

2. Configuration

The following pages provide guidance on the initial setup and how administration and granular role assignment are achieved.

- [End User Scopes](#)
- [Admin Scopes](#)
- [Role Assignment](#)

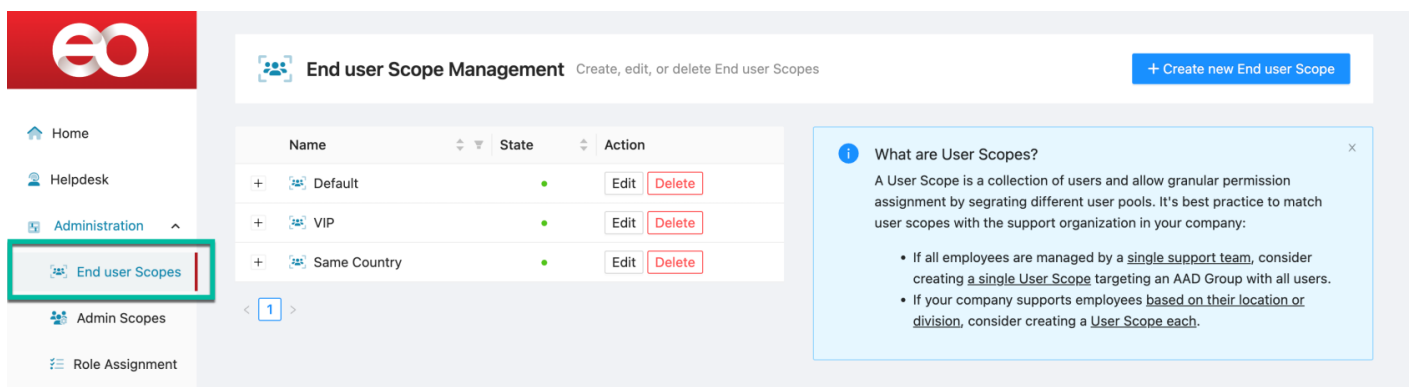
End User Scopes

An *End User Scope* is a collection of users that allows EndpointOps the assignment of granular permissions by segregating different user pools. It's best practice to match *end user scopes* with the support organization set up of your company. E.g.:

- If a single helpdesk team supports all employees, consider creating a single *End User Scope* targeting an AAD Group with all users.
- If your company supports employees based on the employee's location or division, consider creating a User Scope for each.

Required Permissions

End User Scopes are created and managed by EndpointOps Administrators.



| Name | State | Action |
|----------------|-------|-------------|
| + Default | ● | Edit Delete |
| + VIP | ● | Edit Delete |
| + Same Country | ● | Edit Delete |

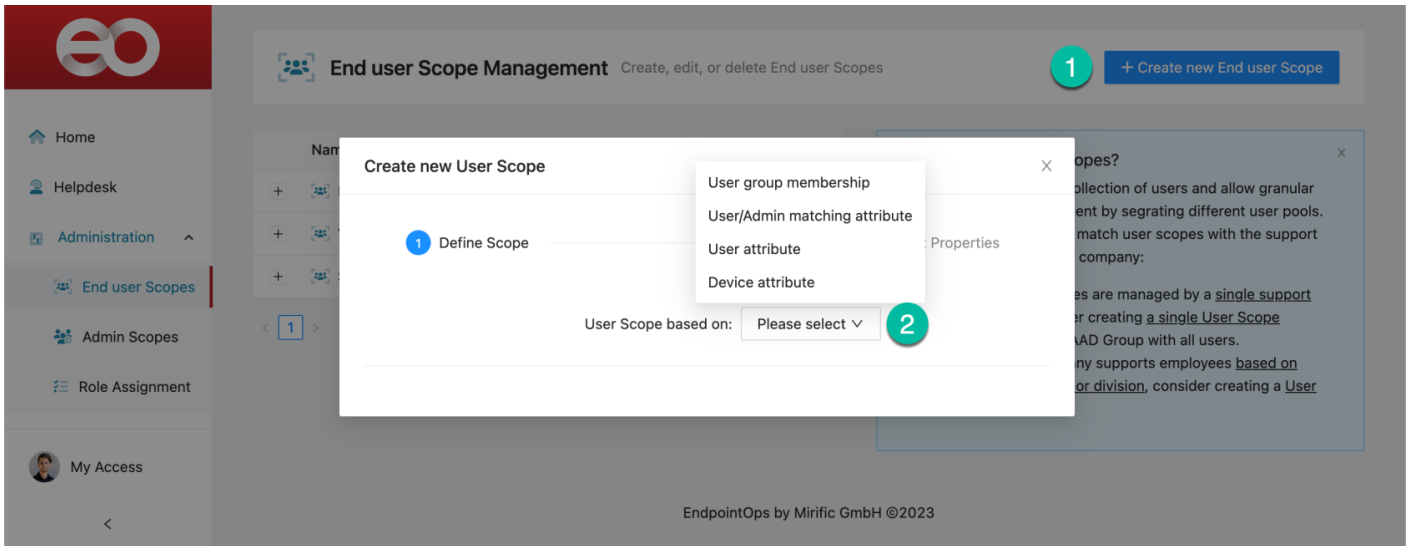
What are User Scopes?

A User Scope is a collection of users and allow granular permission assignment by segregating different user pools. It's best practice to match user scopes with the support organization in your company:

- If all employees are managed by a single support team, consider creating a single User Scope targeting an AAD Group with all users.
- If your company supports employees based on their location or division, consider creating a User Scope each.

Types of End User Scopes

EndpointOps supports different types of *End User Scopes* to support a wide range of setups.



Type: User group membership

A simple way to set up *End User Scopes* is relying on an account's membership to an AAD Group, Administrative Unit(AU), or Global Azure Role. When selecting multiple AAD Groups/AUs, the membership of any AAD Group/AU will assign the user to the respective *End User Scope*.

1. Type the name of an AAD Group, Administrative Unit, or Global Azure Role
2. Select an entry from the list
3. Selected objects will appear on the right side. Undo the selection with the **Remove** Button

Type: User/Admin matching attribute

This option is recommended to set up **country-, site-, or division-based** *End User Scope*.

Instead of manually creating an AAD Group, a single "User/Admin matching attribute"-*End User Scope* can be created. Such an *End User Scope* with the configuration of "Country" will dynamically assign the *End User Scope* to a user if the Helpdesk supporter's country property matches the end user's country property. Supported properties are Department, Country, State, City, and Postal code.

The Azure Active Directory Account properties are used for this assignment:

Home

Create new User Scope

1 Define Scope 2 Set Properties

User Scope based on: Matching user attribute

Matching Attribute: Department

1 How does this work? 2 Matching user scopes are assigned to the user. 3 The helpdesk operator is assigned to the user. 4 The end user is part of the user scope. 5 The user attribute is also set to the user scope. Then perform actions against this user and their devices, given that permissions are assigned to the admin scope against this end user scope.

Department

Country

State

City

Postal code

Next

On EndpointOps: Helpdesk > Search for a user > AAD Account Information:

AAD User Attributes for pascal.pfammatter@mirific.ch

Display options: M L

Technical Account Information

User principal name

User type

Account enabled

Created date time

ID

Mail nickname

Preferred language

Proxy addresses

Refresh tokens valid from date time

Sign in sessions valid from date time

Usage location

Security identifier

Name

Display name

Given name

Surname

Mail

Mobile phone

User Location

Office location

Street address

City

State or province

ZIP or postal code

Country or region

Work Information

Company name

Department

Job title

Employee id

Employee hire date

Employee type

On the Azure Portal:

Microsoft Azure Search resources, services, and docs (G-V)

Home > Users >

Pascal Pfammatter

User

Search Edit properties Delete Refresh Reset password Revoke sessions Manage view Got feedback?

Overview Audit logs Sign-in logs Diagnose and solve problems Manage Custom security attributes Assigned roles Administrative units Groups Applications Licenses Azure role assignments Authentication methods Troubleshooting + Support New support request

Overview Monitoring Properties

Identity

Display name

First name

Last name

User principal name

Object ID

Identities

User type

Creation type

Created date time

Last password change date time

Invitation state

External user state change date ...

Assigned licenses

Password policies

Password profile

Preferred language

Sign in sessions valid from date ...

Authorization info

Job Information

Job title

Company name

Department

Contact Information

Street address

City

State or province

ZIP or postal code

Country or region

Business phone

Mobile phone

Other emails

Proxy addresses

Fax number

IM addresses

Mail nickname

Parental controls

Age group

Consent provided for minor

Legal age group classification

Settings

Account enabled

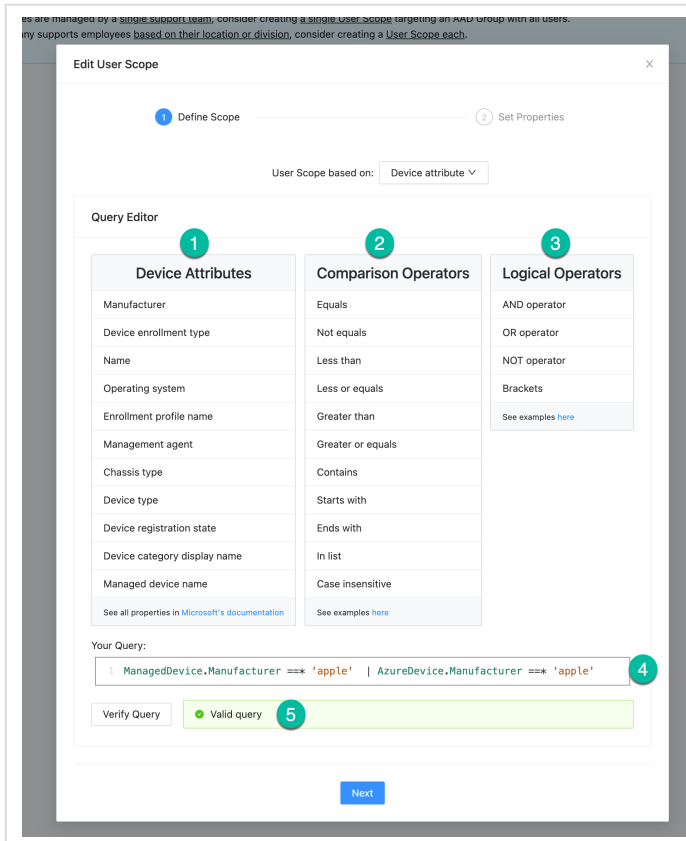
Usage location

Preferred data location

Type: Device Attribute

This option is recommended to set up to assign an *End User Scope* to user-less devices.

When selecting this type, a Query editor will appear.

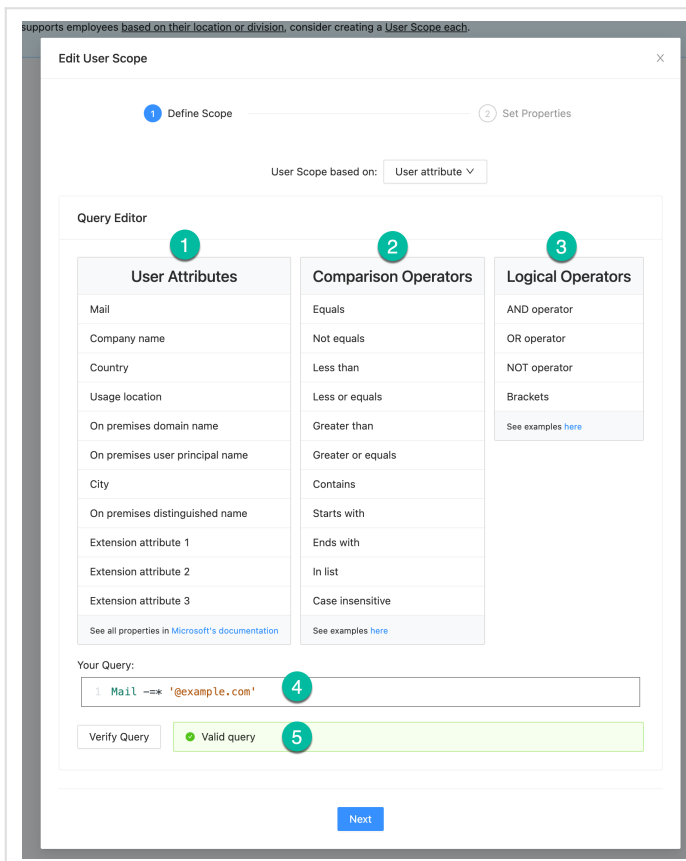


1. Select one of the device attributes you want to test against. All Intune-device attributes are available from the *ManagedDevice* object, and all Azure-device attributes from the *AzureDevice* attribute. Review the examples for additional guidance. Note the URL at the end of the list for all available attributes.
2. Select the desired *Comparison Operator* to complete your query. Note that you can make your query case insensitive by adding an *** character after the operator (eg. *attribute == 'sOmE vAlUe'*)
3. You can combine multiple verifications with a logical operator
4. Double-check or complete your query.
5. Verify the validity of your query or review the errors that appear.

Once valid, you can proceed with the *Next* button

Type: User Attribute

Special use cases may require you to create a user attribute query. When selecting this type, a Query editor will appear.



1. Select one of the user attributes you want to test against. Review the examples for additional guidance. Note the URL at the end of the list for all available attributes.
2. Select the desired *Comparison Operator* to complete your query. Note that you can make your query case insensitive by adding an *** character after the operator (eg. *attribute == 'sOmE vAlUe'*)
3. You can combine multiple verifications with a logical operator
4. Double-check or complete your query.
5. Verify the validity of your query or review the errors that appear.

Once valid, you can proceed with the *Next* button

End User Scope Properties

The second step of any type of *End User Scope* allows you to set the properties.

The screenshot shows the 'Edit User Scope' dialog box. At the top, there is a progress bar with two steps: 'Define Scope' (completed) and 'Set Properties' (active). Below the progress bar, there are three input fields: 'User Scope Name' with the value 'Default', 'Priority' with the value '0', and 'State' with a radio button selected for 'Enabled'. At the bottom, there are two buttons: 'Previous' and 'Next'. The 'Next' button is highlighted in blue. Red circles with numbers 1, 2, 3, and 4 are overlaid on the 'User Scope Name', 'Priority', 'State', and 'Next' button respectively.

1. The **name** of the *End User Scope* is visible to Helpdesk operators when searching for a user or device. Choose a unique and self explanatory name.
2. Users and devices might be members of multiple *End User Scopes*. If the **Priority** of a user's or device's *End User Scope* is elevated, the user will only be part of the *End User Scopes* with the highest priority. Following this logic you can achieve exclusions for special cases. Imagine an *End User Scope* matching all users with the name "Default" and priority of 0, and second *End User Scope* called "VIP users" for a subset of users with a priority of 1 and higher. If a user is associated with the *End User Scope* "VIP users", they will no longer be member of the "Default" *End User scope* due to the elevated priority of the "VIP users" *End User Scope*. Depending on your use case this will allow you to assign different set of permissions to the admin scopes (this could be more permissions, less permissions, or grant specific access to another Admin scope)
3. **Enabled** *End User Scopes* will be used in Endpoint Ops, whereas **Disabled** *End User Scopes* are omitted.
4. Proceed with the **Next** button to Save your *End User Scope*.

Edit or delete End User Scopes

End User Scopes can be updated or deleted at any point. Simply use the **Edit** or **Delete** button on the respective *End User Scope*.



End user Scope Management Create, edit, or delete End user Scopes

[+ Create new End user Scope](#)

- Home
- Helpdesk
- Administration
- End user Scopes**
- Admin Scopes
- Role Assignment

| Name | State | Action |
|-----------------|-------|---|
| + Default | ● | Edit Delete |
| + VIP | ● | Edit Delete |
| + Same Country | ● | Edit Delete |
| + Apple devices | ● | Edit Delete |

< 1 >

What are User Scopes?

A User Scope is a collection of users and allow granular permission assignment by segregating different user pools. It's best practice to match user scopes with the support organization in your company:

- If all employees are managed by a single support team, consider creating a single User Scope targeting an AAD Group with all users.
- If your company supports employees based on their location or division, consider creating a User Scope each.

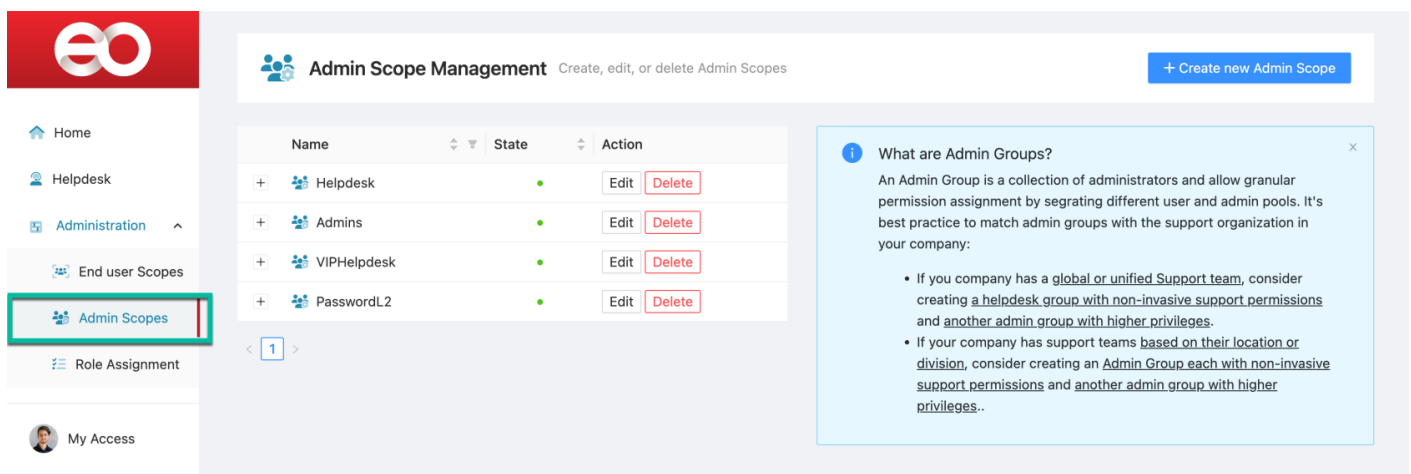
Admin Scopes

An *Admin Scope* is a collection of administrators and allows granular permission assignment by segregating different user and admin pools. It's best practice to match admin groups with the support organization in your company:

- If your company has a global or unified Support team, consider creating a helpdesk group with non-invasive support permissions and another admin group with higher privileges.
- If your company has support teams based on their location or division, consider creating an Admin Group, each with non-invasive support permissions and another admin group with higher privileges.

Required Permissions

Admin Scopes are created and managed by EndpointOps Administrators.



The screenshot displays the 'Admin Scope Management' interface. The left sidebar contains navigation options: Home, Helpdesk, Administration (with a dropdown arrow), End user Scopes, **Admin Scopes** (highlighted with a red box), Role Assignment, and My Access. The main content area shows a table of Admin Scopes:

| Name | State | Action |
|---------------|-------|-------------|
| + Helpdesk | ● | Edit Delete |
| + Admins | ● | Edit Delete |
| + VIPHelpdesk | ● | Edit Delete |
| + PasswordL2 | ● | Edit Delete |

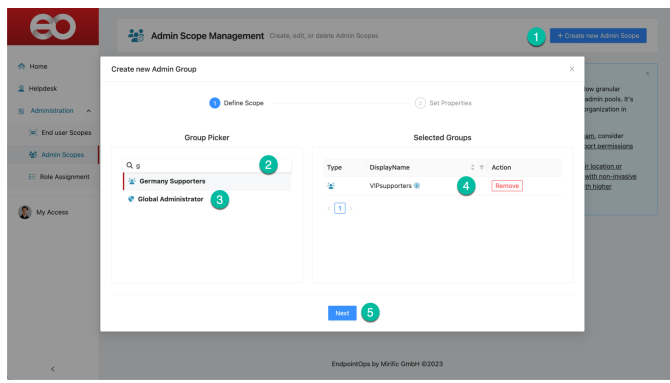
A blue tooltip titled 'What are Admin Groups?' is displayed on the right, containing the following text:

An Admin Group is a collection of administrators and allow granular permission assignment by segregating different user and admin pools. It's best practice to match admin groups with the support organization in your company:

- If you company has a global or unified Support team, consider creating a helpdesk group with non-invasive support permissions and another admin group with higher privileges.
- If your company has support teams based on their location or division, consider creating an Admin Group each with non-invasive support permissions and another admin group with higher privileges.

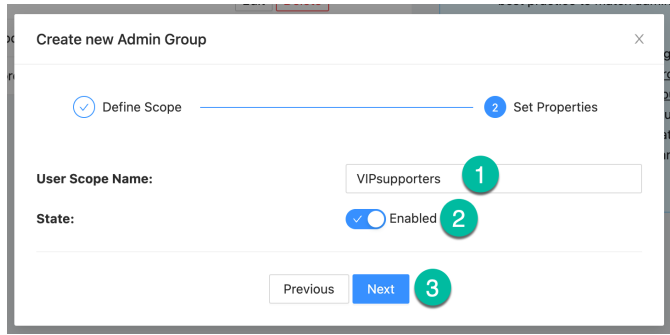
Admin Scope Creation

Admin Scopes follow a similar principle to the [End User Scopes](#), but they only support **User group membership** assignments.



To create a new *Admin Scope*:

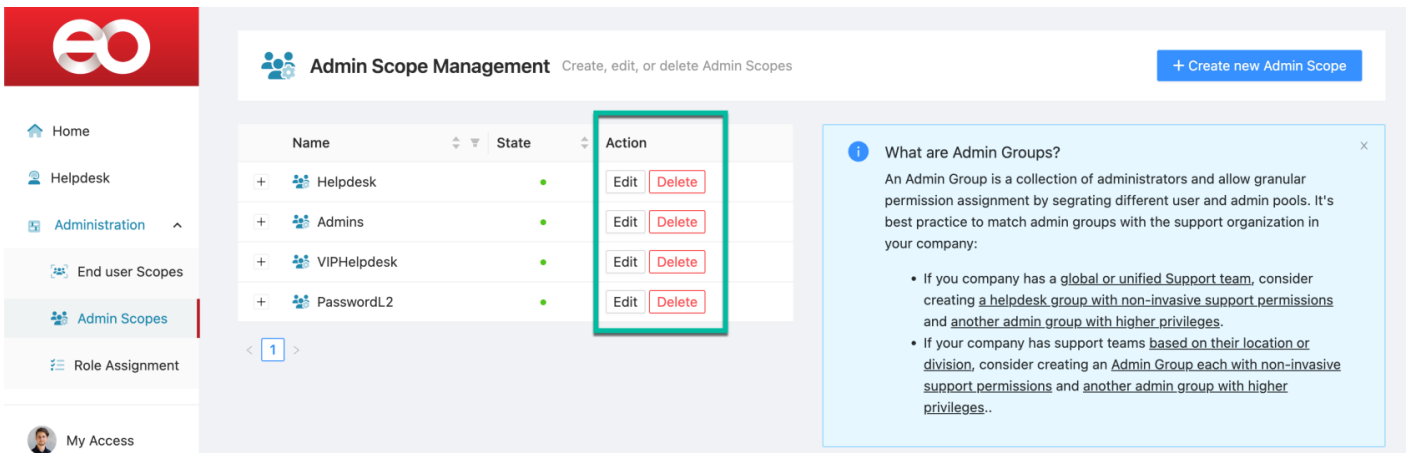
1. Click on **Create new Admin Scope**
2. Type the name of an AAD Group, Administrative Unit, or Global Azure Role. The membership of one of the groups is sufficient to become associated with an *Admin Scope*.
3. Select an entry from the list
4. Selected objects will appear on the right side. Undo the selection with the **Remove** Button
5. Use the **Next** button to proceed with the second step.



1. The **name** of the *Admin Scope* is visible to Helpdesk operators in the **My Access**
2. **Enabled Admin Scopes** will be used in Endpoint Ops, whereas **Disabled Admin Scopes are omitted**.
3. Proceed with the **Next** button to Save your *Admin Scope*.

Edit or delete Admin Scopes

Admin Scopes can be updated or deleted at any point. Simply use the **Edit** or **Delete** button on the respective *Admin Scope*.



Role Assignment

Once [End User Scopes](#) and [Admin Scopes](#) are configured, you can use these entities to assign permissions and allow Admins to perform activities against users.

Required Permissions

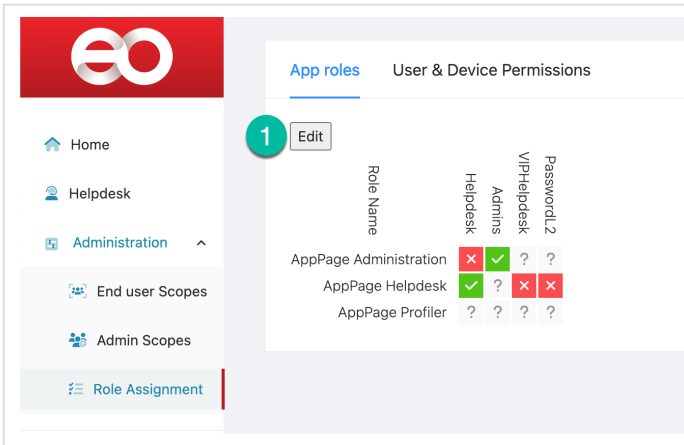
Role Assignments are created and managed by EndpointOps Administrators.

The screenshot shows the EndpointOps interface. On the left is a navigation sidebar with the following items: Home, Helpdesk, Administration (expanded), End user Scopes, Admin Scopes, and Role Assignment (highlighted with a red box). The main content area is titled 'User & Device Permissions' and contains an 'Edit' button and a table of permissions.

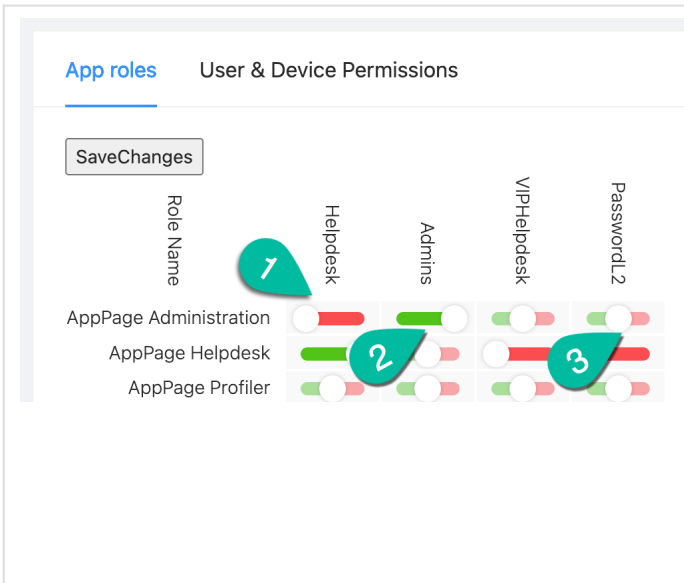
| Role Name | Helpdesk | Admins | VIPHelpdesk | PasswordL2 |
|------------------------|----------|--------|-------------|------------|
| AppPage Administration | ✗ | ✓ | ? | ? |
| AppPage Helpdesk | ✓ | ? | ✗ | ✗ |
| AppPage Profiler | ? | ? | ? | ? |

App role assignments



App roles allow Administrators and Helpdesk operators to access areas within EndpointOps. Granting *User & Device Permissions* to Helpdesk operators will not have any effect if they don't have the role to access the Helpdesk area.







1. Use the **Edit** button to switch into the editing view



Click on the slider to assign or un-assign the permission. The vertical axis lists all configured *Admin Sopes*. The horizontal access lists all *App Roles*

1. A red slider means that the permission is un-assigned.
( or )

2. A green slider means that the permission is assigned.
( or )

3. A slider is also considered un-assigned/unset if the slider is centered.
( or )

Click on **Save Changes** to persist your modifications.

User & Device Permissions

User & Device Permissions follow the same principle as the App roles but provide additional granularity.

App roles **User & Device Permissions** 1

Selected Admin Scope: Helpdesk 2

Save Changes 3 9

Helpdesk Permissions

Show Device Phone Number

Multifactor Authentication Methods

Reset User Password

Phone Authentication Method

Add Phone MFA method

Delete Phone MFA method







Temporary Access Passcode (TAP) Method

Create TAP for user

Delete existing TAP

Device Permissions

| | Default | VIP | Same Country | Apple devices |
|---|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Sync Device(any device) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Delete Azure Device(any device) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Retire Device(any device) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Retire Device(iOS, Any Configuration) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | n/a | n/a |
| Retire Device(Android, Any Configuration) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | n/a | n/a |
| Retire Device(macOS, Any Configuration) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | n/a | n/a |
| Retire Device(macOS + Supervised) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | n/a | n/a |
| Retire Device(macOS + Corporate) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | n/a | n/a |
| Retire Device(macOS + Personal) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | n/a | n/a |
| Retire Device(Windows, Any Configuration) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | n/a | n/a |
| Reset/Remove Device Passcode(any device) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Change Device Ownership to Personal(any device) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Change Device Ownership to Company(any device) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Wipe Device(any device) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Manage App Sign-out for device | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

1. Switch to the *User & Device Permissions* tab
2. Select the *Admin Scope* you want to view/edit the permission assignment
3. Use the **Edit** button to switch to the editing view
4. A green slider means that the permission is assigned. ( or )
5. A red slider means that the permission is un-assigned. ( or )
6. A slider is also considered un-assigned/unset if the slider is centered. ( or )
7. Device actions have an additional **Custom**-setting that allows for additional granularity. The base setting allows the assignment and un-assignment of the device action for "(any device)". Selecting **Custom** will enable 3 extra rows. There, you can assign/un-assign the permission based on the device's operating system (e.g. Allow retirement for iOS devices but prohibit the retirement of Android devices) for a given *Admin Scope* and *End User Scope*.
8. When using the **Custom** setting in a granular setting (like "MacOS, Any Configuration"), you can assign permissions even more granular based on the device's configuration. The three options are *Supervised*, *corporate-owned devices*, and *personal-owned devices*.
9. Use the **Save Changes** button to persist your modifications.