

# Remove Users from Secure Access Dashboard Provisioned Using Microsoft Azure

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Configure](#)

[1. Identify the users that need to be removed](#)

[2. Remove the desired users](#)

[3. Stop and Start Provisioning](#)

### [Verify](#)

[Verify from the logs on the Azure Portal](#)

### [Related Information](#)

---

## Introduction

This document describes how to remove users from Secure Access dashboard provisioned by Microsoft Azure.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Access
- Microsoft Azure
- User provisioning using Enterprise Applications in Azure

### Components Used

The information in this document is based on these software and hardware versions:

- Secure Access
- Microsoft Azure

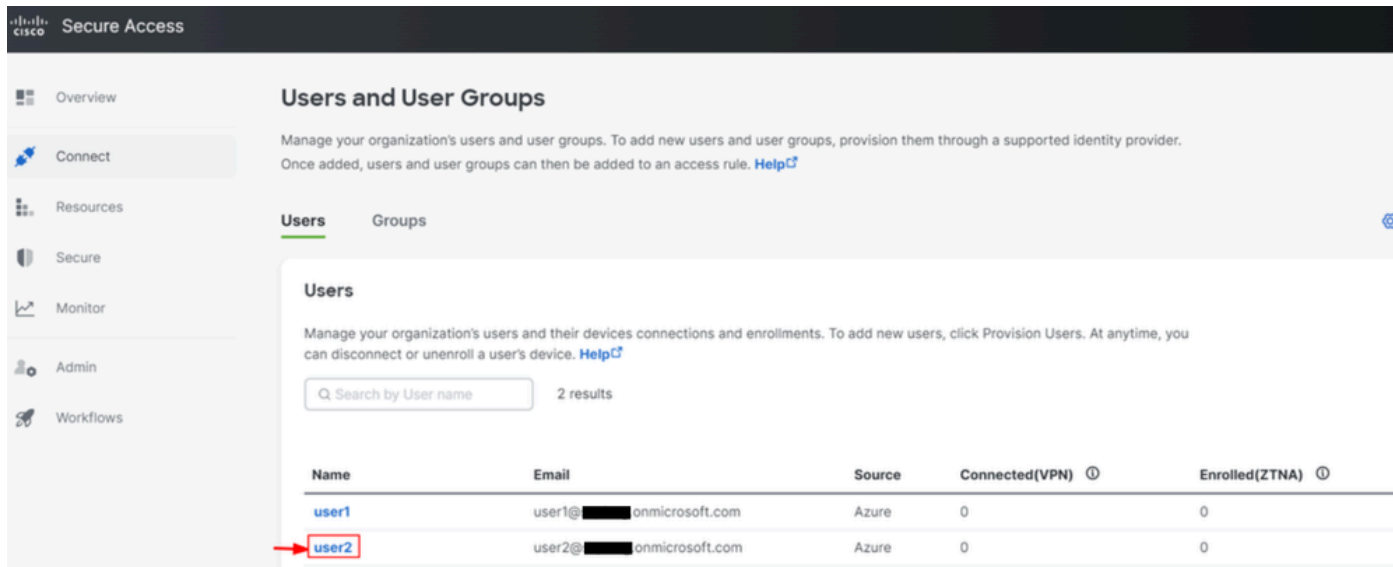
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Configure

# 1. Identify the users that need to be removed

Identify the user which needs to be removed from the dashboard.

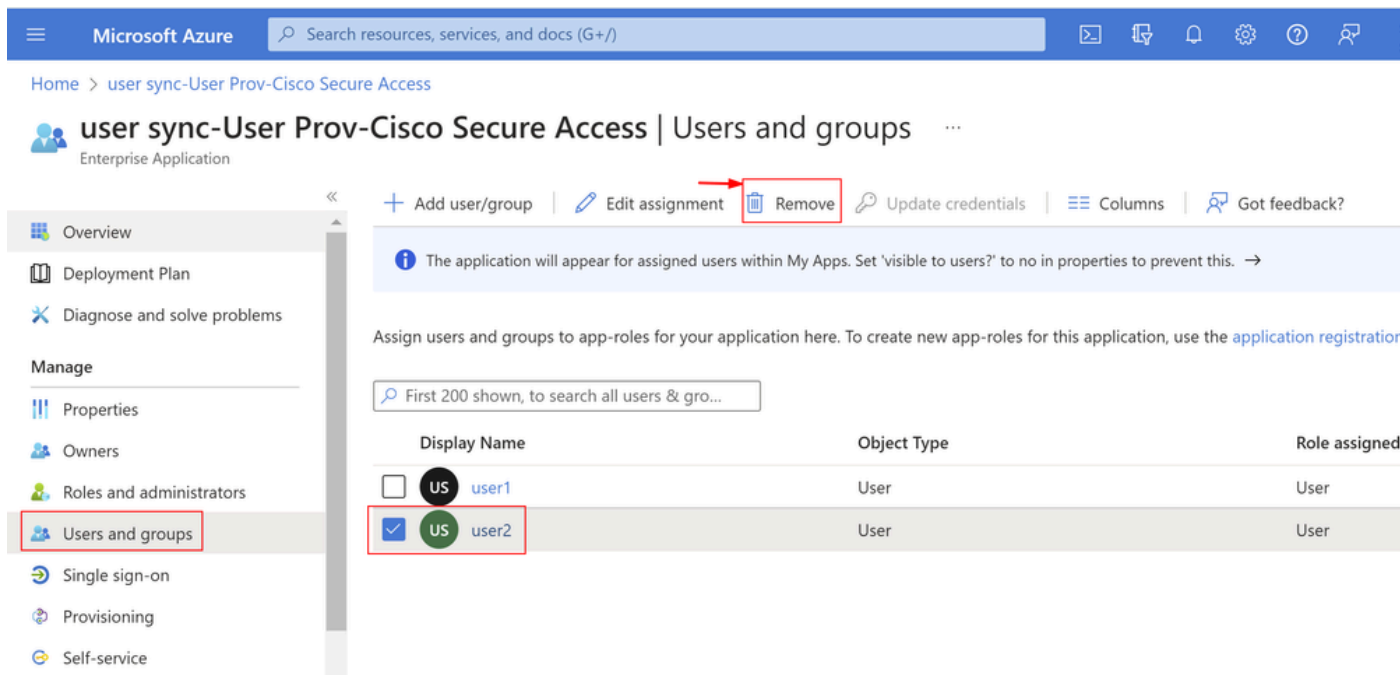
- Navigate to [Secure Access UI](#)
- Connect > Users and Groups
- For this example, you are going to see how to remove user2



# 2. Remove the desired users

Navigate to the [Azure portal](#)

- Enterprise Applications
- Select your provisioning Enterprise Application
- Users and Groups, then choose the users that you want to delete
- Click Remove



### 3. Stop and Start Provisioning

After removing the desired users, navigate to **Provisioning**.

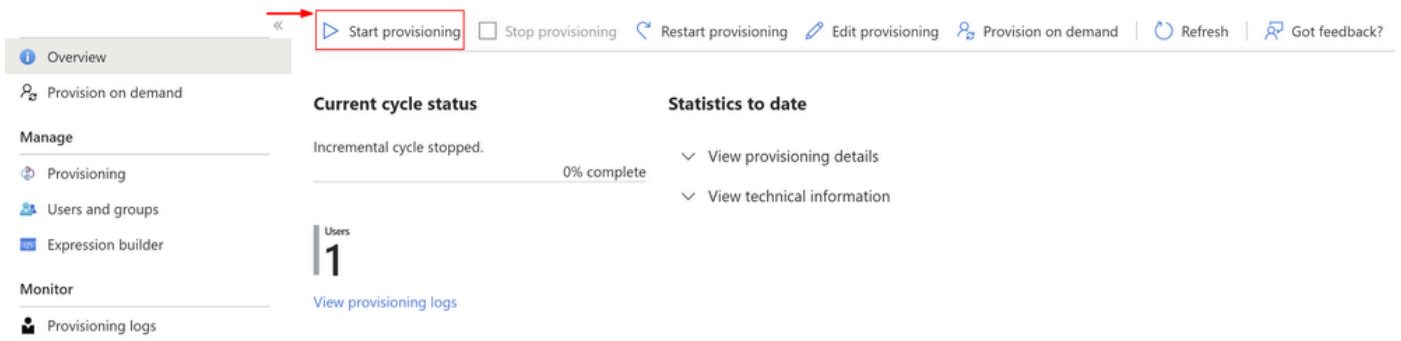
The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and navigation icons. Below that, the breadcrumb trail reads 'Home > user sync-User Prov-Cisco Secure Access'. The main header displays 'user sync-User Prov-Cisco Secure Access | Users and groups' with a menu icon. A left-hand navigation pane is visible, containing sections for 'Overview', 'Deployment Plan', 'Diagnose and solve problems', 'Manage', and 'Self-service'. The 'Provisioning' option under the 'Manage' section is highlighted with a red box and a red arrow pointing to it. The main content area shows a toolbar with options like 'Add user/group', 'Edit assignment', 'Remove', 'Update credentials', 'Columns', and 'Got feedback?'. Below the toolbar, there is a notification banner and a search bar. A table lists assigned users and groups:

Display Name	Object Type	Role assigned
<input type="checkbox"/> US user1	User	User

- Click on Stop Provisioning

The screenshot shows the 'Provisioning' page in the Microsoft Azure portal. The left-hand navigation pane is visible, with 'Provisioning' selected. The main content area features a toolbar with buttons for 'Start provisioning', 'Stop provisioning', 'Restart provisioning', 'Edit provisioning', and 'Provision on demand'. The 'Stop provisioning' button is highlighted with a red box and a red arrow pointing to it. Below the toolbar, there are two main sections: 'Current cycle status' and 'Statistics to date'. The 'Current cycle status' section shows 'Incremental cycle completed.' with a progress bar at '100% complete'. The 'Statistics to date' section shows 'Users' with a large '1' and options to 'View provisioning logs', 'View provisioning details', and 'View technical information'. At the bottom, there is a 'Manage provisioning' section with links for 'Update credentials', 'Edit attribute mappings', 'Add scoping filters', and 'Provision on demand'.

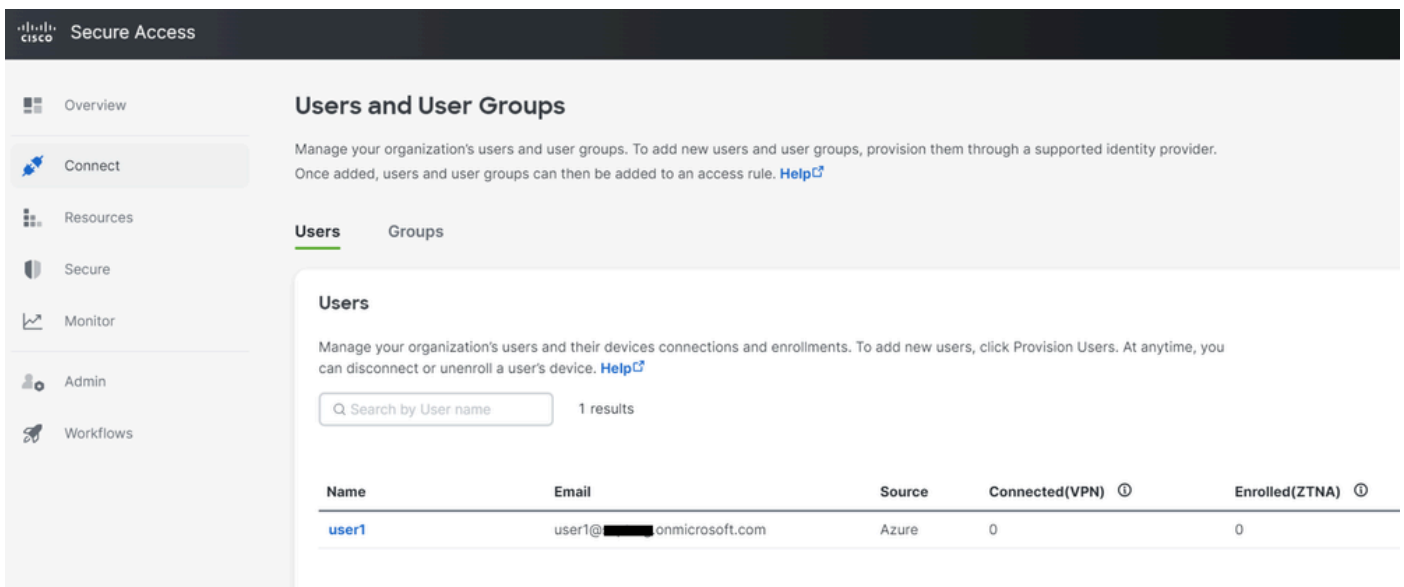
- Next, click on Start Provisioning



Now **Verify** that desired users have been removed from the Secure Access dashboard.

## Verify

As you can see user2 has been removed from the Secure Access dashboard as desired.



## Verify from the logs on the Azure Portal

Navigate to the [Azure Portal](#).

- Enterprise Applications
- Select your provisioning Enterprise Application
- Users and Groups
- Click on View Provisioning logs

Start provisioning  Stop provisioning  Restart provisioning  Edit provisioning

Overview

Provision on demand

Manage

- Provisioning
- Users and groups
- Expression builder

Monitor

- Provisioning logs

**Current cycle status**

Incremental cycle completed.

100% complete

**Statistics to date**

- View provisioning details
- View technical information

Users

1

View provisioning logs

- The log indicates **Action** as Disable with **Status** as **Success**, which confirms the user removal from provisioning on the Secure Access target system

## Provisioning Logs

Download  Learn more  Refresh  Columns  Got feedback?

Identity Name or ID

Date: Last 24 hours Show dates as: Local Status: All Action: All Application contains 6e611dfd-43ed-43b8-bd7e-37ebc1fbf809 Add filters

Date	Iden...	Action	Source System	Target System	Status
12/20/2023, 4:57:27 PM	Display Name: Source ID: Target ID: u	Disable	Azure Active Directory	CiscoUmbrella	Success

## Provisioning log details

Steps Troubleshooting & Recommendations Modified Properties Summary

1. Import urn:ietf:params:scim:schemas:extension:enterprise:2.0:User from Azure Active Directory ✓
2. Match urn:ietf:params:scim:schemas:extension:enterprise:2.0:User between Azure Active Directory and CiscoUmbrella ✓
3. Determine if urn:ietf:params:scim:schemas:extension:enterprise:2.0:User is in scope ✓
4. Provision urn:ietf:params:scim:schemas:extension:enterprise:2.0:User in CiscoUmbrella ✓

EntryExportUpdateSoftDelete

Result

Success

Description

User 'user2@[REDACTED]onmicrosoft.com' was updated in CiscoUmbrella

ReportableIdentifier

user2@[REDACTED]onmicrosoft.com

## Related Information

- [Secure Access UserGuide](#)
- [Cisco Technical Support & Downloads](#)
- [Provision Users and Groups from Azure](#)