PROCESS MANUAL

Document Code: PM-SCIMI (AAD)

SCIM Integration

Azure Active Directory

FastTrack Software

Admin By Request

Table of Contents

Introduction

Admin By Request provides the ability to automatically synchronize data from your Identity Provider (IDP) to your Admin By Request User Portal according to the System for Cross-Domain Identity Management (SCIM) protocol, eliminating the need for manual entering and managing individual users on the Admin By Request side. This process manual provides a step-by-step guide on how to enable and configure the integration and provision users and groups in your User Portal with Azure AD.

Assumptions and Limitations

This implementation is targeted towards Admin By Request Portal users (i.e., company administrators who have access to the User Portal). It does not integrate with endpoint users.

The tasks described in this manual assume that the user has access to and is familiar with Azure Active Directory, the Admin By Request User Portal, and features of the software (e.g., Inventory, Requests, etc.).

Breakdown of Tasks

Seven tasks are covered in this manual:

1. Task A: Enable SCIM
2. Task B: Define Group-Based Roles
3. Task C: Create Azure Application
4. Task D: Set up Provisioning
5. Task E: Assign Users and Groups
6. Task F: Start Provisioning
7. Task G: View Data in User Portal

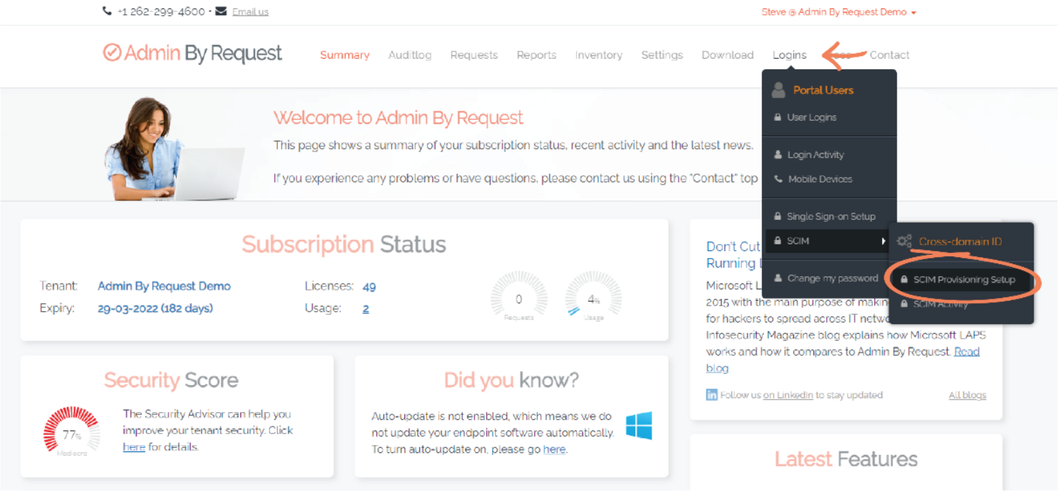
NOTE: Before you begin, we recommend you have a tab open in your Admin By Request User Portal and a second tab open in your Okta portal, as the tasks listed above switch back and forward frequently between the two.

Integration Tasks

Task A: Enable SCIM

The first task of this process involves enabling the integration in the Admin By Request User Portal.

1. In your Admin By Request User Portal, locate **Logins** in the top menu and navigate to **SCIM** > **SCIM Provisioning Setup**:



Welcome to Admin By Request

This page shows a summary of your subscription status, recent activity and the latest news.

If you experience any problems or have questions, please contact us using the "Contact" top

Subscription Status

Tenant: Admin By Request Demo
Expiry: 29-03-2022 (182 days)
Licenses: 49
Usage: 2

Don't Cut
Running
Microsoft L
2015 with the main purpose of makin
for hackers to spread across IT netwo
Infosecurity Magazine blog explains how Microsoft LAPS works and how it compares to Admin By Request. Read blog

Follow us on LinkedIn to stay updated All blogs

Security Score

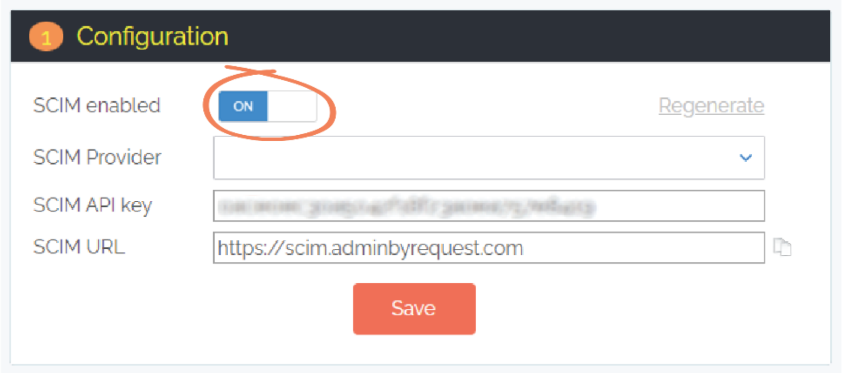
The Security Advisor can help you improve your tenant security. Click here for details.

Did you know?

Auto-update is not enabled, which means we do not update your endpoint software automatically. To turn auto-update on, please go here.

Latest Features

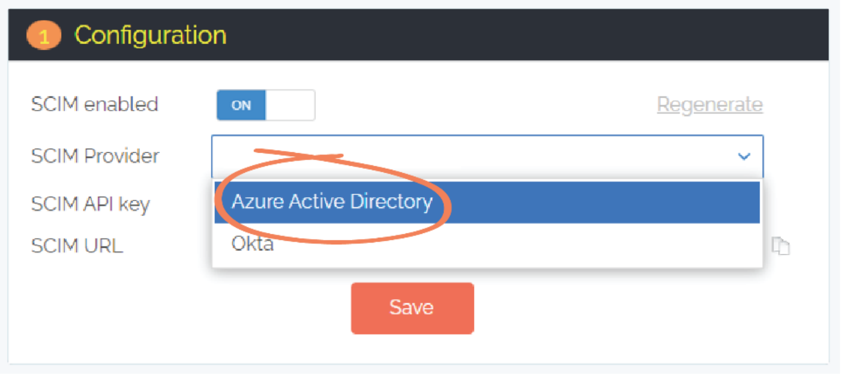
2. In section **1. Configuration**, toggle **SCIM enabled** to **ON**:



SCIM enabled: ON
SCIM Provider:
SCIM API key:
SCIM URL: https://scim.adminbyrequest.com

NOTE: This action generates an API key (blurred out in this document), which appears in the **SCIM API key** field. Using the API key is covered in Task D.

3. From the **SCIM Provider** drop-down menu, select **Azure Active Directory**:



4. Click **Save**:

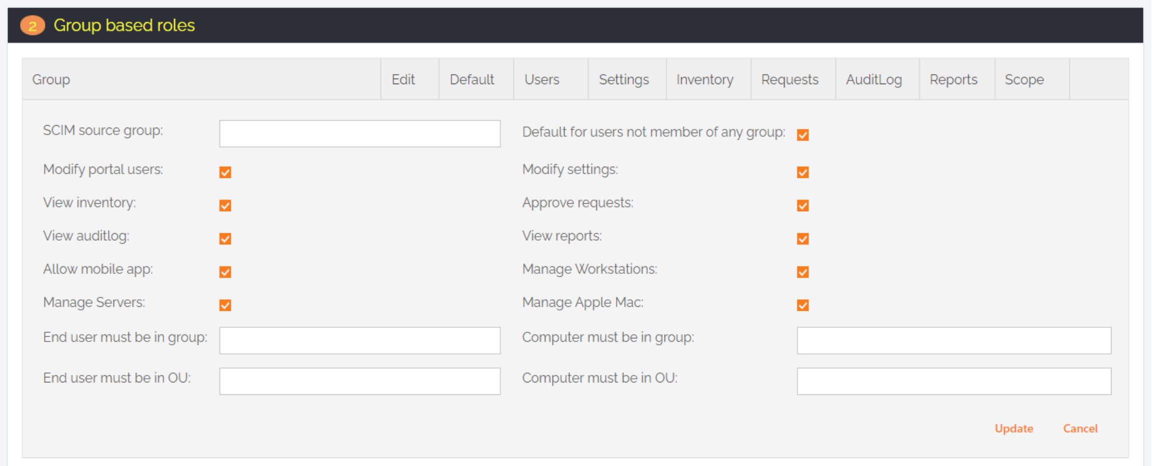
NOTE: Whenever the **Save** button is selected in the Admin By Request User Portal, a green icon appears next to the button when the action is successfully completed.

Task B: Define Group-Based Roles

Admin By Request's SCIM implementation provides the ability to define rules about what synchronized users have access to within the User Portal, based on their SCIM source group (i.e., their group in the IDP). This means that if you don't want all imported users having access to everything within the User Portal, you can create a Group-Based Role for each Azure AD group specifying exactly what the users in that group do and do not have access to. As soon as users are synchronized to Admin By Request, their designated permissions are applied.

If you do not create any Group-Based Roles, all synchronized users will have complete access to the User Portal. If a user belongs to multiple groups – all of which have Group-Based Roles defined – the first Role in the list will apply for that user. You can also create a Default Group-Based Role (covered in detail further down).

The filter options available for Group-Based Roles are as follows:



2 Group based roles

Group	Edit	Default	Users	Settings	Inventory	Requests	AuditLog	Reports	Scope

SCIM source group:		Default for users not member of any group:	☑
Modify portal users:	☑	Modify settings:	☑
View inventory:	☑	Approve requests:	☑
View auditlog:	☑	View reports:	☑
Allow mobile app:	☑	Manage Workstations:	☑
Manage Servers:	☑	Manage Apple Mac:	☑
End user must be in group:		Computer must be in group:	
End user must be in OU:		Computer must be in OU:	

- **SCIM source group** – This refers to the source group in the IDP (i.e., Azure AD). Whatever group is typed here needs to match the name of a group in Azure AD.

- **Default for users not member of any group** – When checked, the permissions defined for this Role become the 'default' permissions, applying to all users who aren't assigned any of the other Group-Based Roles defined for other groups. This checkbox can only be applied to one Group-Based Role.

The checkbox properties such as **Modify Settings**, **View Auditlog**, and **Manage workstations** refer to the various features in Admin By Request. If checked, users assigned the Role have access to the respective feature / can do the specified action.

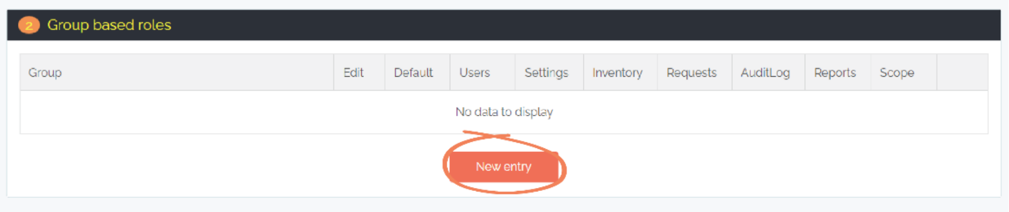
The four textboxes (**End user** and **Computer** etc.) are used to filter out end point data. Here you can specify IDP groups or OUs (Organizational Units) of end users and / or computers, so that Admin By Request Portal users assigned this Group-Based Role only have access to end users and / or computers that fall into those groups / OUs.

NOTE: You can specify multiple groups or OUs in these textboxes, separated by commas.

Before creating Group-Based Roles for specific groups, we recommend that you create a Default Role specifying permissions for the 'general' user; these are all synchronized users who are not members of any of the other groups that you have defined Group-Based Roles for. When synchronized, they get assigned the Default permissions in the User Portal (demonstrated in the example below).

Create Default Group-Based Role

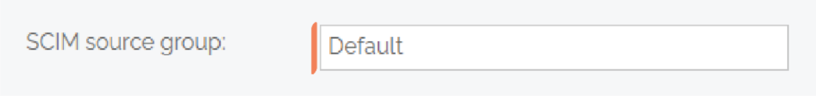
1. In the Admin By Request **SCIM Provisioning Setup** page, section **2. Group based roles**, select the **New entry** button:



2 Group based roles

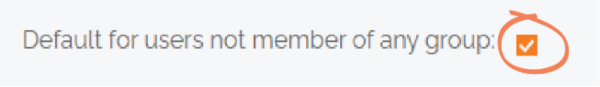
Group	Edit	Default	Users	Settings	Inventory	Requests	AuditLog	Reports	Scope
No data to display									

2. In the **SCIM source group** textbox, type the desired name for this group – this example uses *Default*:



SCIM source group: Default

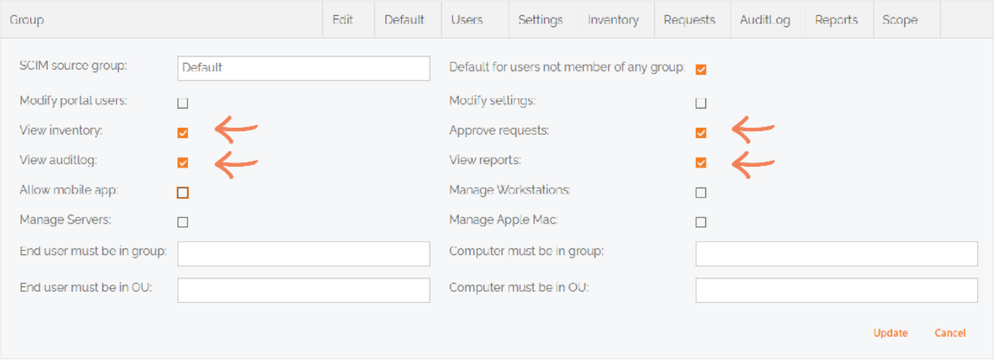
3. Ensure the **Default for users not member of any group** checkbox is checked:



Default for users not member of any group: ☑

IMPORTANT: Only one Group-Based Role can have this property checked, i.e., there can only be one set of default permissions that users without any other Group-Based Role are assigned.

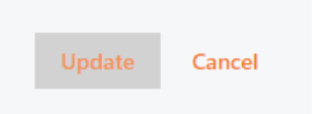
4. Use the filters to define default permissions. In this example, permissions for default users include viewing the Inventory, Auditlog, and Reports, and Approving requests:



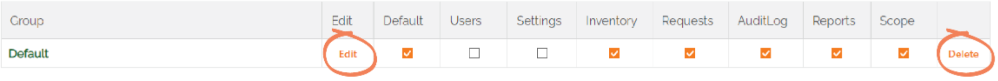
Group	Edit	Default	Users	Settings	Inventory	Requests	AuditLog	Reports	Scope

SCIM source group:	Default	Default for users not member of any group:	☑
Modify portal users:	☐	Modify settings:	☐
View inventory:	☑	Approve requests:	☑
View auditlog:	☑	View reports:	☑
Allow mobile app:	☐	Manage Workstations:	☐
Manage Servers:	☐	Manage Apple Mac:	☐
End user must be in group:		Computer must be in group:	
End user must be in OU:		Computer must be in OU:	

5. Click the **Update** button to save the Role:

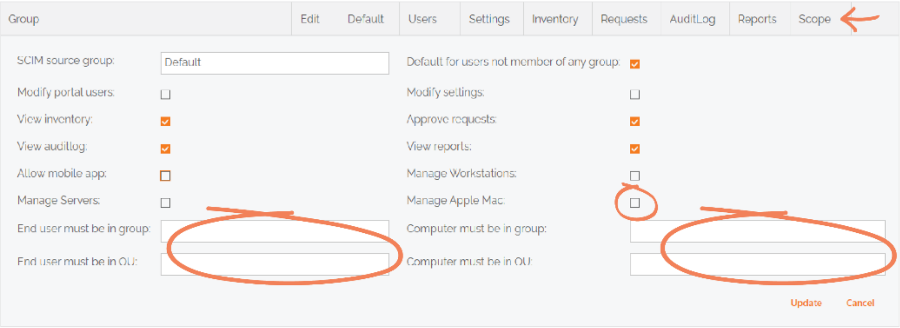


6. To **Edit** or **Delete** the rule, use the respective buttons to the left and right of the eight filter columns:



Group	Edit	Default	Users	Settings	Inventory	Requests	AuditLog	Reports	Scope	
Default	Edit	☑	☐	☐	☑	☑	☑	☑	☑	Delete

NOTE: The first seven filter columns correspond to their matching checkbox in the Edit window (i.e., **Default** to **Reports**), however, the **Scope** checkbox corresponds to multiple properties: the **Manage Apple Mac** checkbox and the **End user** and **Computer** textboxes at the bottom of the window:



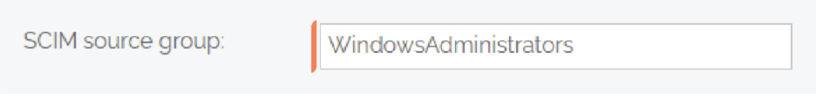
SCIM source group: Default
Modify portal users: □
View inventory: ☑
View auditlog: ☑
Allow mobile app: □
Manage Servers: □
End user must be in group:
End user must be in OU:
Default for users not member of any group: ☑
Modify settings: □
Approve requests: ☑
View reports: ☑
Manage Workstations: □
Manage Apple Mac: □
Computer must be in group:
Computer must be in OU:

The process for assigning Roles with specific permissions to actual IDP groups follows a similar set of steps to those described above. The section below uses a common example to illustrate how Group-Based Roles could be applied.

Create Group-Based Role for Windows Admins

You have a group in Azure AD called 'WindowsAdministrators' whose members only require access to Windows-related data. You therefore want to prevent all users in this group from accessing Mac data in the Admin By Request User Portal (e.g., Inventory, Requests and Auditlogs from Mac devices / users, etc.). The solution is to create a Group-Based Role which filters out Mac access for members of the WindowsAdministrators source group.

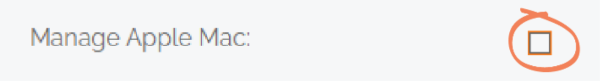
1. After creating a **New entry** in the **SCIM source group** textbox, type the name of the IDP source group you want to define specific permissions for – in this example, *WindowsAdministrators*:



SCIM source group: WindowsAdministrators

NOTE: If you have created a Default group as described above, the **Default for users not member of any group** checkbox will automatically be unchecked when you come to create another Group-Based Role, as this property can only be applied once.

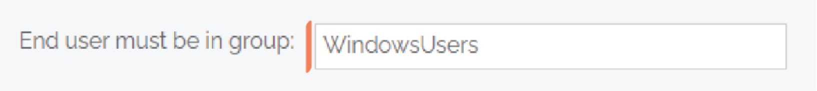
2. Use the checkboxes to filter out the source group's access to the appropriate features. For this example, uncheck the **Manage Apple Mac** checkbox to remove Mac access for the *WindowsAdministrators* source group:



Manage Apple Mac: □

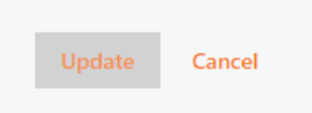
NOTE: You could also use any of the other Scope textboxes to ensure the *WindowsAdministrators* group has the correct permissions. For example:

- If you have a group in Azure AD for Windows end users called *WindowsUsers*, you could type this group name into the **End user must be in group** textbox, which would prevent the *WindowsAdministrators* source group from seeing any data other than that of end users in the *WindowsUsers* Azure AD group:



End user must be in group: WindowsUsers

3. Click the **Update** button to save the Role. When users in the *WindowsAdministrators* Azure AD group are synchronized, they will only have the permissions defined in this Role within the Admin By Request User Portal.

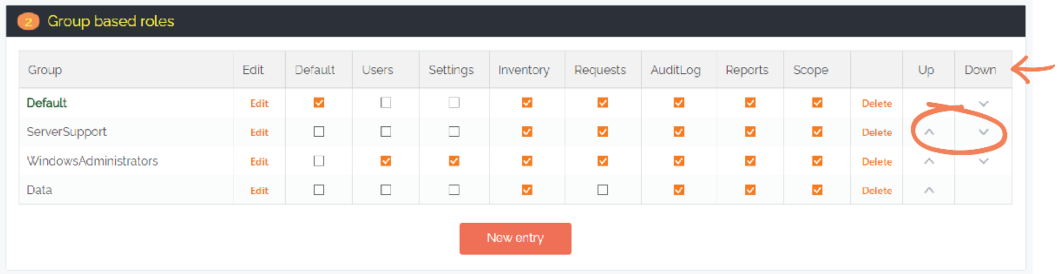


The Group-Based Roles appear in the list according to the order they were created: the first appearing at the top of the list, and the most recent getting added to the bottom. If a user belongs to multiple groups – all of which have Group-Based Roles defined – the first Role in the list will apply for that user.

NOTE: Four Roles have been created in the example below with the following properties checked:

- **Default** – *Default*, *Inventory*, *Requests*, *Auditlog*, *Reports*, *Scope*.
- **ServerSupport** – *Inventory*, *Requests*, *Auditlog*, *Reports*, *Scope*.
- **WindowsAdministrators** – *Users*, *Settings*, *Inventory*, *Requests*, *Auditlog*, *Reports*, *Scope*.
- **Data** – *Inventory*, *Auditlog*, *Reports*, *Scope*.

To change the order of Roles in the list, use the up and down arrows to the right of each entry:



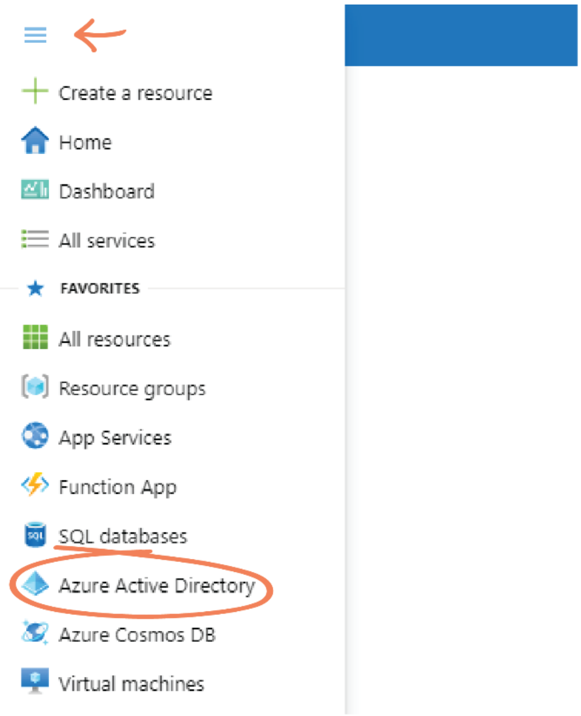
2 Group based roles

Group	Edit	Default	Users	Settings	Inventory	Requests	AuditLog	Reports	Scope		Up	Down
Default	Edit	☑	□	□	☑	☑	☑	☑	☑	Delete		⌄
ServerSupport	Edit	□	□	□	☑	☑	☑	☑	☑	Delete	^	⌄
WindowsAdministrators	Edit	□	☑	☑	☑	☑	☑	☑	☑	Delete	^	⌄
Data	Edit	□	□	□	☑	□	☑	☑	☑	Delete	^	

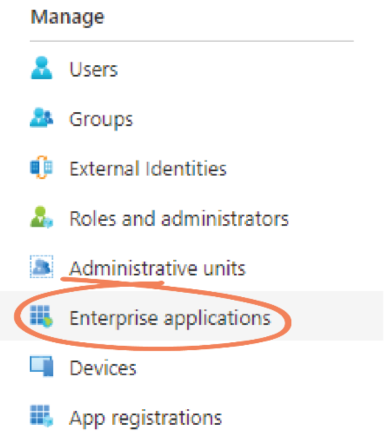
Task C: Create Azure Application

Task C in the integration process involves creating a custom Admin By Request application on the IDP side. In Azure AD, this is done in the form of an Enterprise Application.

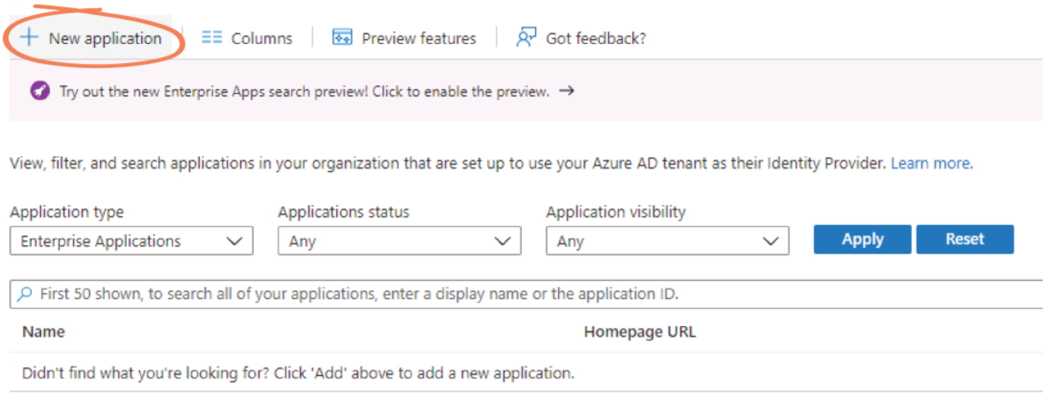
1. In your Azure portal, click the top-left menu icon and select **Azure Active Directory** from the left-hand menu:



2. When the Directory opens, select **Enterprise applications** from the left-hand menu:



3. Click the **+ New Application** tab:



+ New application | Columns | Preview features | Got feedback?

Try out the new Enterprise Apps search preview! Click to enable the preview. →

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider. Learn more.

Application type: Enterprise Applications

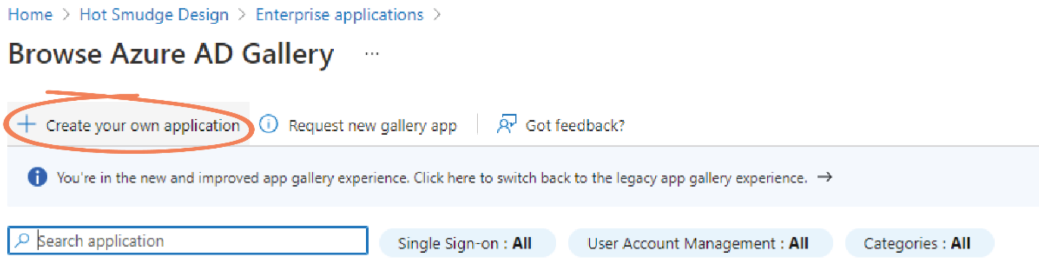
Applications status: Any

Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

Name	Homepage URL
Didn't find what you're looking for? Click 'Add' above to add a new application.	

4. Select **+ Create your own application**:



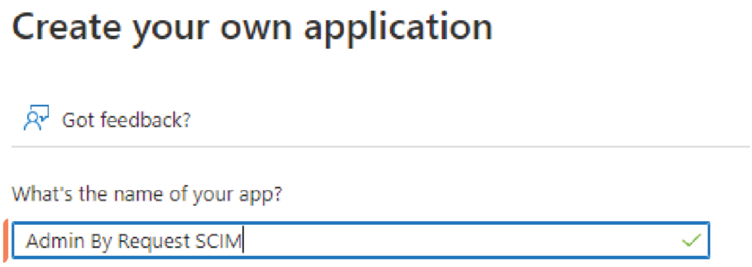
Home > Hot Smudge Design > Enterprise applications >

Browse Azure AD Gallery ...

+ Create your own application | Request new gallery app | Got feedback?

You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. →

5. In the **What's the name of your app** textbox, type *Admin By Request SCIM*:



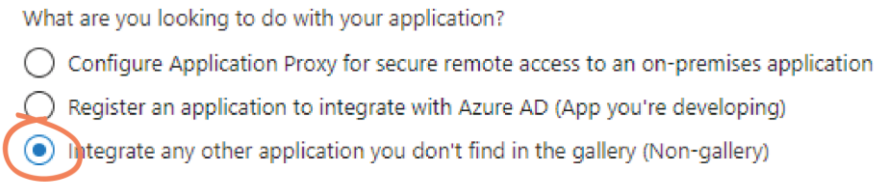
Create your own application

Got feedback?

What's the name of your app?

Admin By Request SCIM

6. In the **What are you looking to do with your application** section, ensure the **Integrate any other application you don't find in the gallery (Non-gallery)** radio button is selected:



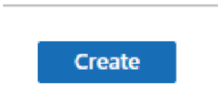
What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

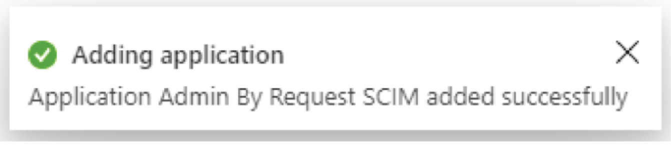
○ Register an application to integrate with Azure AD (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

7. Click **Create**:



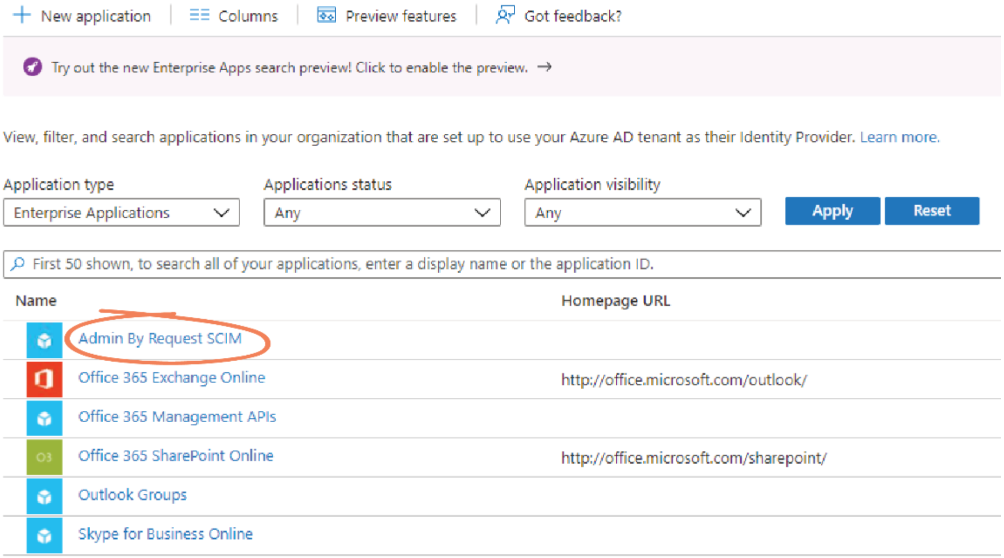
NOTE: The application may take a few moments to create, with a progress message displaying in the top-right corner of the screen during the process; this is the location of all similar progress and success messages in the Azure portal. The following success message displays upon app creation:



Adding application

Application Admin By Request SCIM added successfully

IMPORTANT: If you encounter a **404 Not Found** page after the app is created (even if the success message above was displayed) navigate back to **Enterprise applications** to locate the **Admin By Request SCIM** app:



Try out the new Enterprise Apps search preview! Click to enable the preview. →

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider. Learn more.

Application type: Enterprise Applications

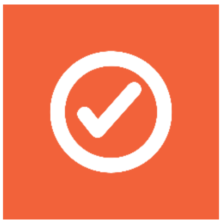
Applications status: Any

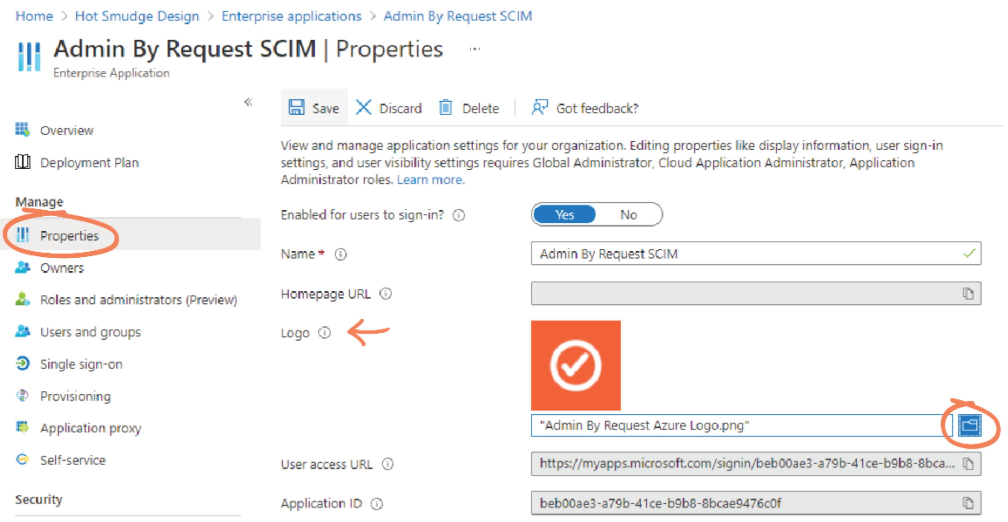
Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

Name	Homepage URL
Admin By Request SCIM	
Office 365 Exchange Online	http://office.microsoft.com/outlook/
Office 365 Management APIs	
Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/
Outlook Groups	
Skype for Business Online	

NOTE: Once in the application page, further configuration steps are available. **Step 1. Users and Groups** is covered in Task E of this process manual; **Step 3. Provision User Accounts** is covered in Task D. You have the option of configuring any of the other settings (e.g., **4. Conditional Access**, **5. Self service**) but these do not affect the Admin By Request integration. You also have the option of navigating to **Properties** in the left-hand menu and setting the **Logo** to the following image:





Admin By Request SCIM | Properties

Enterprise Application

View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. Learn more.

Enabled for users to sign-in? Yes

Name * Admin By Request SCIM

Homepage URL

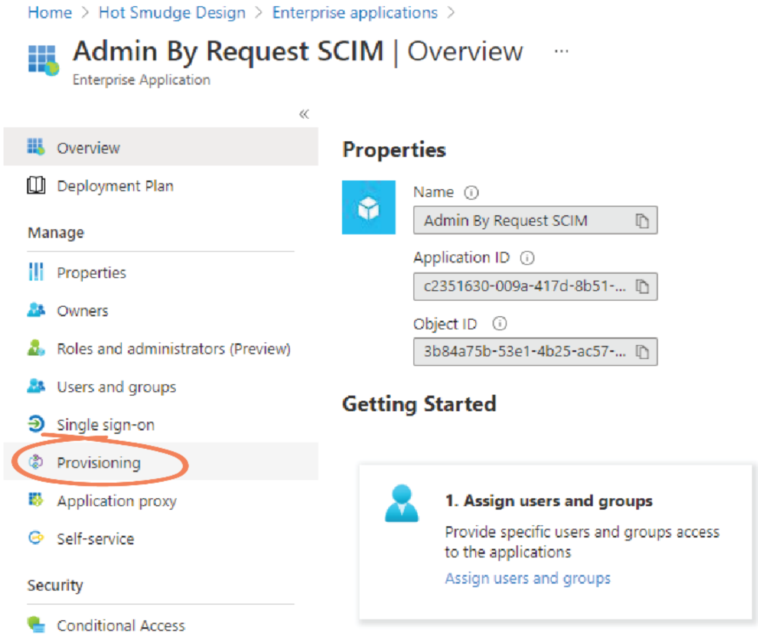
Logo "Admin By Request Azure Logo.png"

User access URL https://myapps.microsoft.com/signin/beb00ae3-a79b-41ce-b9b8-8bca...

Application ID beb00ae3-a79b-41ce-b9b8-8bcae9476c0f

Task D: Set Up Provisioning

1. From the left-hand menu of the **Admin By Request SCIM** application page, select **Provisioning** (located in either the left-hand menu or the main page):



Admin By Request SCIM | Overview

Enterprise Application

Properties

Name Admin By Request SCIM

Application ID c2351630-009a-417d-8b51-...

Object ID 3b84a75b-53e1-4b25-ac57-...

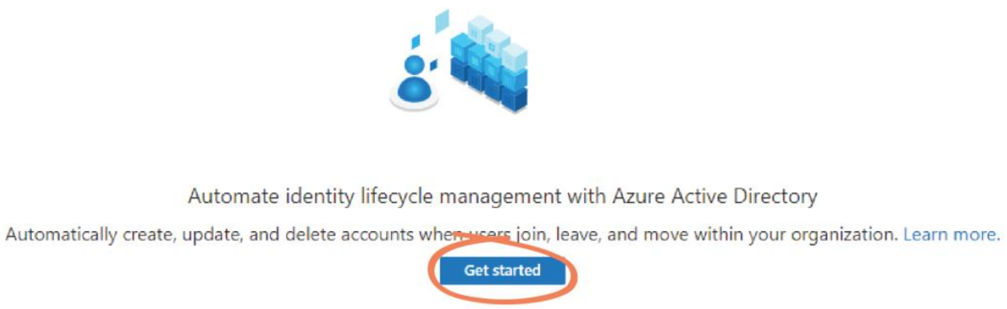
Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

Assign users and groups

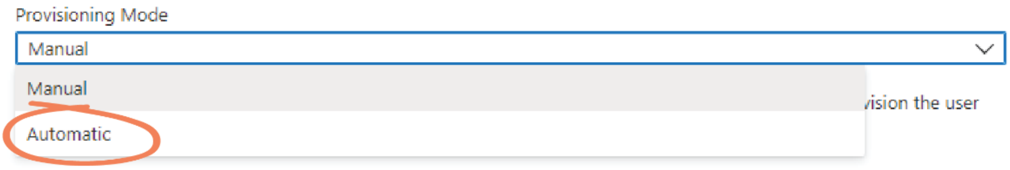
2. Click the **Get Started** button:



Automate identity lifecycle management with Azure Active Directory

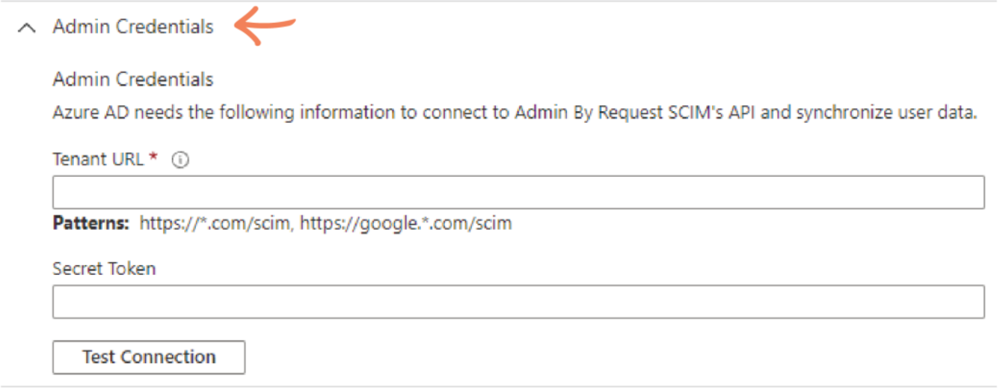
Automatically create, update, and delete accounts when users join, leave, and move within your organization. Learn more.

3. From the **Provisioning Mode** drop-down menu, select **Automatic**:


Provisioning Mode

Manual

NOTE: Doing so displays a new **Admin Credentials** section on the page, used in subsequent steps of this Task (i.e., Task D):



Admin Credentials

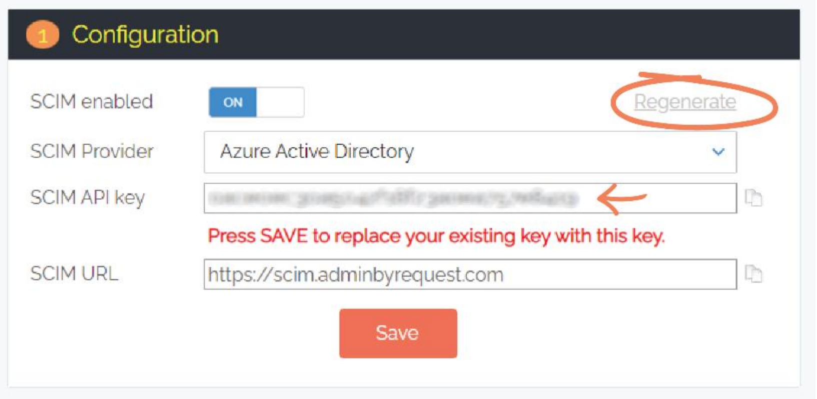
Azure AD needs the following information to connect to Admin By Request SCIM's API and synchronize user data.

Tenant URL *

Patterns: https://*.com/scim, https://google.*.com/scim

Secret Token

4. In your Admin By Request User Portal, ensure you are in the **SCIM Provisioning Setup** page, and select the **Regenerate** button in section **1. Configuration**, to generate a new API key:


1 Configuration

SCIM enabled: ON

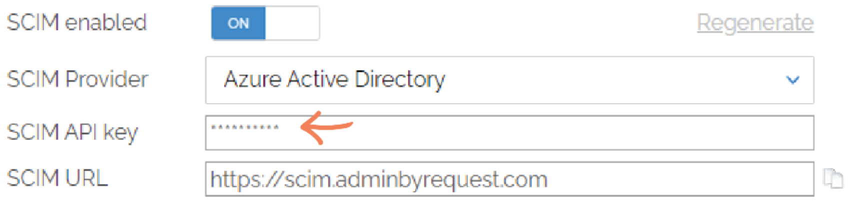
SCIM Provider: Azure Active Directory

SCIM API key: [redacted]

Press SAVE to replace your existing key with this key.

SCIM URL: https://scim.adminbyrequest.com

NOTE: A new API key needs to be generated so that it can be copied to the clipboard for future use. Prior to clicking **Regenerate**, the API key is hidden and cannot be copied:

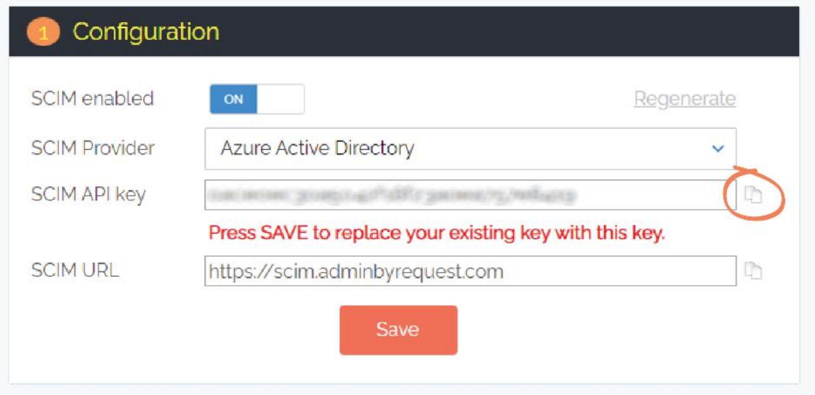

SCIM enabled: ON

SCIM Provider: Azure Active Directory

SCIM API key: **********

SCIM URL: https://scim.adminbyrequest.com

5. Click the clipboard icon to the right of the **SCIM API key** field to copy the key:



1 Configuration

SCIM enabled: ON

Regenerate

SCIM Provider: Azure Active Directory

SCIM API key

Press SAVE to replace your existing key with this key.

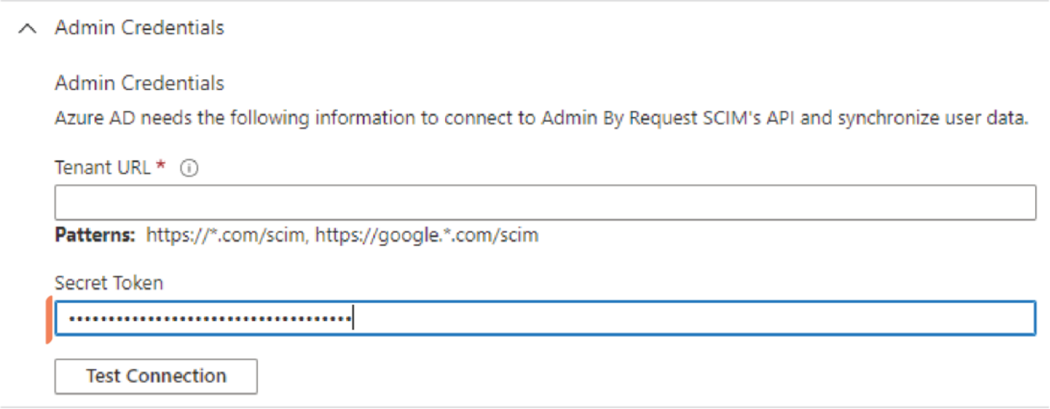
SCIM URL: https://scim.adminbyrequest.com

NOTE: Click **OK** to dismiss the confirmation pop-up that appears.

6. Click **Save** to ensure the new API key is used:

IMPORTANT: Do not click the **Save** button until you have copied the API key. Doing so will hide the key and it will then need to be regenerated before it can be copied. However, it is imperative that you save *after* copying the API key, to ensure this key is used in the SCIM integration.

7. In your Azure portal, in the **Secret Token** field of the **Admin Credentials** section, paste the API key copied from Admin By Request:



Admin Credentials

Admin Credentials

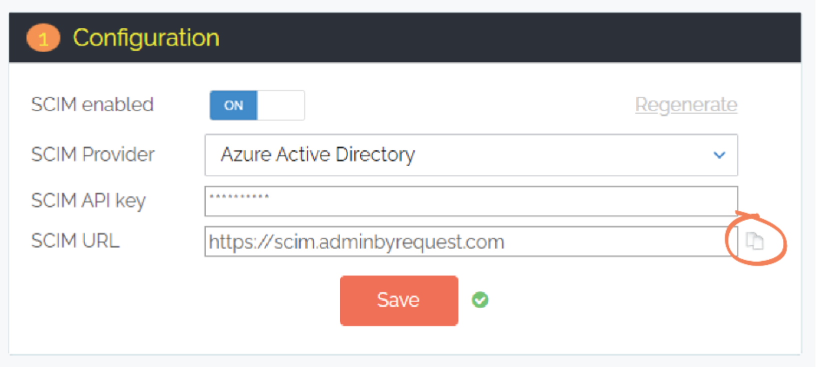
Azure AD needs the following information to connect to Admin By Request SCIM's API and synchronize user data.

Tenant URL *

Patterns: https://*.com/scim, https://google.*.com/scim

Secret Token: ••••••••••••••••••••••••••••••••••••

8. In your Admin By Request User Portal, copy the **SCIM URL**:



Configuration

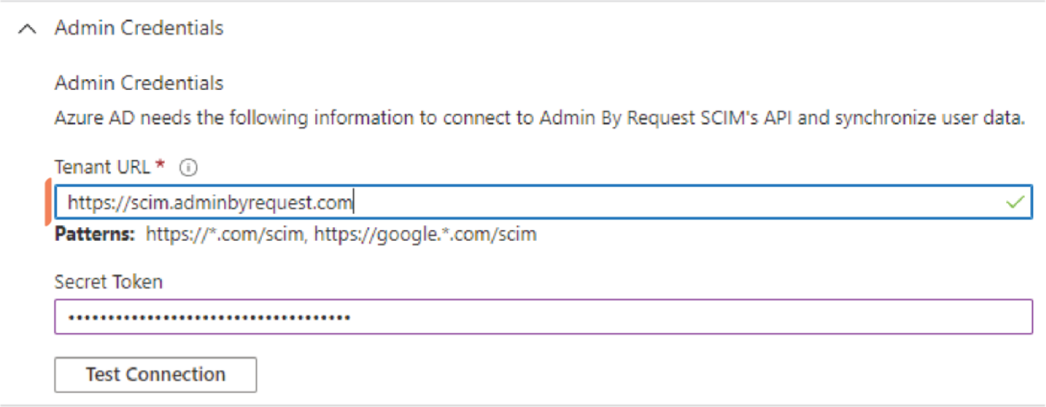
SCIM enabled: ON

SCIM Provider: Azure Active Directory

SCIM API key: ••••••••••

SCIM URL: https://scim.adminbyrequest.com

9. In your Azure portal, paste the URL into the **Tenant URL** textbox:



Admin Credentials

Admin Credentials

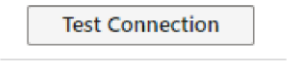
Azure AD needs the following information to connect to Admin By Request SCIM's API and synchronize user data.

Tenant URL *: https://scim.adminbyrequest.com

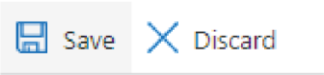
Patterns: https://*.com/scim, https://google.*.com/scim

Secret Token: •••••••••••••••••••••••••••••••••••

10. Click the **Test Connection** button:

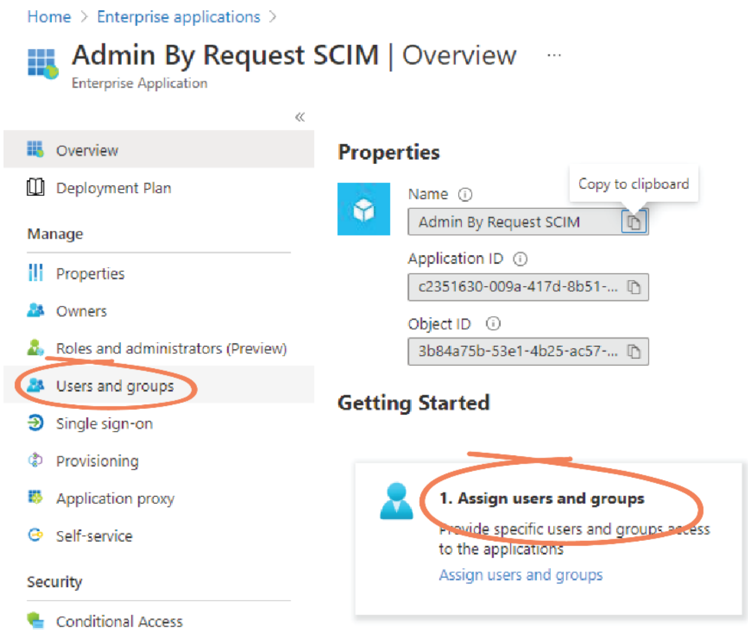


11. Click the **Save** button in the top left:



Task E: Assign Users and Groups

1. Navigate to the application page (**Home** > **Enterprise applications** > **Admin By Request SCIM**) and select **Users and Groups** (located in either the left-hand menu or the main page):



Name: Admin By Request SCIM

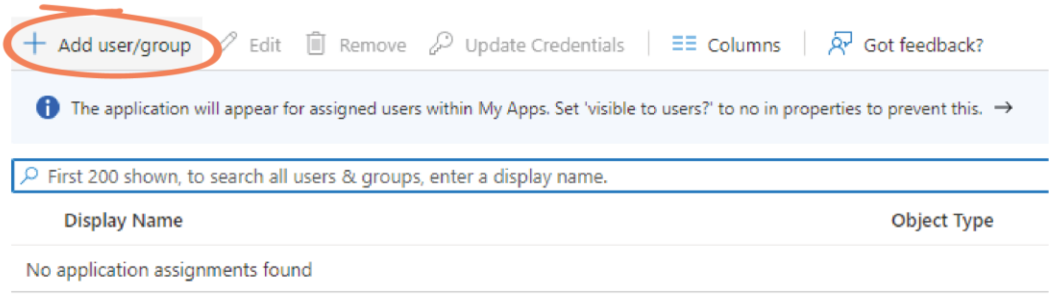
Application ID: c2351630-009a-417d-8b51-...

Object ID: 3b84a75b-53e1-4b25-ac57-...

1. Assign users and groups

Provide specific users and groups access to the applications

2. Click the **+ Add user/group** tab:

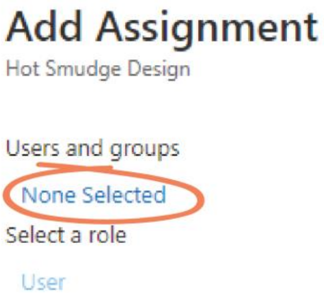


The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type
No application assignments found	

3. Under **Users and groups**, click **None selected**:



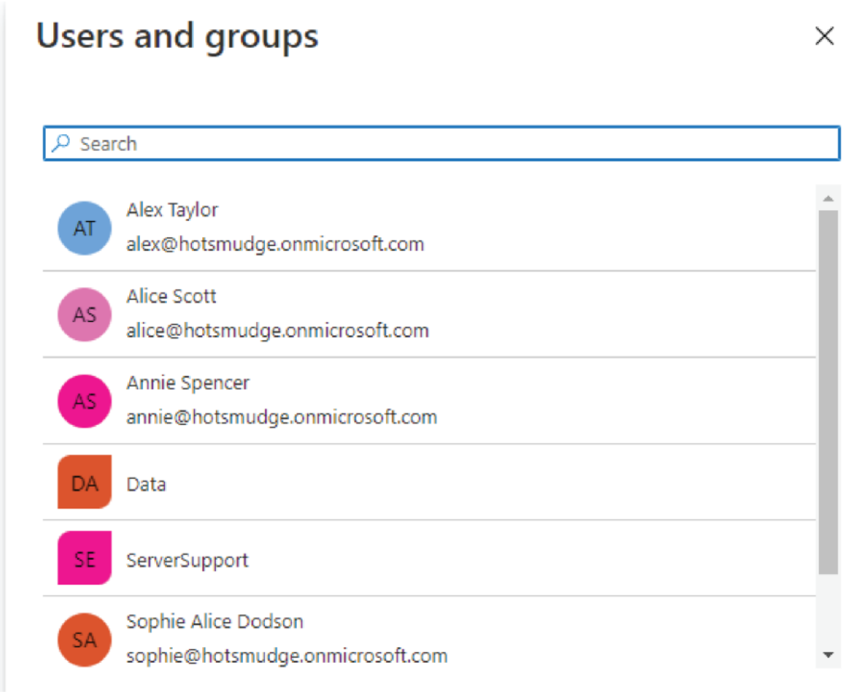
Add Assignment

Hot Smudge Design

Users and groups: None Selected

Select a role: User

4. From the **Users and groups** list on the right-hand side, select the users and / or groups you want to assign:



Users and groups

Search

Alex Taylor
alex@hotsmudge.onmicrosoft.com

Alice Scott
alice@hotsmudge.onmicrosoft.com

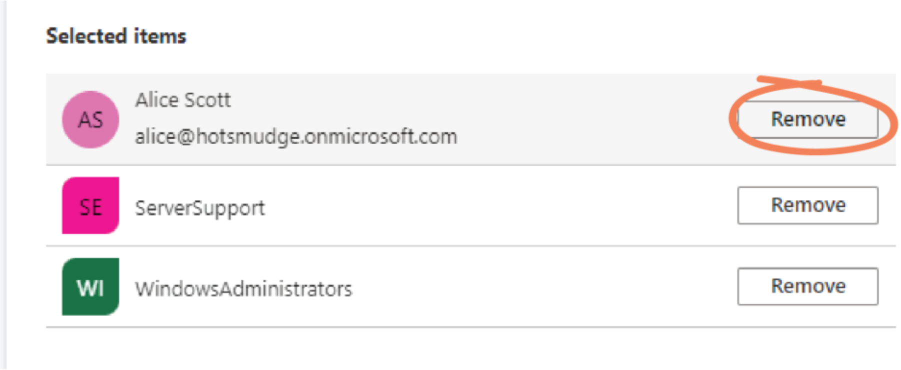
Annie Spencer
annie@hotsmudge.onmicrosoft.com

Data

ServerSupport

Sophie Alice Dodson
sophie@hotsmudge.onmicrosoft.com

NOTE: Multiple users / groups can be selected. As each user / group is selected, they appear in the **Selected items** section. Click the **Remove** button to remove a selection:



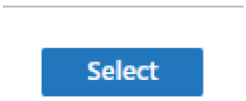
Selected items

Alice Scott
alice@hotsmudge.onmicrosoft.com

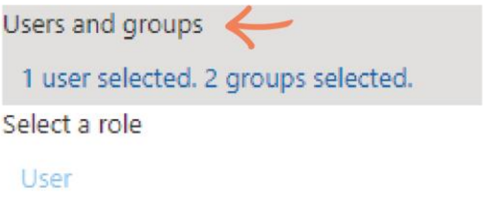
ServerSupport

WindowsAdministrators

5. When the desired users are selected, click **Select**:



NOTE: The number of selected users is now listed under **Users** in the **Users and Groups** page:



Users and groups

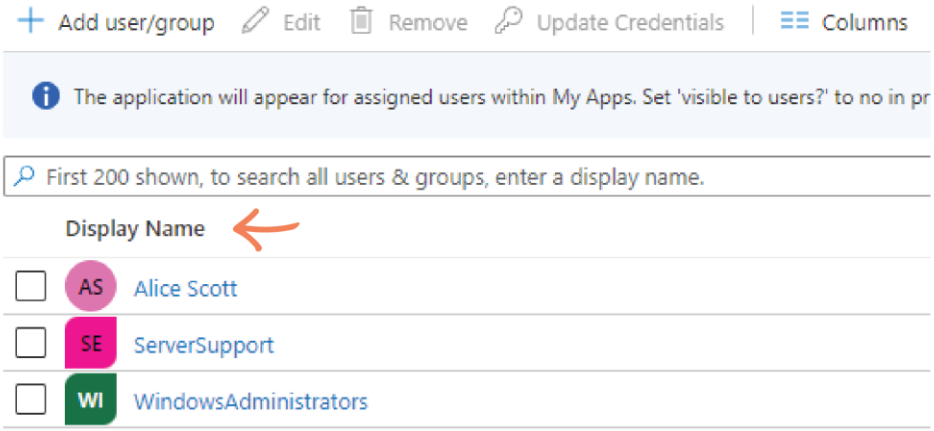
1 user selected. 2 groups selected.

Select a role

User

6. Click the **Assign** button at the bottom of the page:

NOTE: This action returns you to the **Users and Groups** page. A success message appears upon completion, stating the number of users and that have been successfully assigned access to the application. The assigned users are listed under **Display name**:



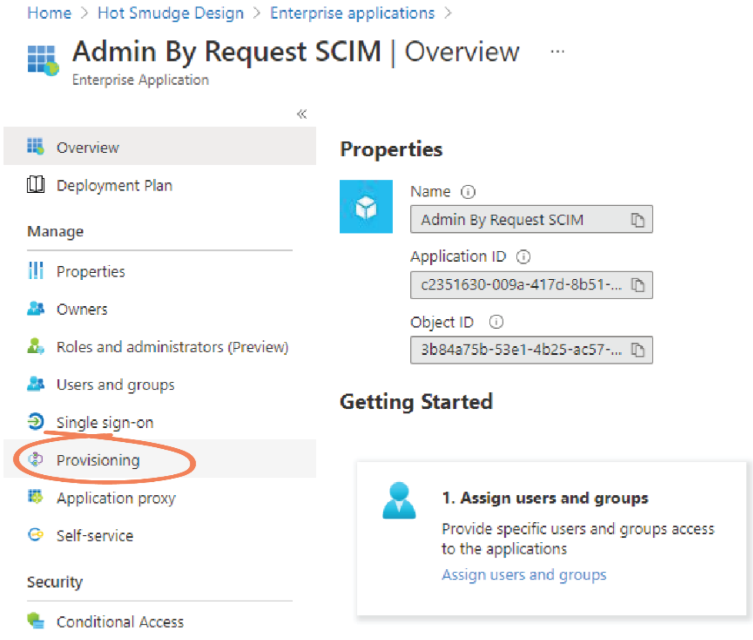
The application will appear for assigned users within My Apps. Set 'visible to users?' to no in pr

First 200 shown, to search all users & groups, enter a display name.

	Display Name
□	AS Alice Scott
□	SE ServerSupport
□	WI WindowsAdministrators

Task F: Start Provisioning

1. From the application page (**Home** > **Enterprise applications** > **Admin By Request SCIM**) select **Provisioning** (located in either the left-hand menu or the main page):



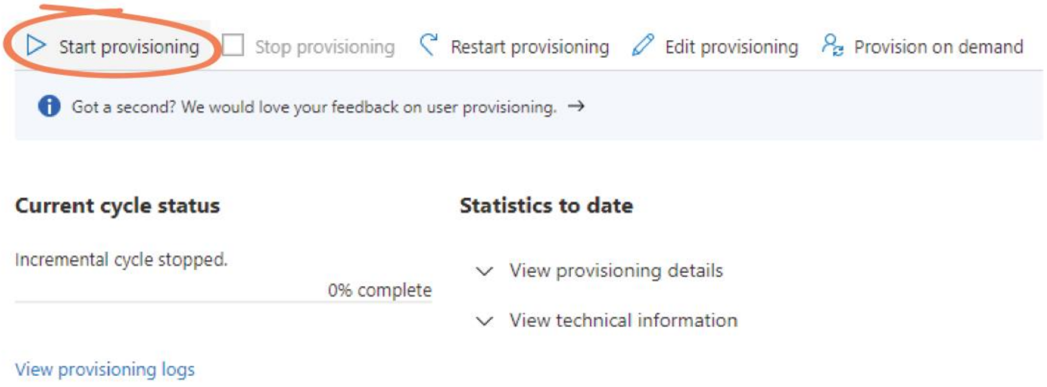
Name: Admin By Request SCIM

Application ID: c2351630-009a-417d-8b51-...

Object ID: 3b84a75b-53e1-4b25-ac57-...

Provide specific users and groups access to the applications

2. Click the **Start Provisioning** tab from the top menu:



Got a second? We would love your feedback on user provisioning. →

Current cycle status

Incremental cycle stopped.

0% complete

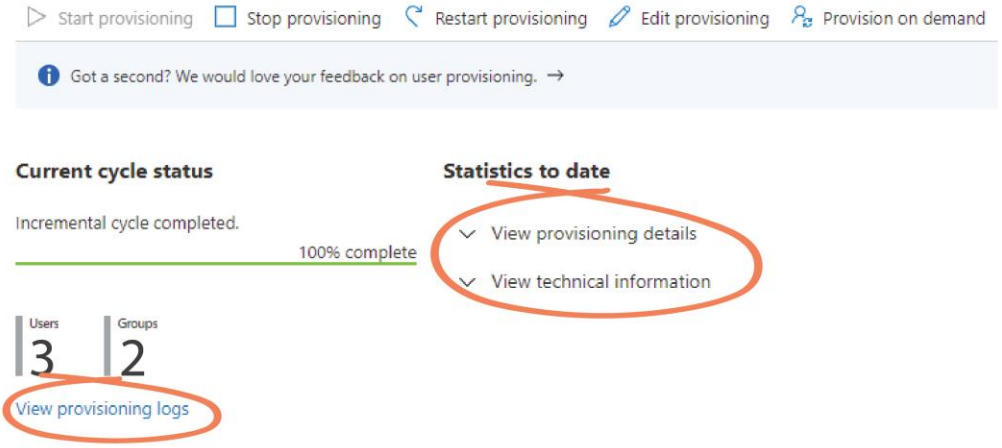
View provisioning logs

Statistics to date

View provisioning details

View technical information

NOTE: Eventually users and groups are synchronized to your Admin By Request User Portal. This usually occurs approximately every 20 to 40 minutes. When synchronization is complete, the page displays provisioning details:



Got a second? We would love your feedback on user provisioning. →

Current cycle status

Incremental cycle completed.

100% complete

Users 3

Groups 2

View provisioning logs

Statistics to date

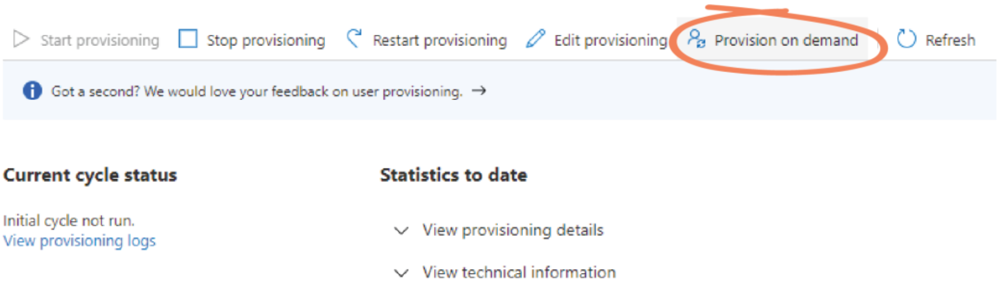
View provisioning details

View technical information

Provision On Demand

Azure AD provides a Provision on demand option which force the synchronization of a user immediately. This is a good way to validate provisioning with a small number of users before rolling out broadly for your organization. You can only **Provision on demand** one user at a time.

1. To do this, select the **Provision on demand** tab from the top menu:



Got a second? We would love your feedback on user provisioning. →

Current cycle status

Initial cycle not run.

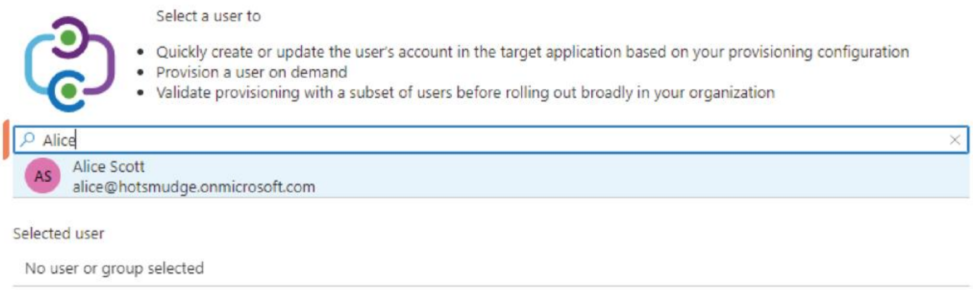
View provisioning logs

Statistics to date

View provisioning details

View technical information

2. In the search bar, type the name of one of the assigned users – in this case, *Alice Scott*.



Select a user to

- Quickly create or update the user's account in the target application based on your provisioning configuration
- Provision a user on demand
- Validate provisioning with a subset of users before rolling out broadly in your organization

Alice

AS Alice Scott
alice@hotsmudge.onmicrosoft.com

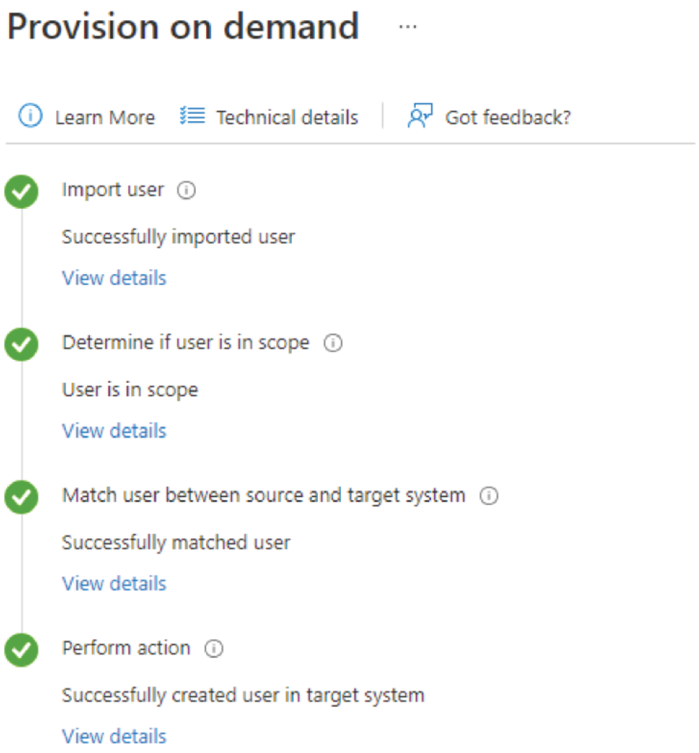
Selected user

No user or group selected

IMPORTANT: You can only provision users that have been assigned to the application (covered in Task E). Users that have not been assigned are still able to be selected if you type their name into the search bar, but the user will not be synchronized to the Admin By Request User Portal (you will receive an **out of scope** error message). However, if you have unassigned a user from the application, you can **Provision on demand** this change to immediately remove them from the Admin By Request User Portal (instead of waiting for the provisioning cycle to run). This is covered in the Deprovisioning section further on in this Task (i.e., Task E).

3. Select the user from the list, and click the **Provision** button at the bottom of the screen:

NOTE: If successful, the **Provision on demand** window details the four completed actions and provides **Export details** listing each target attribute name and its value:



Provision on demand ...

Import user

Successfully imported user

View details

Determine if user is in scope

User is in scope

View details

Match user between source and target system

Successfully matched user

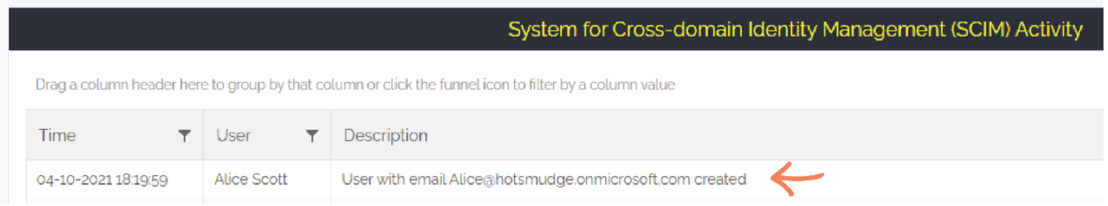
View details

Perform action

Successfully created user in target system

View details

In the Admin By Request User Portal, the user that was **Provisioned on demand** (*Alice Scott*) is now synchronized (viewing data in the User Portal is covered in detail in Task G):

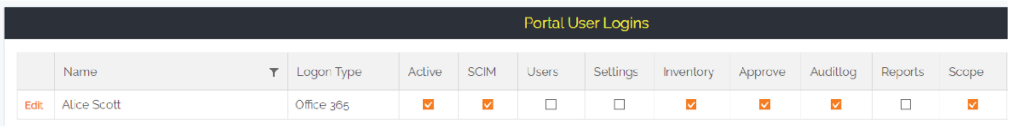


System for Cross-domain Identity Management (SCIM) Activity

Drag a column header here to group by that column or click the funnel icon to filter by a column value

Time	User	Description
04-10-2021 18:19:59	Alice Scott	User with email Alice@hotsmudge.onmicrosoft.com created

IMPORTANT: You cannot use **Provision on demand** for groups. Therefore, all Group-Based Roles other than the *Default* Role are not implemented until the provisioning cycle runs and groups are synchronized. This means that individual users who are **Provisioned on demand** (such as *Alice Scott* in our example) will have the *Default* permissions assigned, as can be seen in the user portal:



Portal User Logins

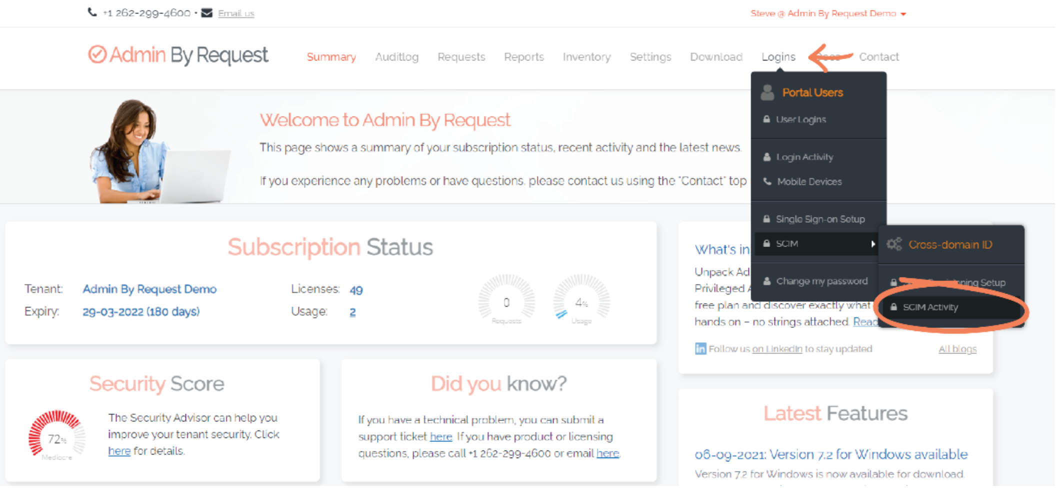
	Name	Logon Type	Active	SCIM	Users	Settings	Inventory	Approve	Auditlog	Reports	Scope
Edit	Alice Scott	Office 365	☑	☑	□	□	☑	☑	☑	□	☑

Deprovisioning

To deprovision users and / or groups [Add screenshots].

Task G: View Data in User Portal

1. In the Admin By Request User Portal, navigate to **Logins** > **SCIM** > **SCIM Activity**:



Welcome to Admin By Request

This page shows a summary of your subscription status, recent activity and the latest news.

If you experience any problems or have questions, please contact us using the 'Contact' top

Subscription Status

Tenant:	Admin By Request Demo	Licenses:	49
Expiry:	29-03-2022 (180 days)	Usage:	2

What's in

Unpack Ad
Privileged
free plan and discover exactly what
hands on – no strings attached. Read

Follow us on LinkedIn to stay updated   All blogs

Security Score

The Security Advisor can help you improve your tenant security. Click here for details.

Did you know?

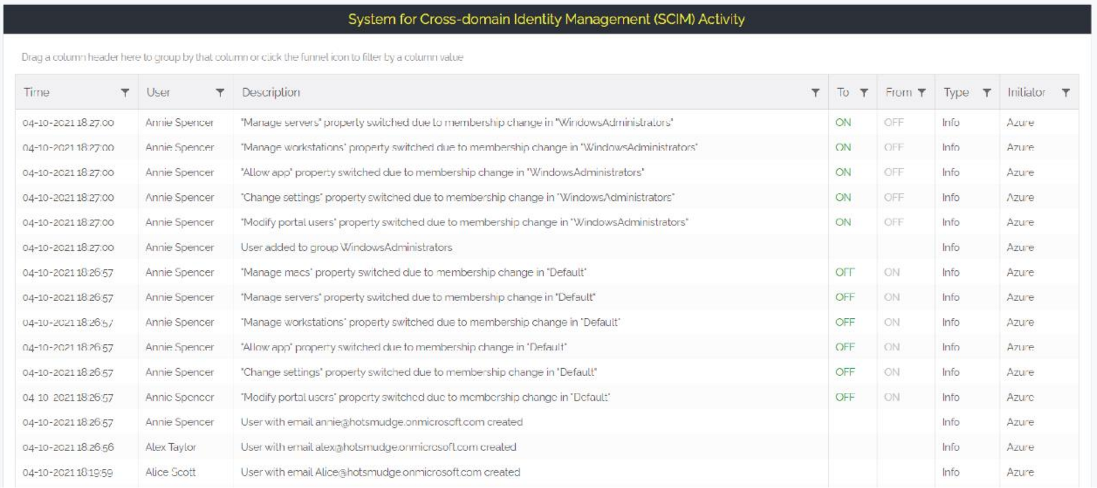
If you have a technical problem, you can submit a support ticket here. If you have product or licensing questions, please call +1 262-299-4600 or email here.

Latest Features

06-09-2021: Version 7.2 for Windows available

Version 7.2 for Windows is now available for download.

2. The table The table displays all synchronized user and group data, including the **Time** synchronization occurred, the name of the **User**, a **Description** of the activity, **To** and **From** columns (which only display content if a permission has changed – i.e., a property has 'switched' from checked to unchecked, such as when a user has been added to a group or their Group-Based Role has been edited, etc.), and the **Initiator** (the IDP – i.e., Azure AD):

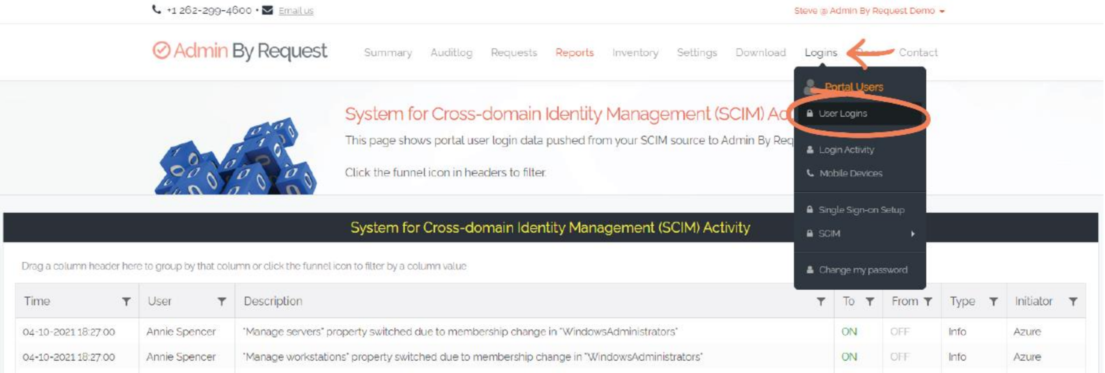


System for Cross-domain Identity Management (SCIM) Activity

Drag a column header here to group by that column or click the funnel icon to filter by a column value

Time	User	Description	To	From	Type	Initiator
04-10-2021 18:27:00	Annie Spencer	"Manage servers" property switched due to membership change in "WindowsAdministrators"	ON	OFF	Info	Azure
04-10-2021 18:27:00	Annie Spencer	"Manage workstations" property switched due to membership change in "WindowsAdministrators"	ON	OFF	Info	Azure
04-10-2021 18:27:00	Annie Spencer	"Allow app" property switched due to membership change in "WindowsAdministrators"	ON	OFF	Info	Azure
04-10-2021 18:27:00	Annie Spencer	"Change settings" property switched due to membership change in "WindowsAdministrators"	ON	OFF	Info	Azure
04-10-2021 18:27:00	Annie Spencer	"Modify portal users" property switched due to membership change in "WindowsAdministrators"	ON	OFF	Info	Azure
04-10-2021 18:27:00	Annie Spencer	User added to group WindowsAdministrators			Info	Azure
04-10-2021 18:26:57	Annie Spencer	"Manage macs" property switched due to membership change in "Default"	OFF	ON	Info	Azure
04-10-2021 18:26:57	Annie Spencer	"Manage servers" property switched due to membership change in "Default"	OFF	ON	Info	Azure
04-10-2021 18:26:57	Annie Spencer	"Manage workstations" property switched due to membership change in "Default"	OFF	ON	Info	Azure
04-10-2021 18:26:57	Annie Spencer	"Allow app" property switched due to membership change in "Default"	OFF	ON	Info	Azure
04-10-2021 18:26:57	Annie Spencer	"Change settings" property switched due to membership change in "Default"	OFF	ON	Info	Azure
04-10-2021 18:26:57	Annie Spencer	"Modify portal users" property switched due to membership change in "Default"	OFF	ON	Info	Azure
04-10-2021 18:26:57	Annie Spencer	User with email annie@hotsmudge.onmicrosoft.com created			Info	Azure
04-10-2021 18:26:56	Alex Taylor	User with email alex@hotsmudge.onmicrosoft.com created			Info	Azure
04-10-2021 18:19:59	Alice Scott	User with email Alice@hotsmudge.onmicrosoft.com created			Info	Azure

3. All provisioned users should have the appropriate permissions as defined in Group-Based Roles (Task B). To view this, navigate to **Logins** > **User Logins**:



System for Cross-domain Identity Management (SCIM) Ac

This page shows portal user login data pushed from your SCIM source to Admin By Req

Click the funnel icon in headers to filter.

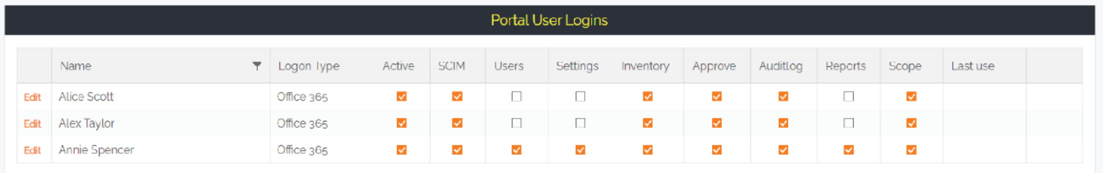
System for Cross-domain Identity Management (SCIM) Activity

Drag a column header here to group by that column or click the funnel icon to filter by a column value

Time	User	Description	To	From	Type	Initiator
04-10-2021 18:27:00	Annie Spencer	"Manage servers" property switched due to membership change in "WindowsAdministrators"	ON	OFF	Info	Azure
04-10-2021 18:27:00	Annie Spencer	"Manage workstations" property switched due to membership change in "WindowsAdministrators"	ON	OFF	Info	Azure

4. The appropriate checkboxes should be ticked next to each user depending on their group and the Group-Based Role defined for that group:

    - *Alice Scott* has the *Default* permissions assigned as she is not a member of any group.
    - *Alex Taylor* has permissions defined for the *ServerSupport* Group-Based Role.
    - *Annie Spencer* has permissions defined for the *WindowsAdministrators* Group-Based Role.

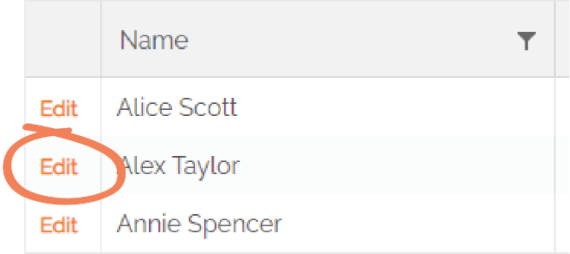


Portal User Logins

	Name	Logon Type	Active	SCIM	Users	Settings	Inventory	Approve	Auditlog	Reports	Scope	Last use
Edit	Alice Scott	Office 365	☑	☑	□	□	☑	☑	☑	□	☑	
Edit	Alex Taylor	Office 365	☑	☑	□	□	☑	☑	☑	□	☑	
Edit	Annie Spencer	Office 365	☑	☑	☑	☑	☑	☑	☑	☑	☑	

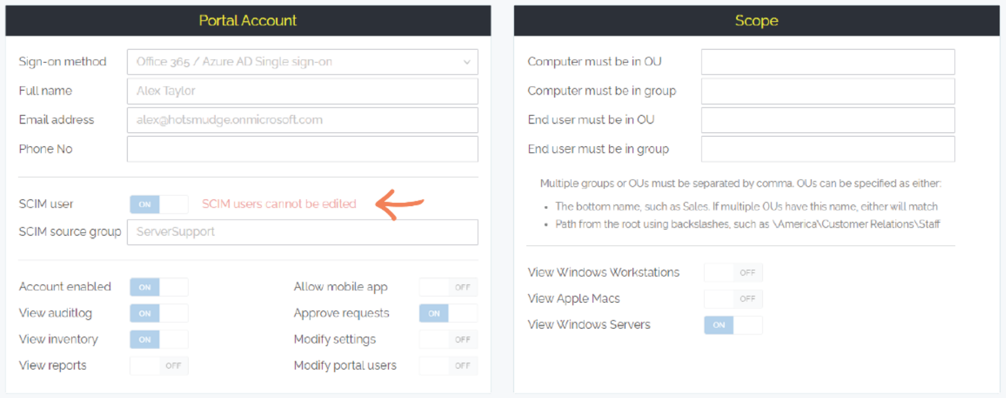
IMPORTANT: As soon as a user is synchronized, they get the permission defined for their group in Group-Based Roles (either Default or specific IDP group). If Group-Based Roles are edited, the users assigned that Role get the updated permissions as soon as the provisioning cycle runs again.

5. Click the **Edit** button next to a user in **Portal User Logins** – in this example, *Alex Taylor*:



	Name
Edit	Alice Scott
Edit	Alex Taylor
Edit	Annie Spencer

IMPORTANT: Users that have been synchronized with SCIM cannot be edited within the Admin By Request User Portal. You can view their data in the Portal Account section, but are not able to make changes because the data is controlled by the IDP (i.e., Azure AD):



Portal Account

Sign-on method: Office 365 / Azure AD Single sign-on

Full name: Alex Taylor

Email address: alex@hotsmudge.onmicrosoft.com

Phone No:

SCIM user: ON — SCIM users cannot be edited

SCIM source group: ServerSupport

Account enabled: ON

View auditlog: ON

View inventory: ON

View reports: OFF

Allow mobile app: OFF

Approve requests: ON

Modify settings: OFF

Modify portal users: OFF

Scope

Computer must be in OU:

Computer must be in group:

End user must be in OU:

End user must be in group:

Multiple groups or OUs must be separated by comma. OUs can be specified as either:

- The bottom name, such as Sales. If multiple OUs have this name, either will match
- Path from the root using backslashes, such as \America\Customer Relations\Staff

View Windows Workstations: OFF

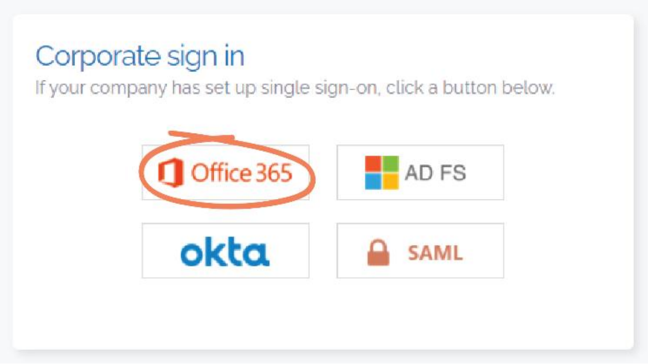
View Apple Macs: OFF

View Windows Servers: ON

User Login

Now that users are provisioned, they can sign into the Admin By Request User Portal using their IDP credentials.

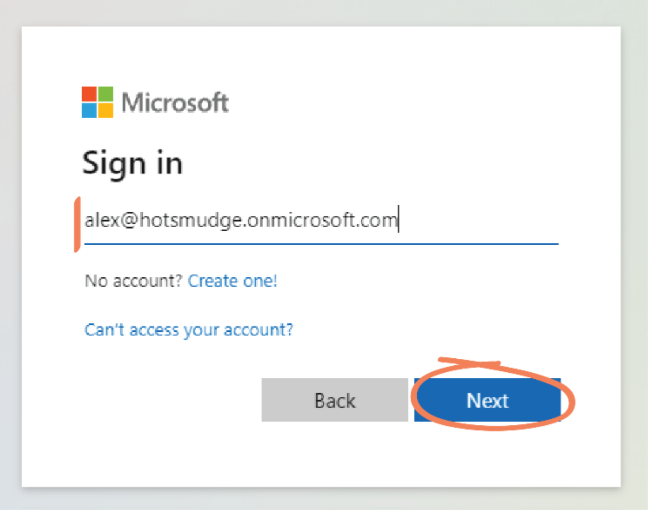
1. Go to the Admin By Request Sign in page and select **Office 365** from the **Corporate Sign-in** section:



Corporate sign in

If your company has set up single sign-on, click a button below.

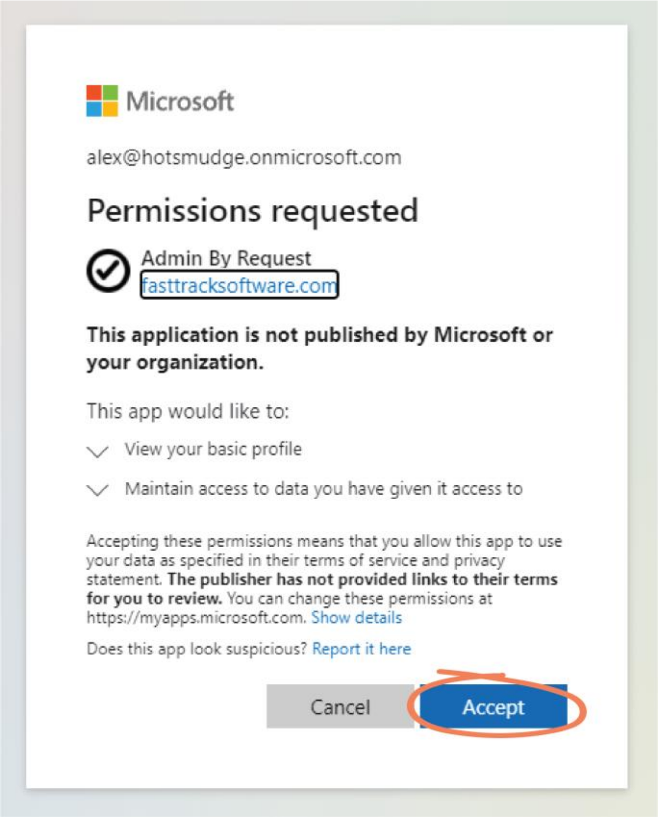
2. Provisioned users can use their Office 365 user name to sign in. This example uses *Alex Taylor*. Click **Next**:



Sign in

alex@hotsmudge.onmicrosoft.com

3. Select **Accept** to give permission to the app the required permissions (listed in the window):



Microsoft

alex@hotsmudge.onmicrosoft.com

Permissions requested

Admin By Request
fasttracksoftware.com

This application is not published by Microsoft or your organization.

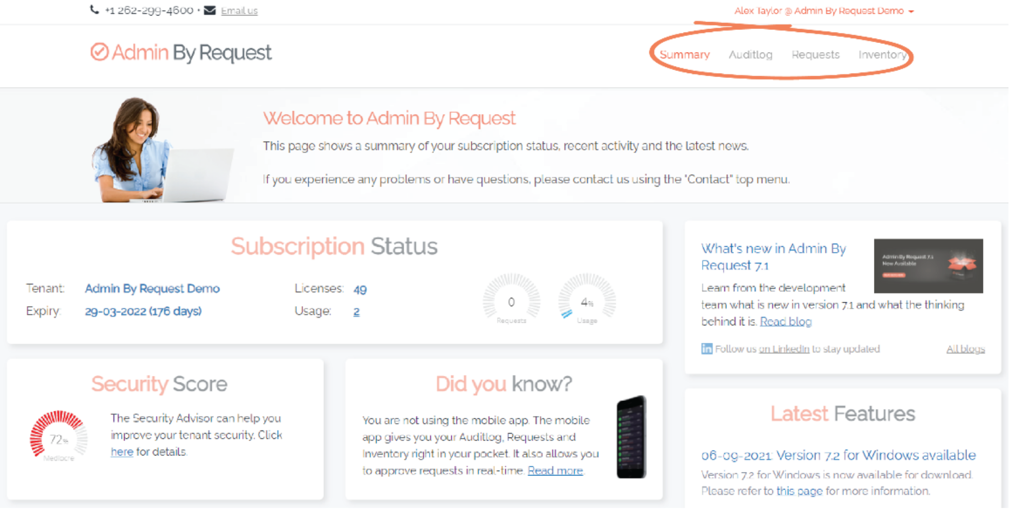
This app would like to:

- View your basic profile
- Maintain access to data you have given it access to

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

4. Once signed in, the user only has access to User Portal features according to the permissions defined in their Group-Based Role. *Alex Taylor* is in the *ServerSupport* group, with access to view the *Auditlog*, *Inventory*, and *Reports* data, approve *Requests*, and *Manage Servers* (not shown on this page):



+1 262-299-4600 · Email us
Alex Taylor @ Admin By Request Demo
Admin By Request
Summary
Auditlog
Requests
Inventory

Welcome to Admin By Request

This page shows a summary of your subscription status, recent activity and the latest news.

If you experience any problems or have questions, please contact us using the 'Contact" top menu.

Subscription Status

Tenant: Admin By Request Demo
Expiry: 29-03-2022 (176 days)
Licenses: 49
Usage: 2

What's new in Admin By Request 7.1

Learn from the development team what is new in version 7.1 and what the thinking behind it is. Read blog

Follow us on LinkedIn to stay updated All blogs

Security Score

The Security Advisor can help you improve your tenant security. Click here for details.

Did you know?

You are not using the mobile app. The mobile app gives you your Auditlog, Requests and Inventory right in your pocket. It also allows you to approve requests in real-time. Read more

Latest Features

06-09-2021 Version 7.2 for Windows available

Version 7.2 for Windows is now available for download. Please refer to this page for more information.