.
3. Under **Manage**, select **Password reset** as follows:



sjoukjezaal.com
PuttySoft Inc
Azure AD Premium P2

Global administrator and 2 other roles

Azure AD Connect sync
Status Enabled
Last sync Less than 1 hour ago

What's new in Azure AD
Stay up to date with the latest release notes and blog posts.
24 entries since January 20, 2019.

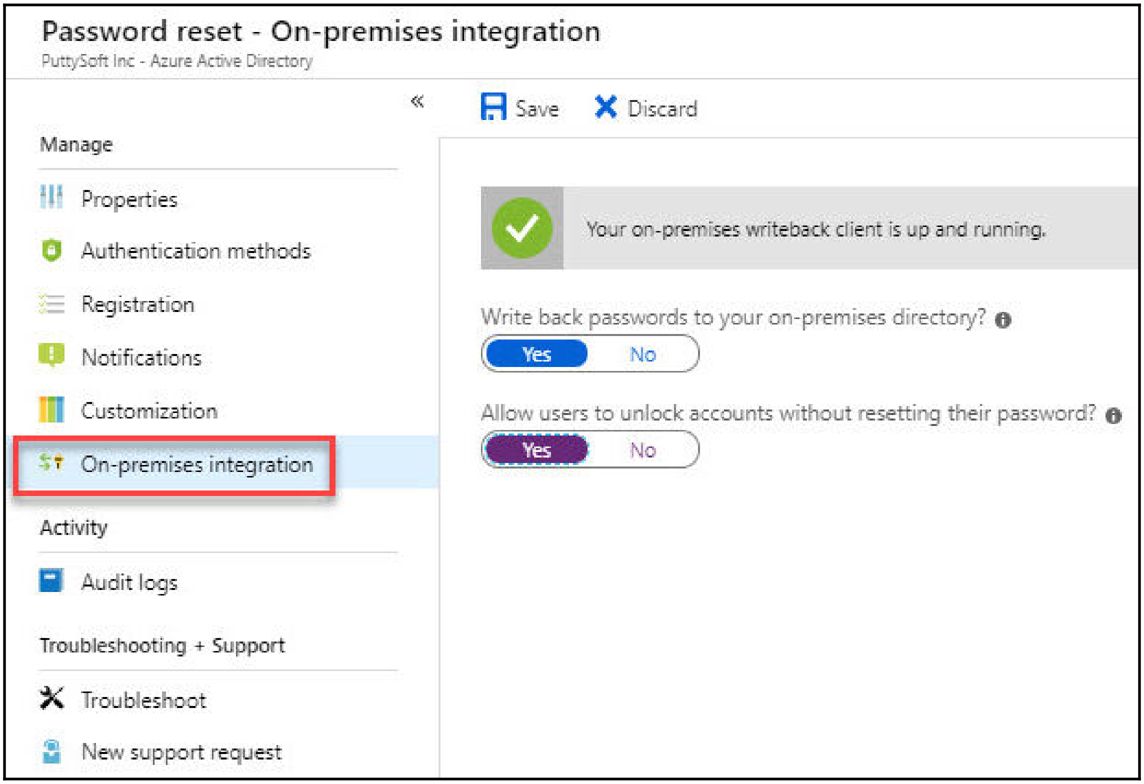
☑ All services (24)
□ B2B/B2C (6)
□ 3rd Party Integration (4)
□ Collaboration (1)
□ Access Control (2)
□ User Authentication (2)
□ Monitoring & Reporting (2)
□ Identity Security & Protection (3)

B2C - Consumer Identity Management - B2B/B2C
March 20, 2019
Identity Experience Framework and custom policy support in Azure Active Directory B2C is now available (GA)

Enterprise Apps - 3rd Party Integration
March 20, 2019

Password reset in the Azure portal

4. In the **password reset** blade, under **Manage**, select **On-premises integration**. Set the option for **Write back passwords to your on-premises directory?** to **Yes** and set the option for **Allow users to unlock accounts without resetting their password?** to **Yes** as follows:



Password reset - On-premises integration

PuttySoft Inc - Azure Active Directory

Your on-premises writeback client is up and running.

Write back passwords to your on-premises directory? Yes [✓] No

Allow users to unlock accounts without resetting their password? Yes [✓] No

Enabling password writeback

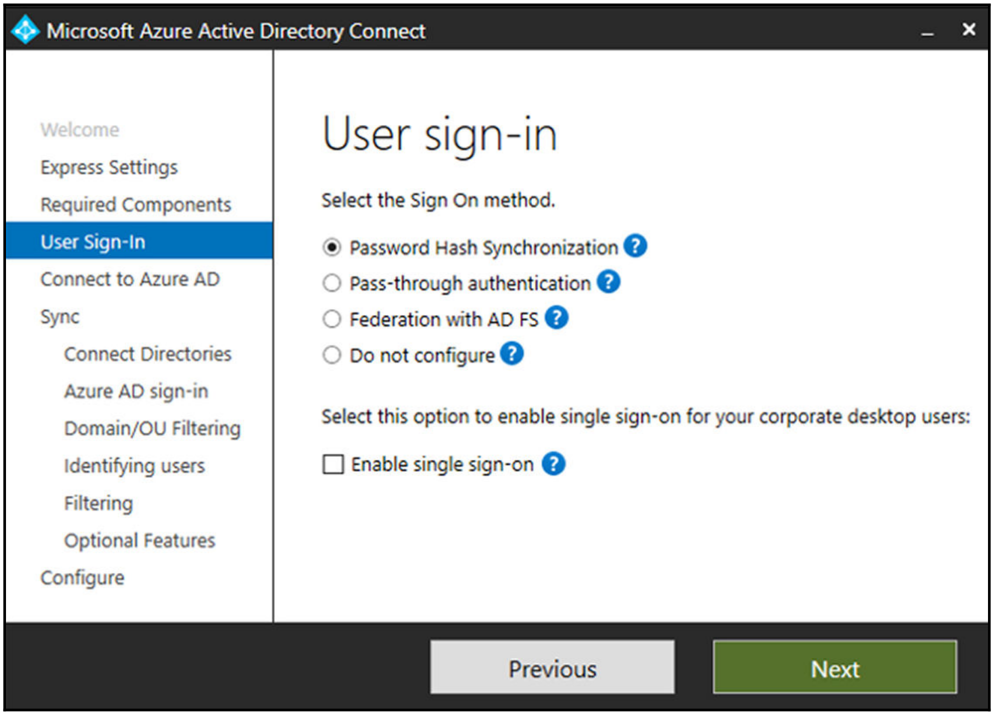
5. Click **Save**.

We have now completely configured password writeback in Azure AD Connect and the Azure portal. In the next section, we are going to cover how to manage password sync.

Password sync

In this last section of this chapter, we are going to cover password sync. We installed Azure AD Connect using the **Express Settings** option. Password hash synchronization is automatically enabled if you use this option.

If you install Azure AD Connect using the custom settings, password hash synchronization is available on the **User sign-in** screen and you can enable it there, as shown in the following screenshot:



User sign-in

Select the Sign On method.

● Password Hash Synchronization
○ Pass-through authentication
○ Federation with AD FS
○ Do not configure

Select this option to enable single sign-on for your corporate desktop users:

□ Enable single sign-on

Enabling password hash synchronization during installation

Summary

In this chapter, we covered the second part of the *Managing Identities* objective. We covered Azure AD Connect and you've learned how to install and manage it after installation. We also covered how to enable password writeback and password hash synchronization.

In the next chapter, we will cover the third and final part of this exam objective. In this chapter, we will cover how to implement **Multi-Factor Authentication** (**MFA**) in Azure.

Questions

Answer the following questions to test your knowledge of the information in this chapter. You can find the answers in the *Assessments* section at the end of this book:

1. If you use the **Express Settings** when installing Azure AD Connect, password hash synchronization is disabled by default.
   - Yes
   - No
2. When you want to enable password sync, you only have to do this inside the Azure portal.
   - Yes
   - No
3. If the on-premises Forest name doesn't match one of the Azure AD custom domain names, you cannot install Azure AD Connect.
   - Yes
   - No