



Managing Azure AD Organization

Managing cloud solutions (Lovely Professional University)



Scan to open on Studocu

Managing Azure AD Organization, Users, Groups, and Roles

RBAC (Role-Based Access Control)



Name: Sandeep Chouhan

Registration Number: 12113018

Section: K21KR


Create the Senior Admins group with the user account Joseph Price as its member (the Azure portal).

- Task 1: Use the Azure portal to create a user account for Joseph Price

In this task, you will create a user account for Joseph Price.

1. Start a browser session and sign-in to the Azure portal <https://portal.azure.com/>.
- Note: Sign in to the Azure portal using an account that has the Owner or Contributor role in the Azure subscription you are using for this lab and the Global Administrator role in the Microsoft Entra tenant associated with that subscription.
2. In the Search resources, services, and docs text box at the top of the Azure portal page, type Microsoft Entra ID and press the Enter key.
3. On the Overview blade of the Microsoft Entra ID tenant, in the Manage section, select Users, and then select + New user.
4. On the New User blade, ensure that the Create user option is selected, and specify the following settings:
5. Click on the copy icon next to the **User name** to copy the full user.
6. Ensure that the **Auto-generate** password is selected, select the **Show password** checkbox to identify the automatically generated password. You would need to provide this password, along with the user name to Joseph.
7. Click **Create**.

Basic info



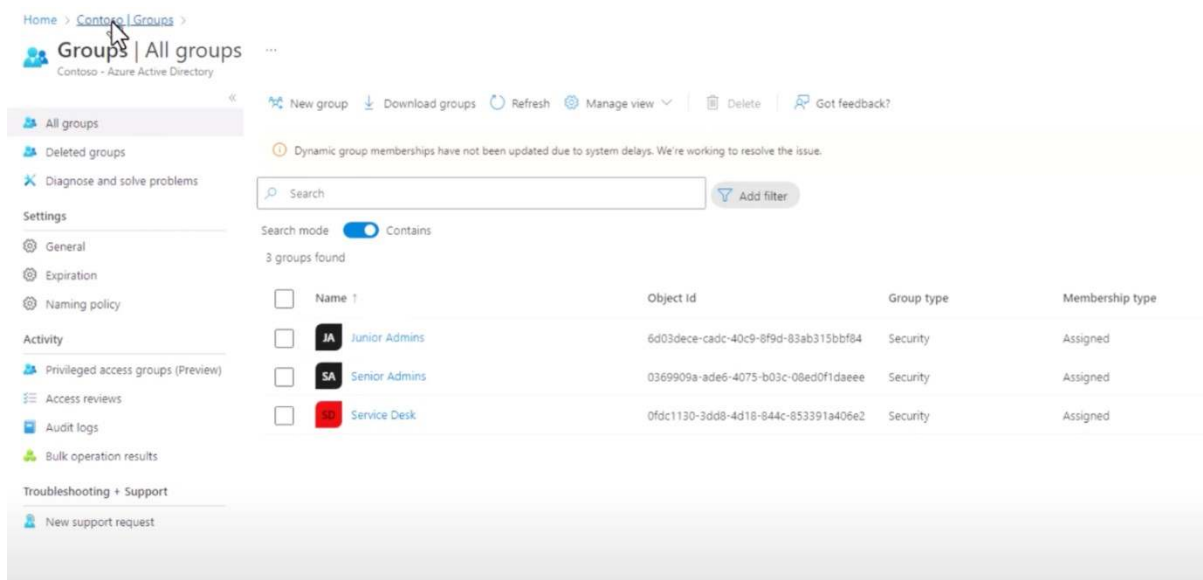
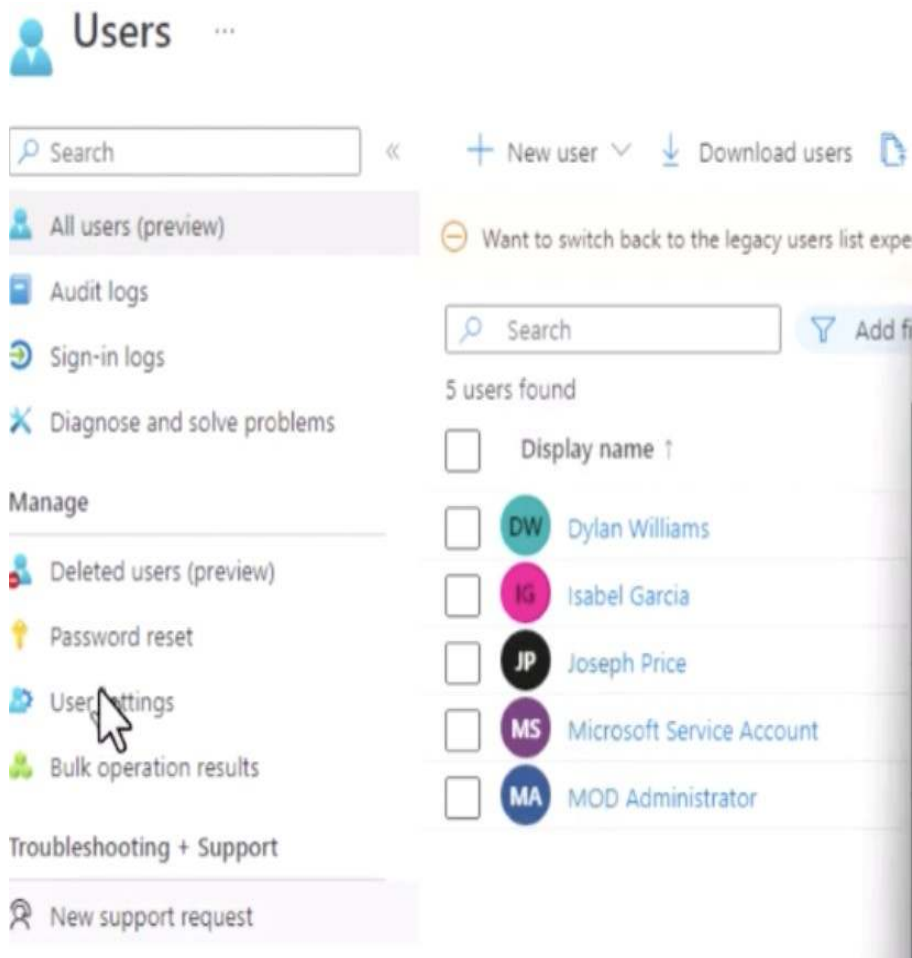
Joseph Price

Joseph@yashkarn3133gmail.onmicrosoft.com

Member

| | | | |
|---------------------|--|-------------------|---|
| User principal name | Joseph@yashkarn3133gmail.onmicrosoft.com | Group memberships | 0 |
| Object ID | 14621cea-b9e8-4c71-9d13-f336f6c6e48e | Applications | 0 |
| Created date time | Feb 7, 2025, 10:27 AM | Assigned roles | 0 |
| User type | Member | Assigned licenses | 0 |
| Identities | yashkarn3133gmail.onmicrosoft.com | | |

My Feed



Create the Junior Admins group with the user account Isabel Garcia as its member (PowerShell).

- In this task, you will create the *Senior Admins* group, add the user account of Isabel Gracia to the group, and configure it as the group owner.
1. In the Azure portal, navigate back to the blade displaying your Microsoft Entra ID tenant.
 2. In the Manage section, click Groups, and then select + New group.
 3. On the New Group blade, specify the following settings (leave others with their default values):
 4. Click the **No owners selected** link, on the **Add owners** blade, select **Joseph Price**, and click **Select**.
 5. Click the **No members selected** link, on the **Add members** blade, select **Joseph Price**, and click **Select**.
 6. Back on the **New Group** blade, click **Create**.

```
Administrator: Windows PowerShell
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> Install-Module AzureAD

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet provider must be
available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\Admin\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running
'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and import the NuGet
provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its InstallationPolicy value by running
the Set-PSRepository cmdlet. Are you sure you want to install the modules from 'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): a

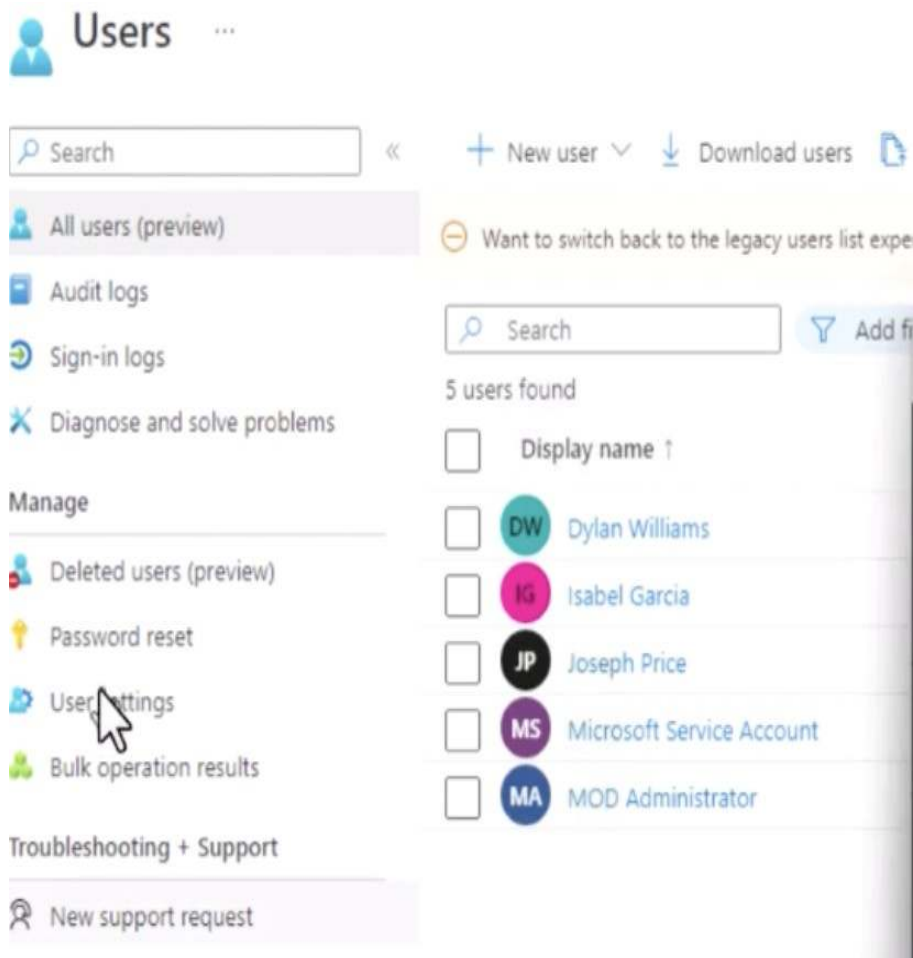
PS C:\Windows\system32> Import-Module AzureAD
PS C:\Windows\system32> $passwordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile
PS C:\Windows\system32> $passwordProfile.Password = 'Pa55w.rd1234'
PS C:\Windows\system32> Connect-AzureAD

Account                                Environment TenantId                                TenantDomain                                AccountType
-----                                -
admin@M365x66430656.onmicrosoft.com AzureCloud 4924f825-e219-4b73-9969-64ab5b7bb2dd M365x66430656.onmicrosoft.com User

PS C:\Windows\system32> $domainName = ((Get-AzureAdTenantDetail).VerifiedDomains)[0].Name
PS C:\Windows\system32> New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@domainN
ame" -AccountEnabled $true -MailNickName 'Isabel'

ObjectId                                DisplayName UserPrincipalName                                UserType
-----                                -
8bcb2cc2-d844-4e55-91cd-34799703f77e Isabel Garcia Isabel@M365x66430656.onmicrosoft.com Member

PS C:\Windows\system32> Get-AzureADUser
```



```

Administrator: Windows PowerShell
PS C:\Windows\system32> Get-AzureADUser

ObjectId                DisplayName                UserPrincipalName          UserType
-----
4412301a-67a2-4547-b853-50a867e8eb30 MOD Administrator         admin@M365x66430656.onmicrosoft.com Member
8bcb2cc2-d844-4e55-91cd-34799703f77e Isabel Garcia              Isabel@M365x66430656.onmicrosoft.com Member
d63bebec-1611-429f-b4da-ff297a5ecbf6 Joseph Price               Joseph@M365x66430656.onmicrosoft.com Member
83be8533-3c85-408f-b680-661b56c608f6 Microsoft Service Account ms-serviceaccount@M365x66430656.OnMicrosoft.com Member

PS C:\Windows\system32> New-AzureADGroup -DisplayName 'Junior Admins' -MailEnabled $false -SecurityEnabled $true -MailNickName JuniorAdmins

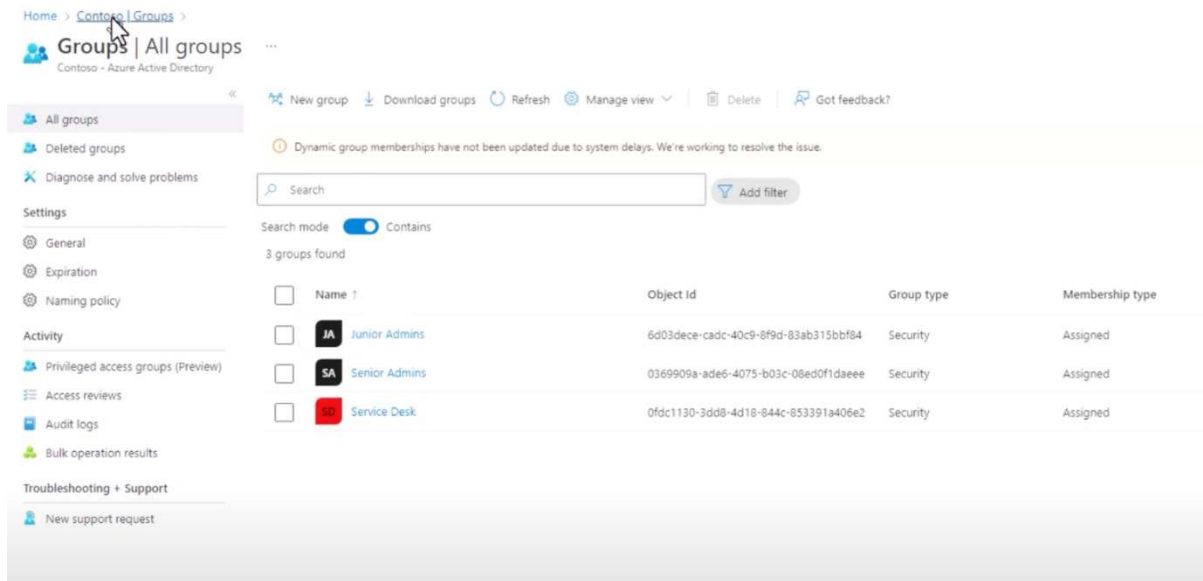
ObjectId                DisplayName                Description
-----
6d03dece-cadc-40c9-8f9d-83ab315bbf84 Junior Admins

PS C:\Windows\system32> Get-AzureADGroup

ObjectId                DisplayName                Description
-----
0369909a-ade6-4075-b03c-08ed0f1daeee Senior Admins
6d03dece-cadc-40c9-8f9d-83ab315bbf84 Junior Admins

PS C:\Windows\system32> $user = (Get-AzureADUser -Filter "MailNickName eq 'Isabel'").objectId
PS C:\Windows\system32> $group = (Get-AzureADGroup -SearchString "Jun").objectId
PS C:\Windows\system32> Add-AzureADGroupMember -ObjectId $group -RefObjectId $user
PS C:\Windows\system32> Get-AzureADGroupMember -ObjectId $group

ObjectId                DisplayName                UserPrincipalName          UserType
-----
8bcb2cc2-d844-4e55-91cd-34799703f77e Isabel Garcia              Isabel@M365x66430656.onmicrosoft.com Member
  
```

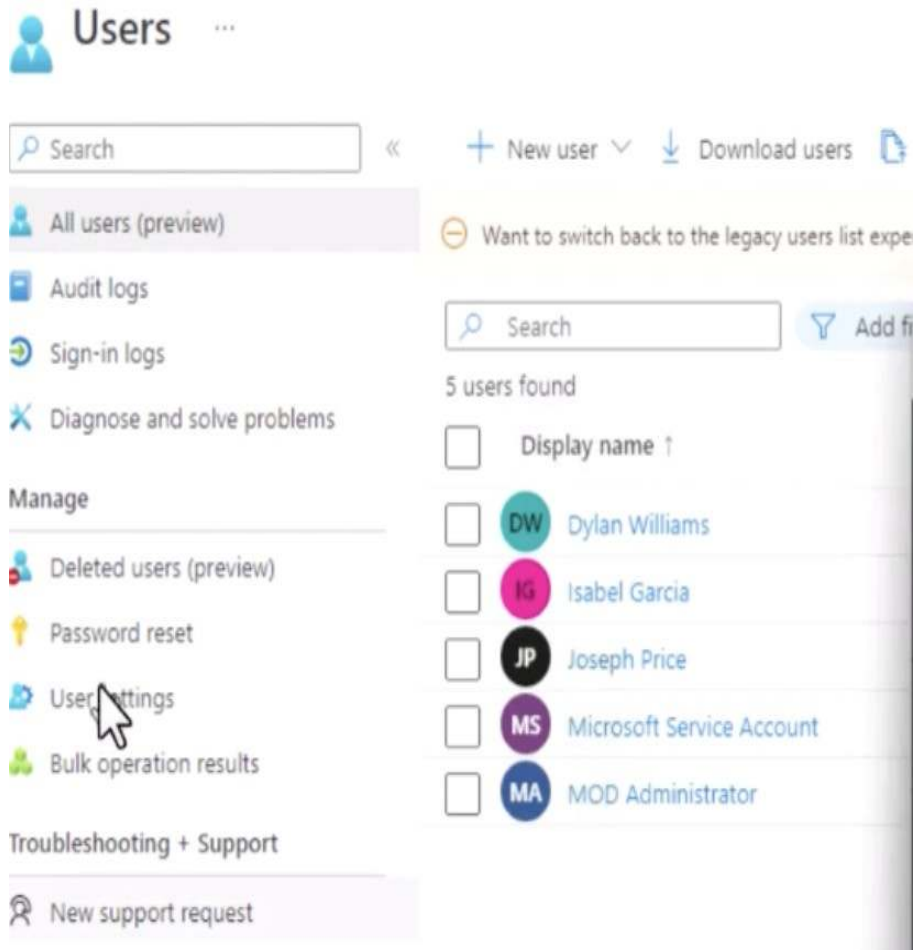
Create the Service Desk group with the user Dylan Williams as its member (Azure CLI).

- Task 1: Use Azure CLI to create a user account for Dylan Williams.
 - In this task, you will create a user account for Dylan Williams.
1. In the drop-down menu in the upper-left corner of the Cloud Shell pane, select Bash, and, when prompted, click Confirm.
 2. In the Bash session within the Cloud Shell pane, run the following to identify the name of your Microsoft Entra tenant:
 3. `DOMAINNAME=$(az ad signed-in-user show --query 'userPrincipalName' | cut -d '@' -f 2 | sed 's/\\/\\/')`
 4. In the Bash session within the Cloud Shell pane, run the following to create a user, Dylan Williams. Use *yourdomain*.
 5. `az ad user create --display-name "Dylan Williams" --password "Pa55w.rd1234" --user-principal-name Dylan@$DOMAINNAME`
 6. In the Bash session within the Cloud Shell pane, run the following to list Microsoft Entra ID user accounts (the list should include user accounts of Joseph, Isabel, and Dylan)
 7. `az ad user list --output table`

```

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.
yash [ ~ ]$ az ad user create --display-name "Dylan Williams" --user-principal-name "dylan@yashkarn3133gmail.onmicrosoft.com" --password "Y@sh3133"
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity",
  "businessPhones": [],
  "displayName": "Dylan Williams",
  "givenName": null,
  "id": "c7b75ad2-1108-4936-8052-4da59a300b5e",
  "jobTitle": null,
  "mail": null,
  "mobilePhone": null,
  "officeLocation": null,
  "preferredLanguage": null,
  "surname": null,
  "userPrincipalName": "dylan@yashkarn3133gmail.onmicrosoft.com"
}
yash [ ~ ]$

```



Users ...

Search < + New user ▾ ⬇ Download users 📄

All users (preview) ⚠ Want to switch back to the legacy users list experience

Audit logs

Sign-in logs

Diagnose and solve problems

Manage

Deleted users (preview)

Password reset

User settings

Bulk operation results

Troubleshooting + Support

New support request

Search Add filters

5 users found

☐ Display name ↑

☐ DW Dylan Williams

☐ IG Isabel Garcia

☐ JP Joseph Price

☐ MS Microsoft Service Account

☐ MA MOD Administrator

Home > Contoso | Groups

Groups | All groups

Contoso - Azure Active Directory

- All groups
- Deleted groups
- Diagnose and solve problems
- Settings
 - General
 - Expiration
 - Naming policy
- Activity
 - Privileged access groups (Preview)
 - Access reviews
 - Audit logs
 - Bulk operation results
- Troubleshooting + Support
 - New support request

New group Download groups Refresh Manage view Delete Got feedback?

Dynamic group memberships have not been updated due to system delays. We're working to resolve the issue.

Search Add filter

Search mode Contains

3 groups found

| <input type="checkbox"/> | Name | Object id | Group type | Membership type |
|--------------------------|------------------|--------------------------------------|------------|-----------------|
| <input type="checkbox"/> | JA Junior Admins | 6d03dece-cadc-40c9-8f9d-83ab315bbf84 | Security | Assigned |
| <input type="checkbox"/> | SA Senior Admins | 0369909a-ade6-4075-b03c-08ed0f1daeee | Security | Assigned |
| <input type="checkbox"/> | SD Service Desk | 0fdc1130-3dd8-4d18-844c-853391a406e2 | Security | Assigned |

Home > Contoso | Roles and administrators

Roles and administrators | All roles

Contoso - Azure Active Directory

- All roles
- Diagnose and solve problems
- Activity
 - Access reviews
 - Audit logs
- Troubleshooting + Support
 - New support request

New custom role Delete custom role Download assignments Refresh Preview features Got feedback?

Get just-in-time access to a role when you need it using PIM. Learn more about PIM.

Your Role: Global administrator

Administrative roles

Administrative roles are used for granting access for privileged actions in Azure AD. We recommend using these built-in roles for delegating access to manage broad application configuration permissions without granting access to manage other parts of Azure AD not related to application configuration. Learn more.

Learn more about Azure AD role-based access control

Search by name or description Add filters

| Role | Description | Type |
|---|---|----------|
| <input type="checkbox"/> Application administrator | Can create and manage all aspects of app registrations and enterprise apps. | Built-in |
| <input type="checkbox"/> Application developer | Can create application registrations independent of the 'Users can register applications' setting. | Built-in |
| <input type="checkbox"/> Attack payload author | Can create attack payloads that an administrator can initiate later. | Built-in |
| <input type="checkbox"/> Attack simulation administrator | Can create and manage all aspects of attack simulation campaigns. | Built-in |
| <input type="checkbox"/> Attribute assignment administrator | Assign custom security attribute keys and values to supported Azure AD objects. | Built-in |
| <input type="checkbox"/> Attribute assignment reader | Read custom security attribute keys and values for supported Azure AD objects. | Built-in |
| <input type="checkbox"/> Attribute definition administrator | Define and manage the definition of custom security attributes. | Built-in |
| <input type="checkbox"/> Attribute definition reader | Read the definition of custom security attributes. | Built-in |
| <input type="checkbox"/> Authentication administrator | Has access to view, set, and reset authentication method information for any non-admin user. | Built-in |
| <input type="checkbox"/> Authentication policy administrator | Can create and manage all aspects of authentication methods and password protection policies. | Built-in |
| <input type="checkbox"/> Azure AD joined device local administrator | Users assigned to this role are added to the local administrators group on Azure AD-joined devices. | Built-in |
| <input type="checkbox"/> Azure DevOps administrator | Can manage Azure DevOps organization policy and settings. | Built-in |

Home > Contoso | Roles and administrators > Roles and administrators | All roles > Azure DevOps administrator

Azure DevOps administrator | Assignments

All roles

- Diagnose and solve problems
- Manage
 - Assignments
 - Description
- Activity
 - Bulk operation results
- Troubleshooting + Support
 - New support request

Add assignments Remove assignments Download assignments Refresh Manage in PIM Got feedback?

You can also assign built-in roles to groups now. Learn More

Search by name Type All

| Name | Username | Type | Scope |
|---|--------------------------------------|------|-----------|
| <input type="checkbox"/> Joseph Price | Joseph@m365ad6430656.onmicrosoft.com | User | Directory |
| <input type="checkbox"/> Dylan Williams | Dylan@m365ad6430656.onmicrosoft.com | User | Directory |

Successfully added assignment
Successfully added assignment: Joseph Price