

Step-By-Step Configuration Guide for MDM Integration

About This Document

This guide provides a clear, step-by-step configuration for integrating Microsoft Intune MDM with the Versa SASE UEM profile. It explains how to enable Intune device compliance checks and apply Secure Access rules based on compliance state for both Windows and macOS devices.

Document Information

Title	Step-By-Step Configuration Guide for MDM Integration
Author	Versa Professional Services
Version	V 1.0

Disclaimer

Information contained in this document regarding Versa Networks (the Company) is considered proprietary.

Before you begin

Before you proceed with the steps outlined in this document, please ensure you've met the following prerequisites.

- The provider administrator must complete your tenant configuration. If you haven't received this information, please contact your Managed Service Provider or Account Manager for assistance.
- You have the Enterprise Administrator (Tenant Admin) credentials for the Versa SASE portal, also called the Concerto User Interface.
- You have administrative access to the Microsoft Azure Portal, specifically App registrations, Enterprise applications, and Intune configuration pages

Contents

Unified Endpoint Management (UEM)	5
Common Use Case	5
How UEM Works in Versa Secure Access	5
Microsoft Intune Requirements	6
Configure Microsoft ENTRA	7
Validate Licenses	7
Create Users and Groups in Microsoft 365 Admin Centre	7
1. Creating a New User.....	8
2. Creating a Group.....	9
3. Assigning Licenses to Users or Groups	12
Assigning Intune Under Mobility MDM and WIP	12
Configure App Registration	14
1. Navigate to App Registrations.....	14
2. Create a New Application	14
3. Retrieve Required Identifiers	16
4. Generating a Client Secret.....	17
5. Configure API Permissions	18
6. Assign Users and Groups	19
Configuration in Concerto	20
Integration with Accessing Unified Endpoint Management	20
Windows OS Enrollment	24
Configuration in Microsoft Intune – Create Windows Compliance Policies	25
1. create a compliance policy	25
2. Review Compliance Policy Example.....	26
3. confirm Windows device has synchronized on Intune	28
Apply Secure Access Rules for Intune-Managed Devices	29
1. Configure Policy Rule Criteria.....	29
Verification – How to Validate the Integration with Windows	32
MACOS Enrollment	35
Generate the Apple MDM Push Certificate	35
1. Download Apple MDM Push certificate in Intune for Mac enrollment	36

2. Upload the CSR File in the Apple Push Certificates Portal	37
3. Upload the New Apple MDM Push Certificate in Microsoft Intune	39
Install Company Portal on macOS.....	39
1. Install and sign in Microsoft Company Portal	40
2. Install the downloaded profile in macOS.....	43
3. Review Device Visibility in Intune.....	44
Apply Secure Access Rules for Intune-Managed Devices	45
1. Configure Policy Rule Criteria.....	45
Verification – How to validate the integration with macOS Compliance.....	48
About Versa.....	50

Unified Endpoint Management (UEM)

Unified Endpoint Management (UEM) refers to third-party platforms such as Microsoft Intune or Ivanti Neurons that centrally manage and validate endpoints. Versa does not provide its own UEM system; instead, the **Versa UEM Profile integrates** with external services to obtain device information such as device ID, enrollment status, operating system, and compliance state. This information is used by Versa gateways and portals to enforce access policies based on whether a device is managed and compliant, ensuring that only devices that meet corporate security requirements can access protected resources.

By leveraging **UEM profiles** (as defined in the Versa Concerto UI), SASE gateways can enforce device-based access policies during user registration and throughout client sessions. When a device connects to a SASE gateway via the SASE Client, the UEM integration queries the Intune Graph API to verify whether the device is enrolled and compliant with the security policies configured on the customer's MDM/UEM server.

Common Use Case

Users should be able to connect to and access internal applications only when using a managed, **compliant corporate device**. Personal, unmanaged, or non-compliant devices must not be allowed to reach protected resources.

How Intune Helps

Microsoft Intune evaluates each enrolled device and assigns a **compliance state**, for example:

- Compliant
- Non-compliant
- Unknown / not evaluated

This compliance value is what Versa SASE Gateway reads and uses for access decisions.

How UEM Works in Versa Secure Access

This section explains what happens behind the scenes inside Versa:

Portal Registration

1. SASE Client collects device identifiers.
2. The gateway and portal receive the registration request.
3. SSE Gateway triggers a **Graph API query** using:
 - Device ID
 - Tenant + Client ID + Secret
4. Microsoft Graph responds with:

- Management state
- Operating system details
- Compliance status

If the device is compliant → registration succeeds.

Gateway Authentication

Each time the device forms a tunnel:

1. Gateway triggers a new UEM query.
2. Device posture is rechecked in real-time.
3. Compliance must remain intact.

This ensures **continuous posture validation throughout the session**, enforcing a Zero Trust model.

Microsoft Intune Requirements

To integrate Microsoft UEM (Intune) with Versa SASE Gateway, the following prerequisites must be fulfilled:

Licensing Requirements

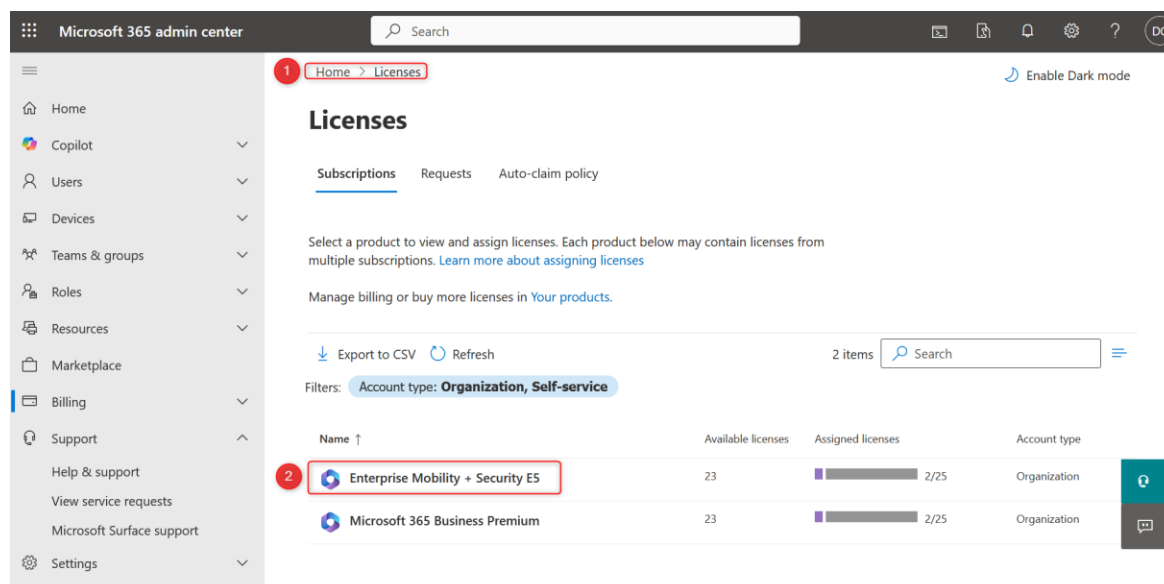
Ensure your Microsoft tenant includes one of the following subscriptions:

- **Enterprise Mobility + Security E3** (includes Intune). **or**
- **Enterprise Mobility + Security E5**

How to Verify Licenses

1. Log in to the Microsoft 365 Admin Centre: <https://admin.microsoft.com>
2. Navigate to **Billing > Licenses**.
3. Confirm that Intune licenses are available.

Sign in to the Microsoft 365 Admin Center at <https://admin.microsoft.com> and navigate to **Billing > Licenses** to verify that your organization has either **Enterprise Mobility + Security (EMS) E3** or **Enterprise Mobility + Security (EMS) E5**, both of which include Microsoft Intune.



These licenses must be assigned to the users who will enroll and manage devices through Intune. Verifying this licensing requirement ensures that Intune can act as the MDM authority and that Versa can retrieve device compliance and management attributes through the Graph API during UEM queries.

Assigning Intune Licenses to Users or Groups

1. Go to **Users > Active Users**.
2. Select the user.

Under **Licenses and Apps**, assign the required Intune subscription.

Note: You may optionally use a Microsoft 365 Business Premium trial for lab/testing purposes.

Configure Microsoft ENTRA

Validate Licenses

Before integrating Microsoft Intune with the Versa SASE Gateway, ensure the required Intune-eligible licenses are available in your Microsoft tenant.

Create Users and Groups in Microsoft 365 Admin Centre

After validating that the required EMS E3/E5 (or Business Premium) licenses exist, continue in the **Microsoft 365 Admin Center** to create the user and assign the Intune license.

From the left navigation panel, the following options allow you to create and manage identities:

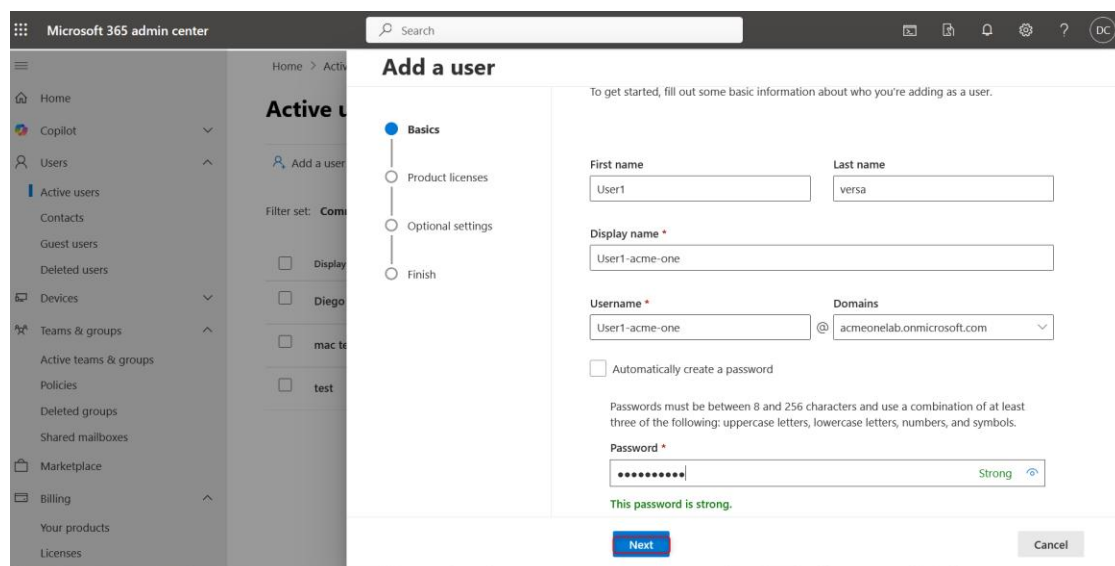
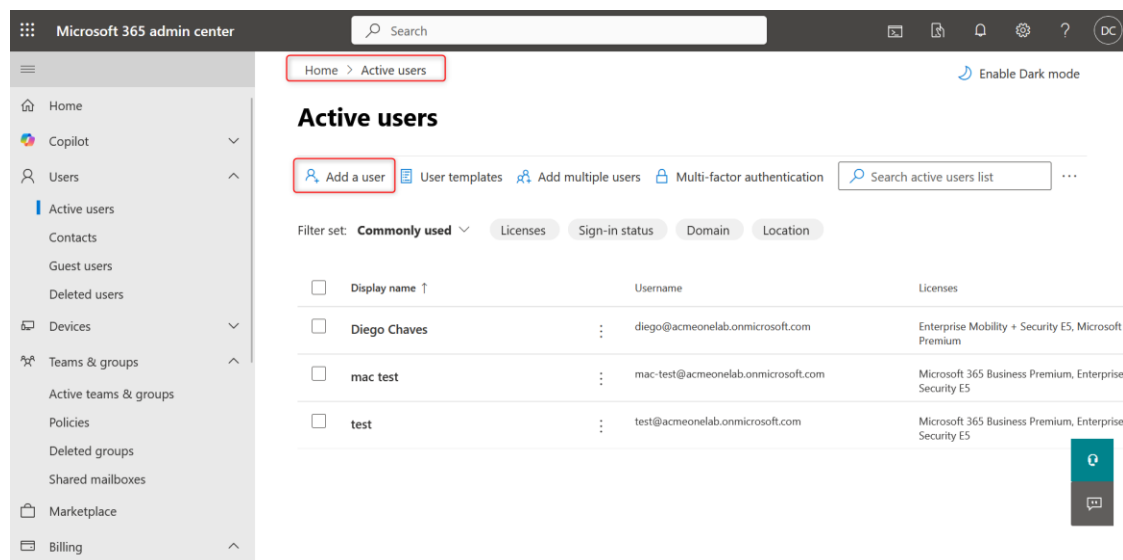
1. Creating a New User

Navigate to **Users** → **Active users** inside the Admin Center.

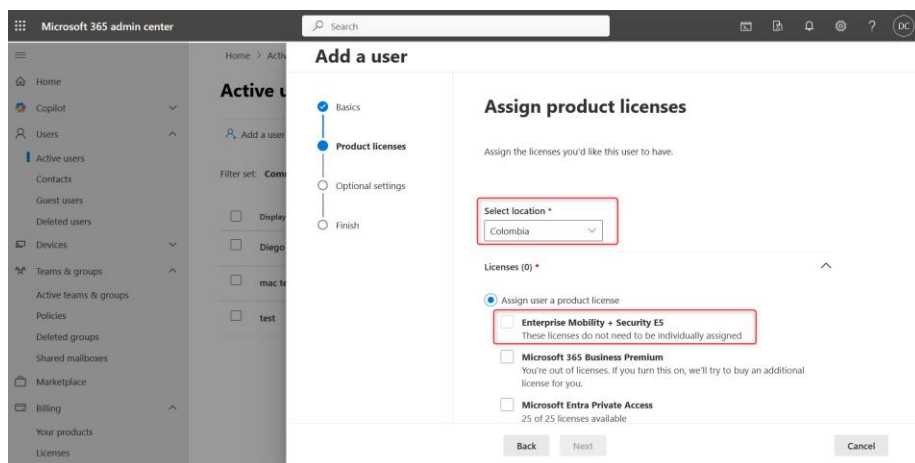
This page displays all users currently registered in your Microsoft tenant.

From here you can add new users who will be managed through Intune and later evaluated by Versa SASE Gateway.

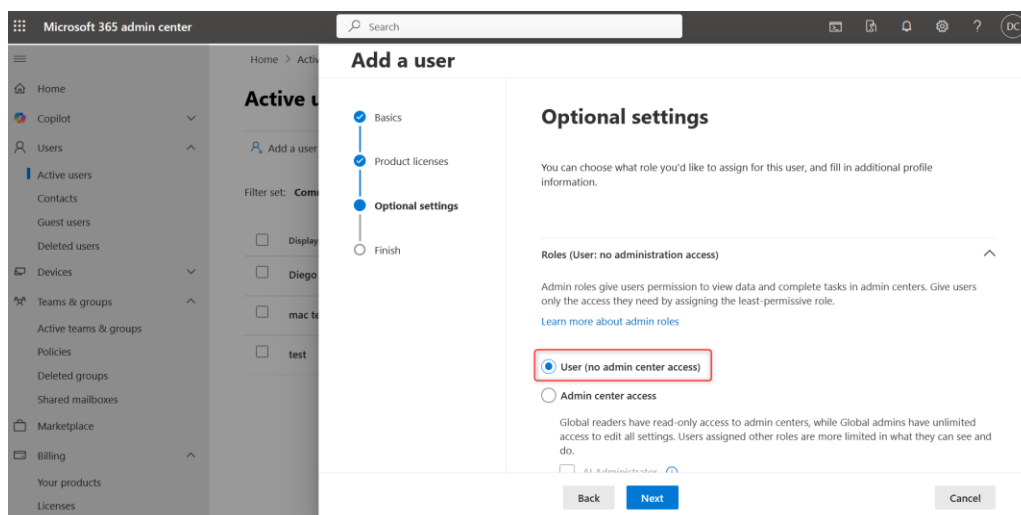
When creating a user, ensure that the account is assigned an appropriate usage location, as licensing availability depends on this attribute.



Then select **location** and assign the specific **license**.



Next to other options, you would select No admin centre access or yes to choose the correct privileges.



Then **Review** user parameters and **save** it.

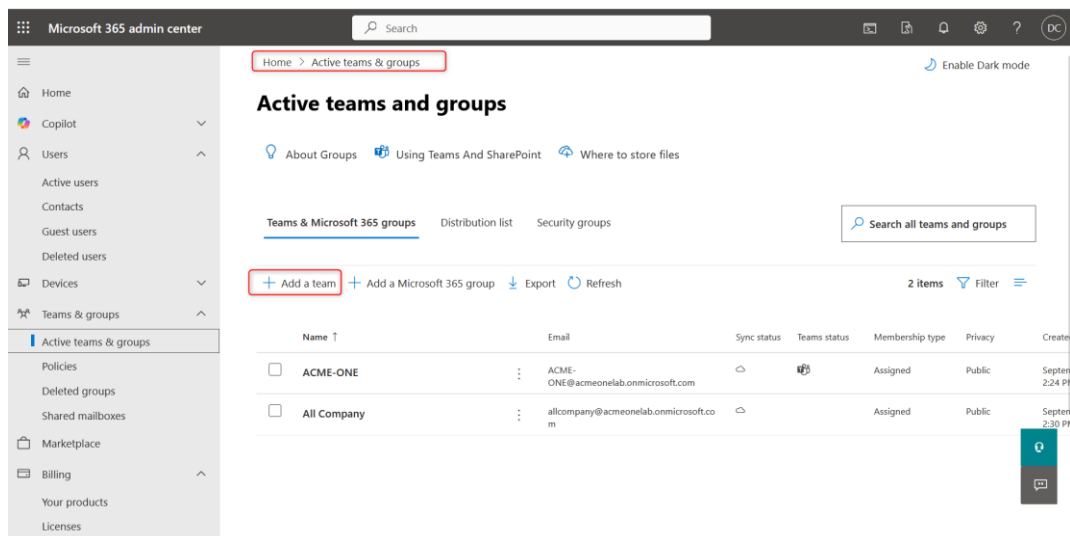
2. Creating a Group

To create a group that can be used for Intune policy targeting or license assignment, go to:

Teams & groups → Active teams & groups

This section allows you to view and create Microsoft 365 groups, security groups, and distribution lists. Groups may be used to organize users for easier license assignment or compliance policy targeting.

Your screenshot shows the available groups (ACME-ONE, All Company), and the action bar offering options such as **Add a Microsoft 365 group** and **Add a team**. These options may differ slightly depending on the tenant type and enabled services.



Microsoft 365 admin center

Home > Active teams and groups

Active teams and groups

About Groups Using Teams And SharePoint Where to store files

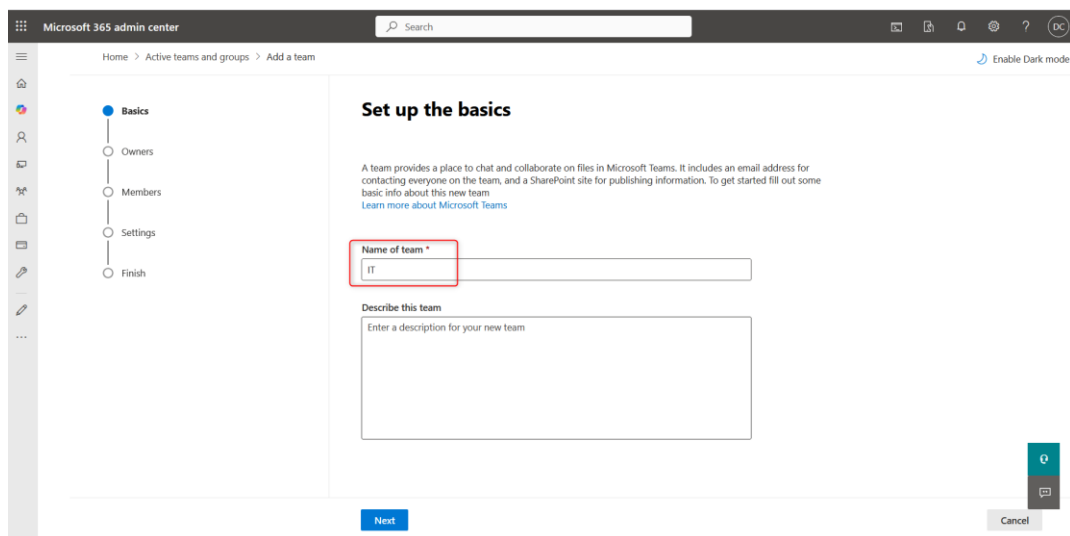
Teams & Microsoft 365 groups Distribution list Security groups

Search all teams and groups

+ Add a team + Add a Microsoft 365 group Export Refresh

2 items Filter

Name	Email	Sync status	Teams status	Membership type	Privacy	Created
ACME-ONE	ACME-ONE@acmeonlab.onmicrosoft.com			Assigned	Public	September 2, 2024
All Company	allcompany@acmeonlab.onmicrosoft.com			Assigned	Public	September 2, 2024



Microsoft 365 admin center

Home > Active teams and groups > Add a team

Set up the basics

A team provides a place to chat and collaborate on files in Microsoft Teams. It includes an email address for contacting everyone on the team, and a SharePoint site for publishing information. To get started fill out some basic info about this new team. [Learn more about Microsoft Teams](#)

Name of team *

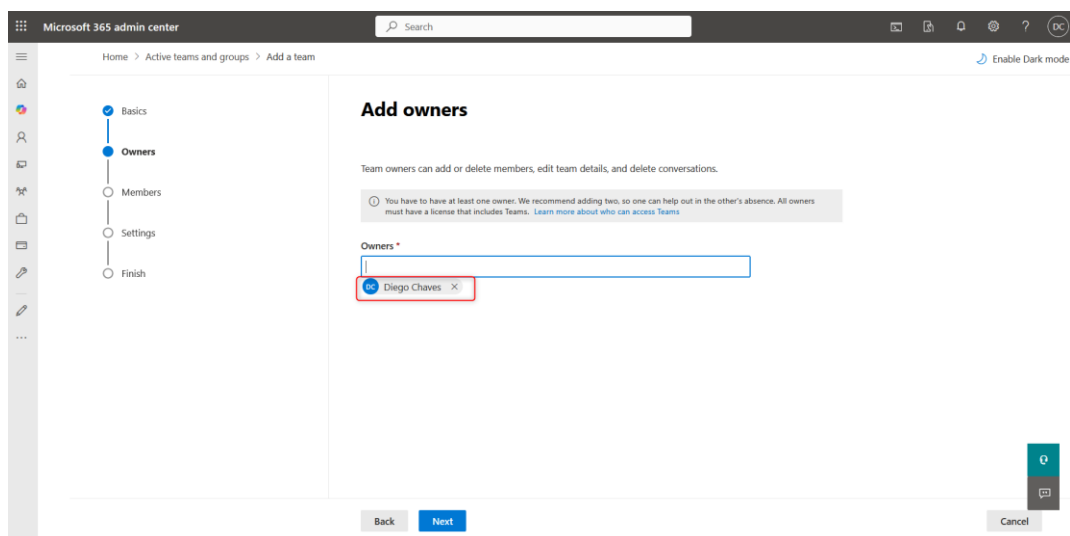
IT

Describe this team

Enter a description for your new team

Next Cancel

Assigning at least one owner to the Group



Microsoft 365 admin center

Home > Active teams and groups > Add a team

Add owners

Team owners can add or delete members, edit team details, and delete conversations.

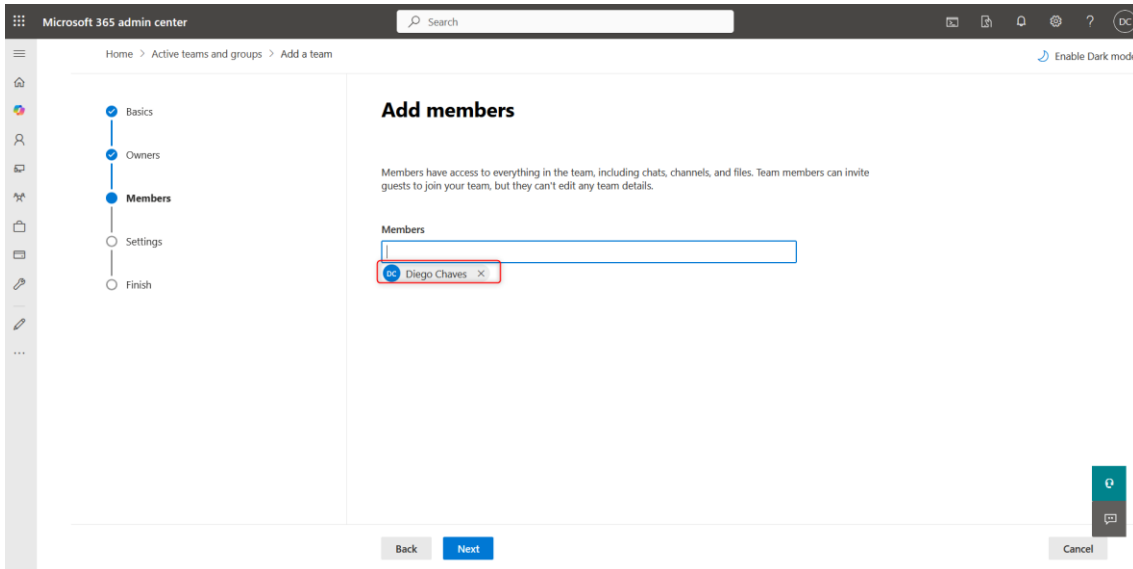
You have to have at least one owner. We recommend adding two, so one can help out in the other's absence. All owners must have a license that includes Teams. [Learn more about who can access Teams](#)

Owners *

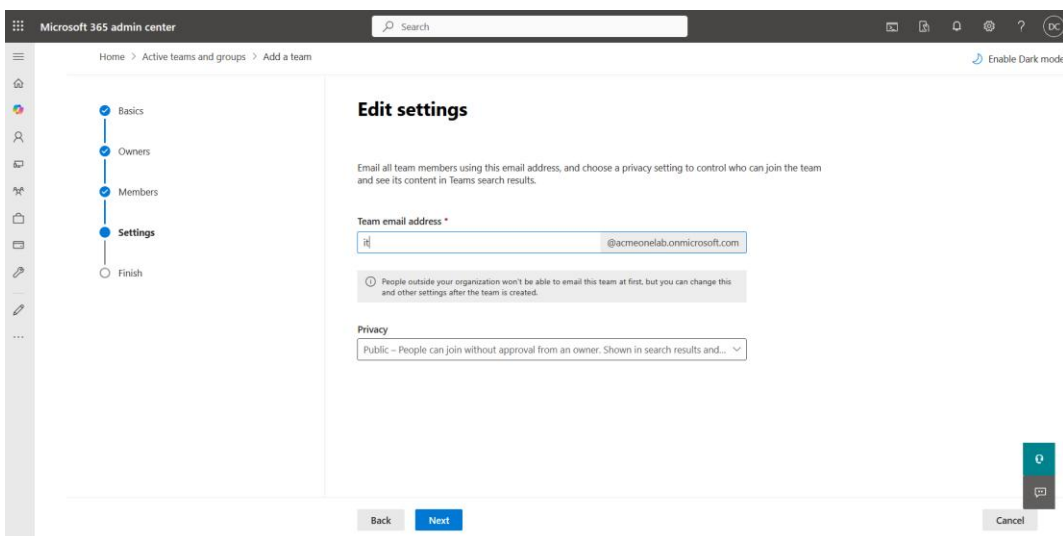
Diego Chaves

Back Next Cancel

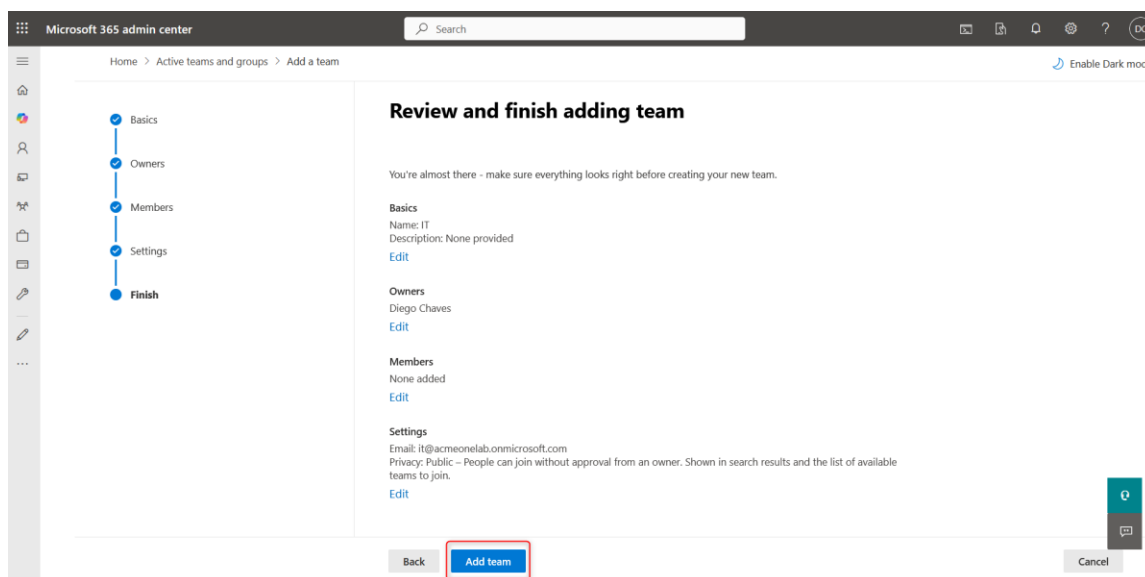
You can add members to the group now or add them later.



Choose an email to all team members.



Then **Review** and Add Team

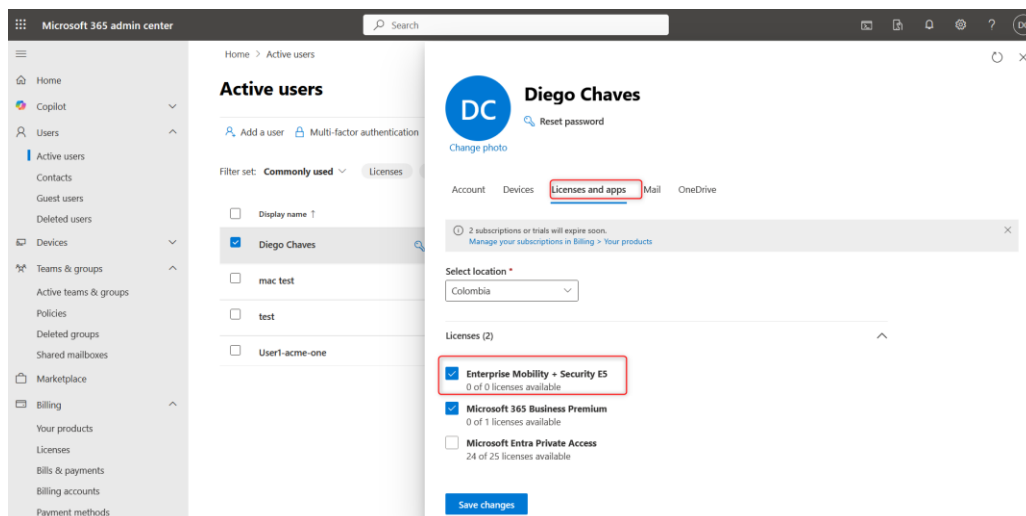


3. Assigning Licenses to Users or Groups

Once the required user or group exists, licenses can be assigned to enable Intune functionality.

To assign a license to a user, go to:

Users → Active users → Select the user → Licenses and Apps



Assigning Intune Under Mobility MDM and WIP

To add the user to the Microsoft Intune application under *Mobility (MDM and WIP)*, follow the navigation inside the Microsoft Entra Admin Centre.

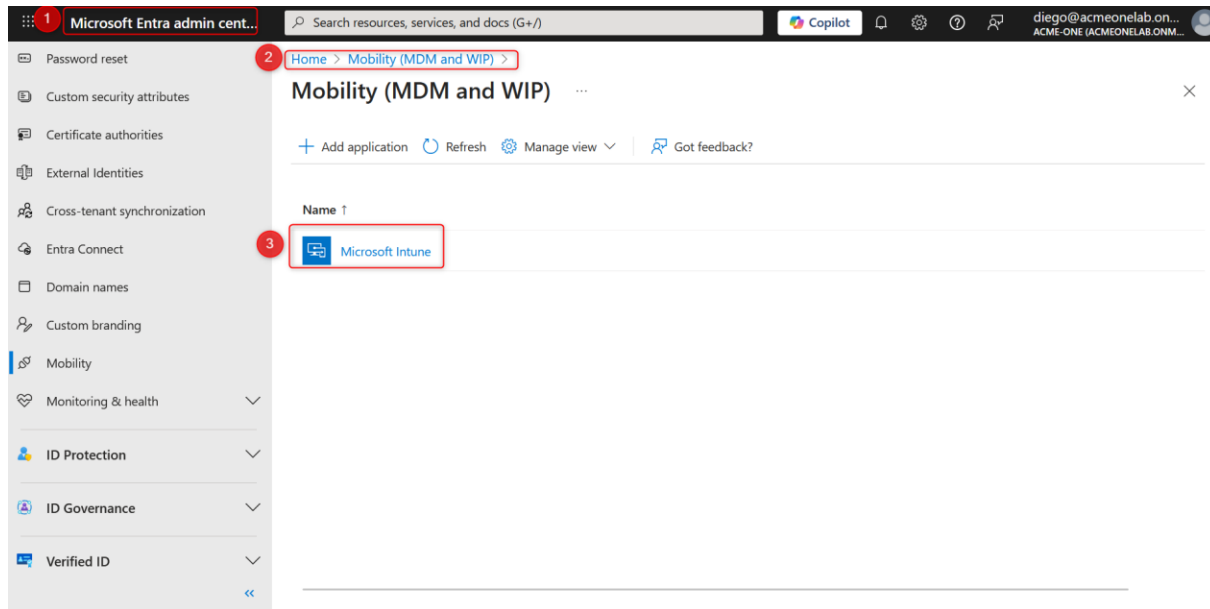
Access Microsoft Entra

- Log in to the Microsoft Entra admin portal:

<https://entra.microsoft.com>

Navigate to Mobility (MDM and WIP)

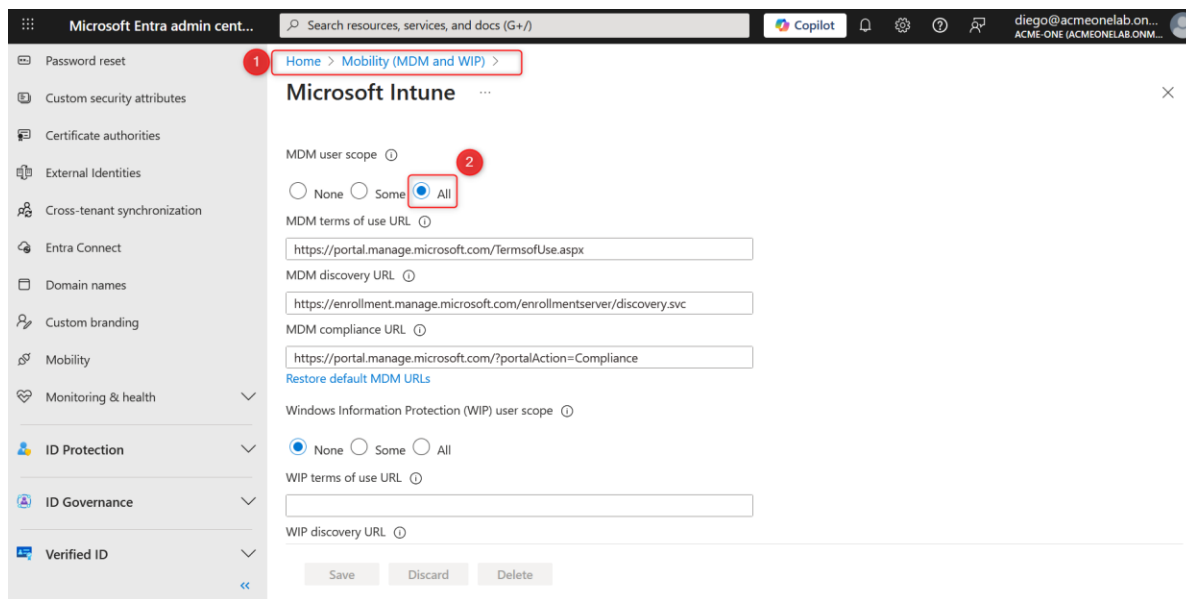
- In the left navigation panel, go to **Home**.
- Select Mobility (MDM and WIP).
- Open the **Microsoft Intune** application.



Inside the *Microsoft Intune* page under *Mobility (MDM and WIP)*, validate or modify the **MDM user scope**.

By default, **All** is selected, which allows all users in the directory to enroll devices into Intune.

If your environment requires stricter control or you have limited licenses, change the scope to **Some** and select a specific group. Leave the default **All** if every user should be allowed to enroll.



Configure App Registration

To create the application required for communication between Versa SASE Gateway and the Microsoft Graph API, follow the steps below inside the Microsoft Entra Admin Center.

1. Navigate to App Registrations

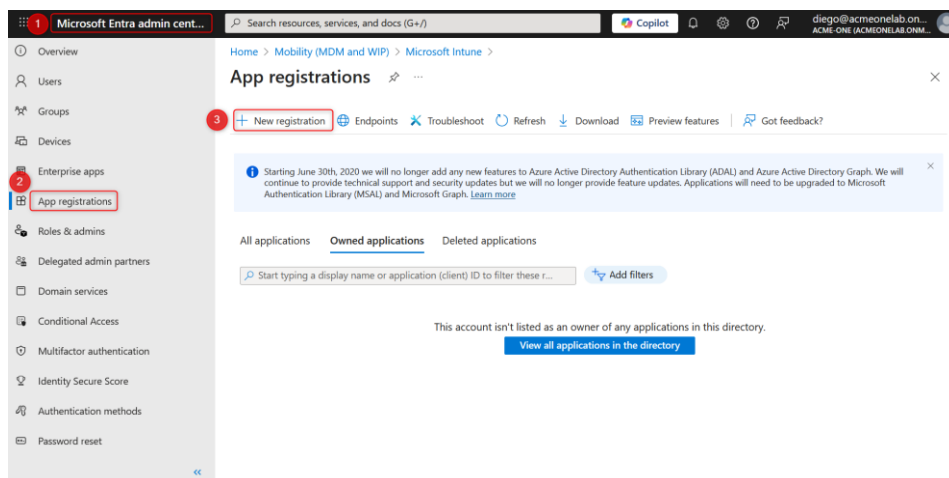
Inside the Microsoft Entra Admin Center, go to:

Home > Mobility (MDM and WIP) > Microsoft Intune > App registrations

This page displays all existing applications registered in the tenant.

2. Create a New Application

Select **New registration** to start creating the application that will be used by Versa for UEM (MDM) integration.



Provide Application Details

In the Register an application page:

- Enter a **Name** for the application (for example: *ACME-ONE*).
- Under Supported account types, select:

Accounts in this organizational directory only (Single-tenant)

This option restricts usage to your Entra tenant, which is required for Versa integrations.

Register the Application

Select **Register** to finalize creation of the application.

Once registered, the app will generate identifiers (Tenant ID, Client ID, and Client Secret later) that are required for configuration in Versa Concerto.

Home > Mobility (MDM and WIP) > Microsoft Intune > Enterprise applications | All applications > App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

1 ACME-ONE ✓

Supported account types

Who can use this application or access this API?

- 2 ☒ Accounts in this organizational directory only (ACME-ONE only - Single tenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

3 By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

After registering application go to **App registrations > All applications** and Click your previously created app (Example ACME-ONE).

Microsoft Entra admin center

Home > App registrations

+ New registration | Endpoints | Troubleshoot | Refresh | Download | Preview features | Got feedback?

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

2 All applications | Owned applications | Deleted applications

Start typing a display name or application (client) ID to filter these r... | Add filters

2 applications found

Display name ↑	Application (client) ID	Created on ↑↓	Certificates & secrets
Concert-Intune-acmeone	18bea91a-611e-4108-b446-40a0902b764e	9/8/2025	Current
P2P Server	8b1b2ec7-e071-4781-8582-11fdea078799	9/10/2025	-

3. Retrieve Required Identifiers

Inside the App Registration **Overview** page, copy the following values:

- Application (Client) ID

- Directory (Tenant) ID

These two values will be required when configuring the Intune MDM profile in Versa Concerto.

Home > Mobility (MDM and WIP) > Microsoft Intune > Enterprise applications | All applications > App registrations >

Concert-Intune-acmeone ✕

Search « Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Essentials

Display name
[Concert-Intune-acmeone](#)

Application (client) ID
18bea91a-611e-4108-b446-40a0902b764e

Object ID
1b1cac51-00cc-4502-8646-be6ece71f52c

Directory (tenant) ID
92896a25-7228-4f74-9bf4-fc31c21284be

Supported account types
[My organization only](#)

Client credentials
[0 certificate, 1 secret](#)

Redirect URIs
[Add a Redirect URI](#)

Application ID URI
[Add an Application ID URI](#)

Managed application in local directory
[Concert-Intune-acmeone](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

[Get Started](#) [Documentation](#)

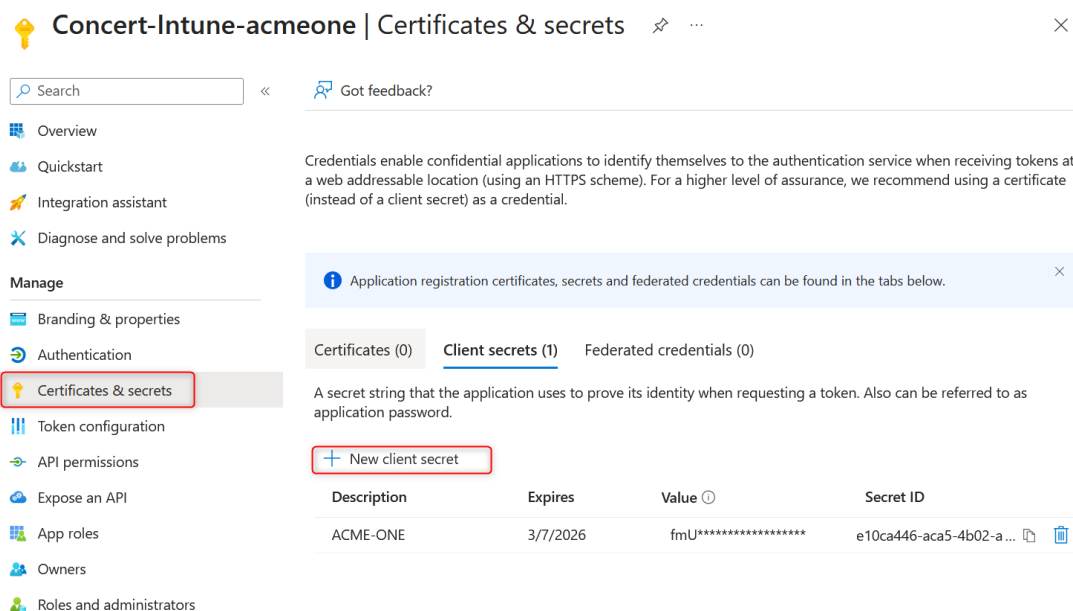
4. Generating a Client Secret

From the same application:

- Go to Certificates & secrets.
- Under Client secrets, select New client secret.
- Provide a description, choose an expiration option, and create the secret.
- Copy the **Value** of the secret immediately (it will not be shown again).

This Client Secret is required for Versa to authenticate against Microsoft Graph when retrieving device information.

Home > Mobility (MDM and WIP) > Microsoft Intune > Enterprise applications | All applications > App registrations > Concert-Intune-acmeone



Concert-Intune-acmeone | Certificates & secrets

Search < Got feedback?

Overview
Quickstart
Integration assistant
Diagnose and solve problems

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
ACME-ONE	3/7/2026	fmU*****	e10ca446-aca5-4b02-a...  

5. Configure API Permissions

To allow Sase gateway to read device compliance data from Microsoft Intune, configure the required API permissions on the Azure App Registration.

Navigate to the API Permissions Page

- In the Microsoft Entra admin center, go to:
App registrations > All applications > Select the application you created earlier
- In the left menu, select **API permissions**.

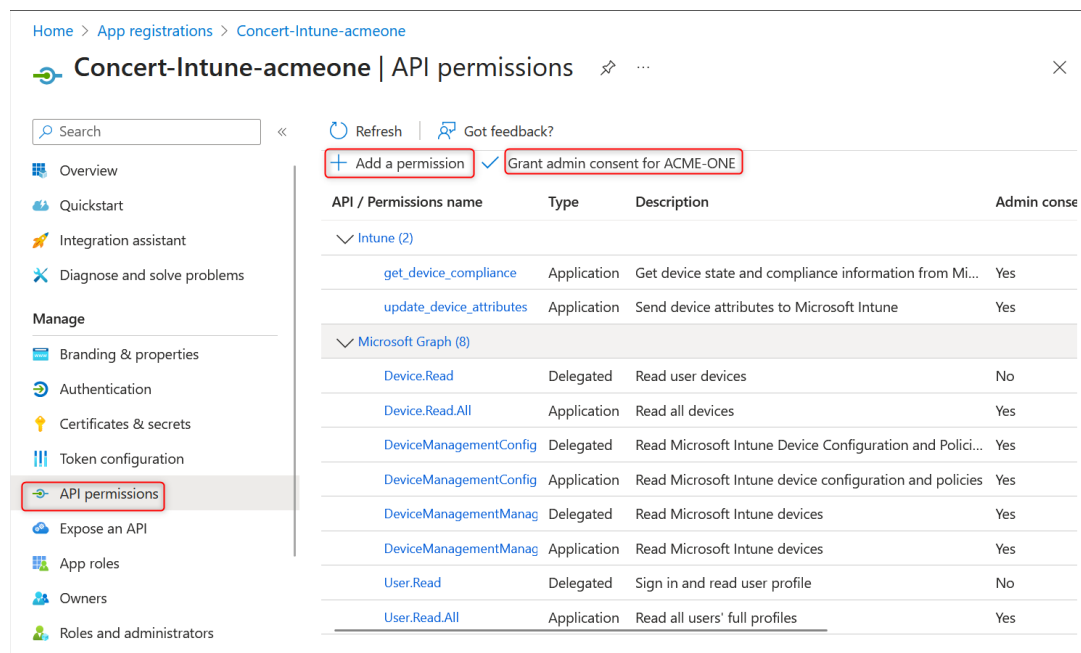
Add Required Permissions

- Click Add a permission.
- Select at least all permissions shown in the next image, which include the required Intune and Microsoft Graph application permissions:
 - Intune
 - get_device_compliance
 - update_device_attributes
 - Microsoft Graph
 - Device.Read.All
 - User.Read.All

Grant Tenant-Wide Consent

- After adding the permissions, click **Grant admin consent for <TenantName>** (Example ACME-ONE).
- Verify that the permissions show **Admin consent = Yes**.

These permissions ensure that the UEM integration in Versa Concerto can retrieve device posture and compliance attributes from Intune.



Home > App registrations > Concert-Intune-acmeone

Concert-Intune-acmeone | API permissions

Search Refresh Got feedback?

+ Add a permission ✓ Grant admin consent for ACME-ONE

API / Permissions name	Type	Description	Admin conse
Intune (2)			
get_device_compliance	Application	Get device state and compliance information from Mi...	Yes
update_device_attributes	Application	Send device attributes to Microsoft Intune	Yes
Microsoft Graph (8)			
Device.Read	Delegated	Read user devices	No
Device.Read.All	Application	Read all devices	Yes
DeviceManagementConfig	Delegated	Read Microsoft Intune Device Configuration and Polici...	Yes
DeviceManagementConfig	Application	Read Microsoft Intune device configuration and policies	Yes
DeviceManagementManag	Delegated	Read Microsoft Intune devices	Yes
DeviceManagementManag	Application	Read Microsoft Intune devices	Yes
User.Read	Delegated	Sign in and read user profile	No
User.Read.All	Application	Read all users' full profiles	Yes

6. Assign Users and Groups

To authorize which identities are allowed to use the registered Intune application for this integration, assign the appropriate users or groups inside **Enterprise Applications**.

From the Microsoft Entra admin center:

Enterprise applications > All applications > Select your Intune app > Users and groups

Once inside the *Users and Groups* panel:

- Select Add user/group.
- Choose the user(s) or group(s) that will be permitted to use this application for the UEM (MDM) integration.
- Confirm the assignment.

This ensures only the selected identities are allowed to authenticate against the registered Intune

application used by Versa SASE Gateway

Home > Enterprise applications | All applications > Concert-Intune-acmeone

Concert-Intune-acmeone | Users and groups

Enterprise Application

« **+ Add user/group** Edit assignment Remove assignment Update credential Re

Overview

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups**
- Single sign-on
- Provisioning
- Application proxy
- Self-service

Users and groups

The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in properties this.

Assign users and groups to app-roles for your application here. To create new app-roles for this application [application registration](#)

First 200 shown, search all users & groups

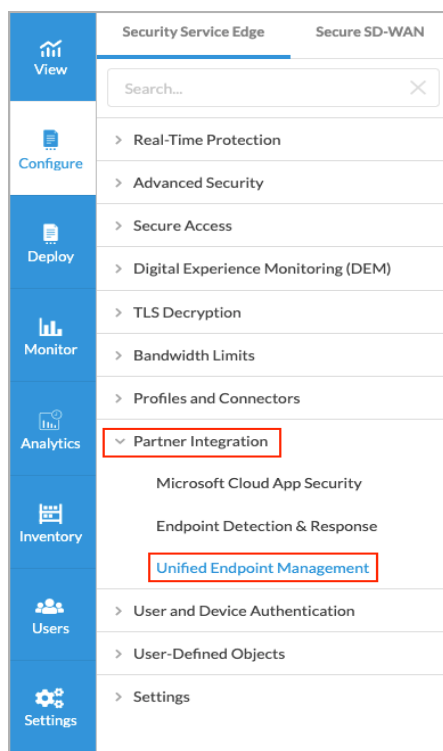
	Display name
<input type="checkbox"/>	DC Diego Chaves
<input type="checkbox"/>	T test

Configuration in Concerto

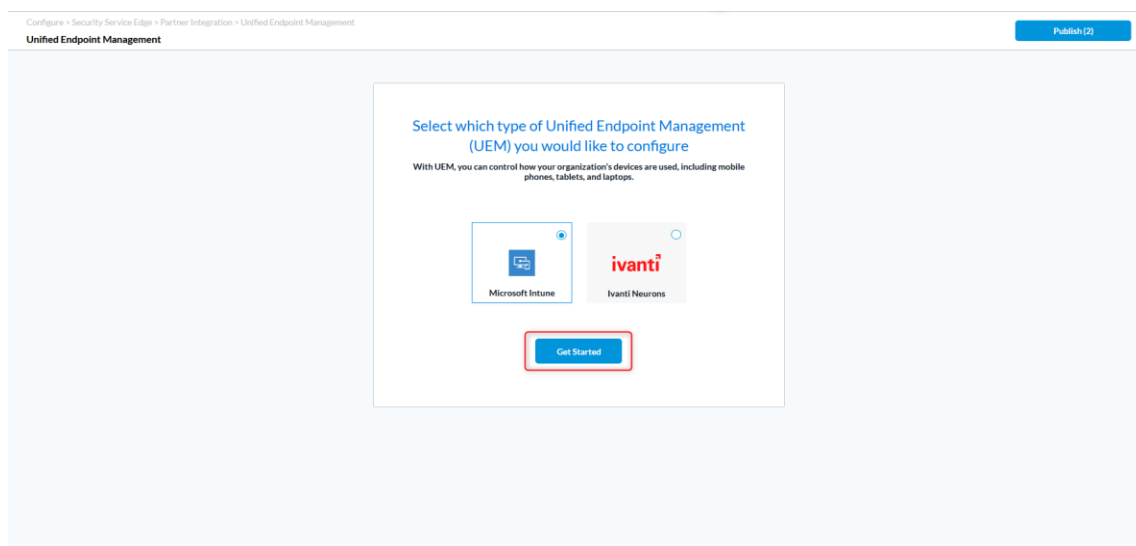
Integration with Accessing Unified Endpoint Management

To begin the Intune MDM setup and integrate it with **Concerto 12.2.x**, go to:

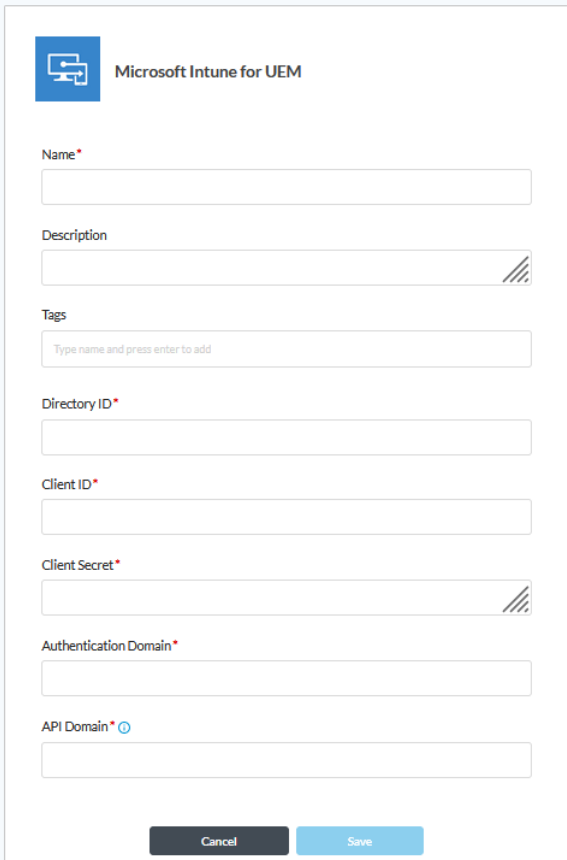
Configure > Security Service Edge (SSE) > Partner Integration > Unified Endpoint Management



In the **Unified Endpoint Management** screen, select **Microsoft Intune**, and then click **Get Started** to begin configuring the Intune MDM integration.



To continue the Intune MDM configuration inside Versa Concerto, fill in the fields shown in the **Microsoft Intune for UEM** screen.



Microsoft Intune for UEM

Name*

Description

Tags
Type name and press enter to add

Directory ID*

Client ID*

Client Secret*

Authentication Domain*

API Domain* ⓘ

Cancel Save

The following table provides a short description for each field that appears in the form.

Field	Description
Name (Required)	Enter a name for the UEM profile.
Description	Enter a text description for the UEM profile.
Tags	Enter tags to associate with the UEM profile.
Directory ID (Required)	Enter the tenant or directory ID registered on the graph (Intune) server.
Client ID (Required)	Enter the client identifier provided by the graph (Intune) server, in string format.


Client Secret (Required)	Enter the client secret provided by the graph (Intune) server, in string format.
Authentication Domain (Required)	Enter the domain name to use for authentication. login.microsoftonline.com
API Domain (Required)	Enter the domain name to use for APIs. graph.microsoft.com

In the previous section **Configure App Registration**, you obtained the values required here:

- Directory (Tenant) ID
- Application (Client) ID
- Client Secret

Note: The **Authentication Domain** and **API Domain** values shown on table represent the standard default values used in most **Microsoft Intune integrations**. These values apply to regular commercial tenants. Environments using sovereign clouds or specialised infrastructure may require different domain values.

These are the same values that must be entered into the corresponding fields in Concerto.


Microsoft Intune for UEM

Name *

Description

Tags

Directory ID *

Client ID *

Client Secret *

Authentication Domain *

API Domain * ⓘ

Windows OS Enrollment

To ensure that Microsoft Intune can evaluate the device posture (compliant or non-compliant) and allow **Versa SASE Gateway** to retrieve this information during Secure Access validation, each Windows device must be enrolled into Intune.

Enroll Client Machine	Start Enrollment	Authenticate	Restart & Sign In	Verify Enrollment
<p>Example:</p> <p>test devices</p> <p>(one with Firewall disabled > non-compliant)</p>	<p>Open in Edge or Chrome:</p> <p>Paste ms-device-enrollment:?mode=aad</p> <p>Or Go to Settings > Accounts > Access work or school then Connect</p>	<p>Enter email + password.</p> <p>Select Join > click Done.</p>	<p>Reboot PC.</p> <p>Select Other user → sign in with same enrollment credentials.</p>	<p>Check that the Intune MDM certificate is present in the Computer certificate store.</p>

Configuration in Microsoft Intune – Create Windows Compliance Policies

1. create a compliance policy

To define the compliance criteria that Versa will read from Intune during access checks, create a compliance policy in Microsoft Intune.

Navigation

Go to:

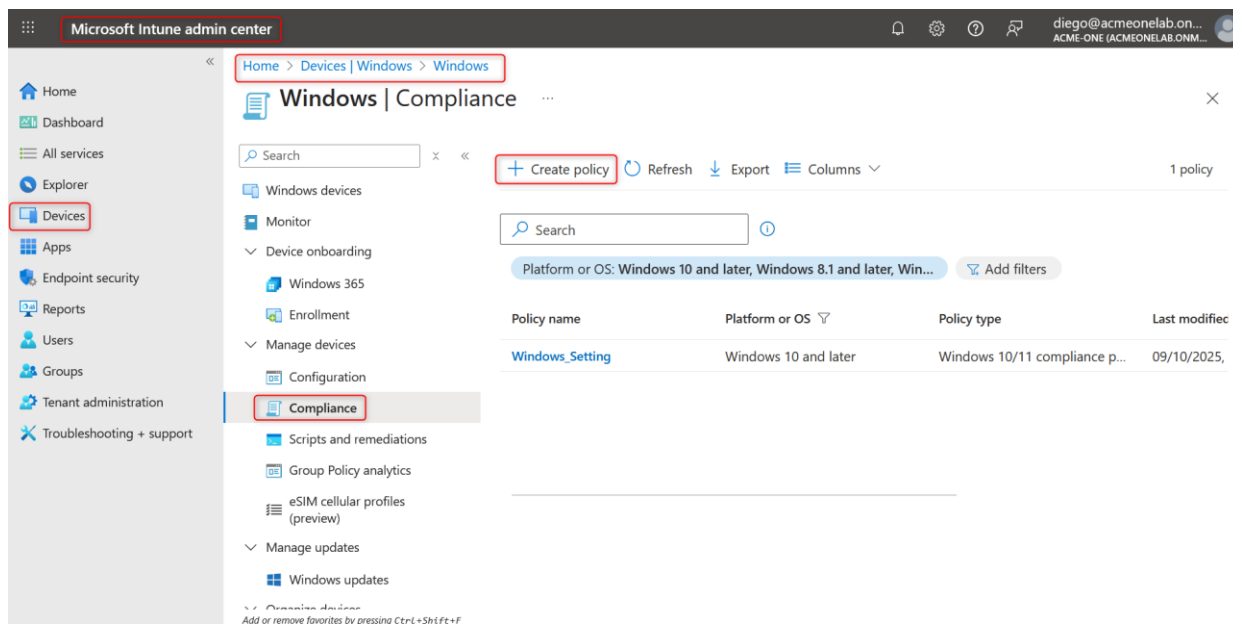
<https://endpoint.microsoft.com>

Inside the Intune admin center **for Windows devices**, go to:

Devices > Windows > Compliance > Create policy

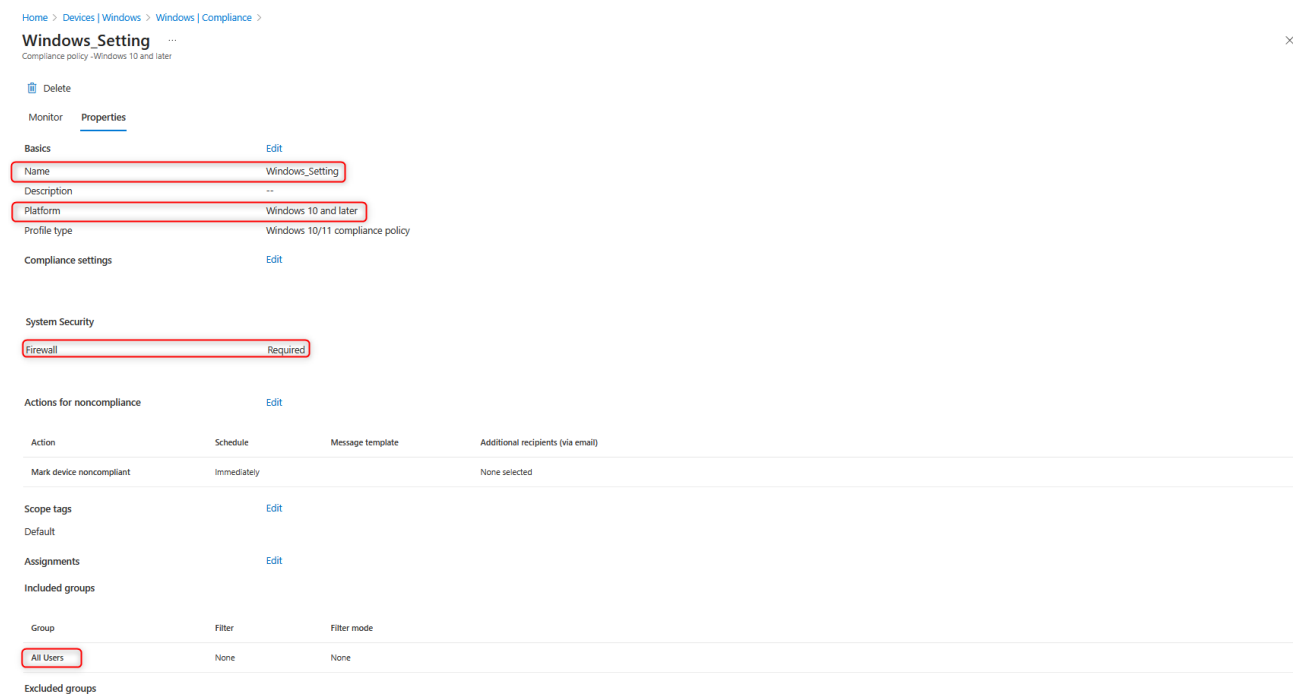
Description

Use this section to configure the compliance posture that Windows devices must satisfy (Example, OS version, security settings, encryption, TPM, antivirus). The compliance state generated from this policy is what Versa retrieves during Secure Access registration and gateway authentication.



Example Compliance Policy

As an example in policy, the requirement is set for the **Firewall** to be enabled, and the policy is assigned to the **All Users** group. The slide illustrates how a basic Windows compliance rule appears once created.



2. Review Compliance Policy Example

Device Enrollment (Compliance Policy Example)

This example shows how a Windows compliance policy appears once configured in Microsoft Intune. The policy named **Windows_Setting** is applied to **Windows 10 and later** devices and includes a requirement for the **Firewall** to remain enabled. The policy is assigned to **All Users**, ensuring that every user targeted by the policy must meet these compliance conditions before their device is considered compliant by Intune.

Home > Devices | Windows > Windows | Compliance >

Windows_Setting

Compliance policy - Windows 10 and later

Delete

Monitor Properties

Basics [Edit](#)

Name Windows_Setting

Description --

Platform Windows 10 and later

Profile type Windows 10/11 compliance policy

Compliance settings [Edit](#)

System Security

Firewall Required

Actions for noncompliance [Edit](#)

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		None selected

Scope tags [Edit](#)

Default

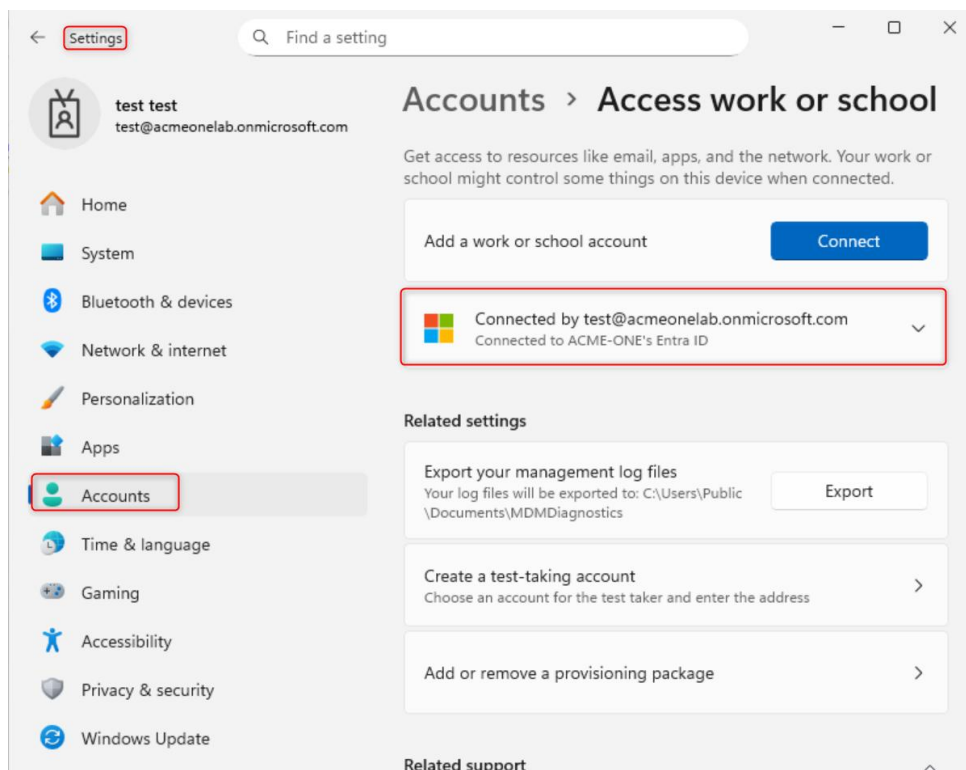
Assignments [Edit](#)

Included groups

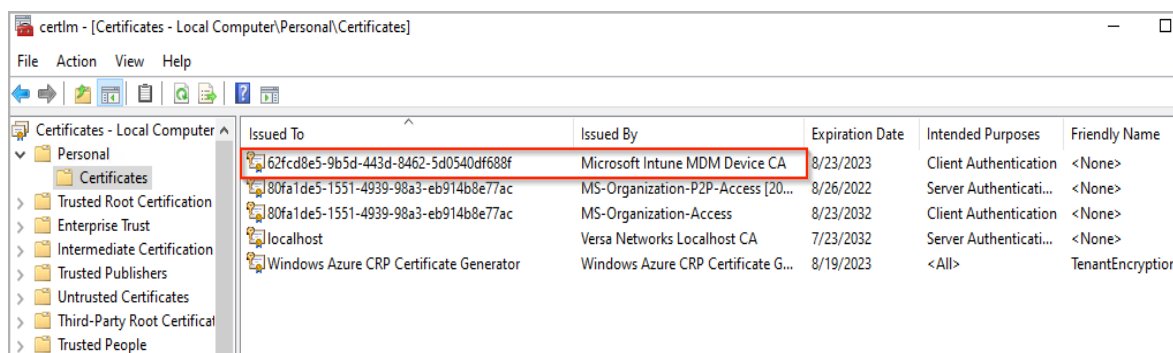
Group	Filter	Filter mode
All Users	None	None

Excluded groups

On a Windows device, once it is successfully joined to Microsoft Entra ID via a work or school account, it appears as *Connected*.



Once enrollment is complete, Intune issues the **Microsoft Intune MDM Device CA** certificate, which appears in the local computer certificate store. This certificate confirms that the Windows device is successfully enrolled and ready to report compliance status to Intune.



3. confirm Windows device has synchronized on Intune

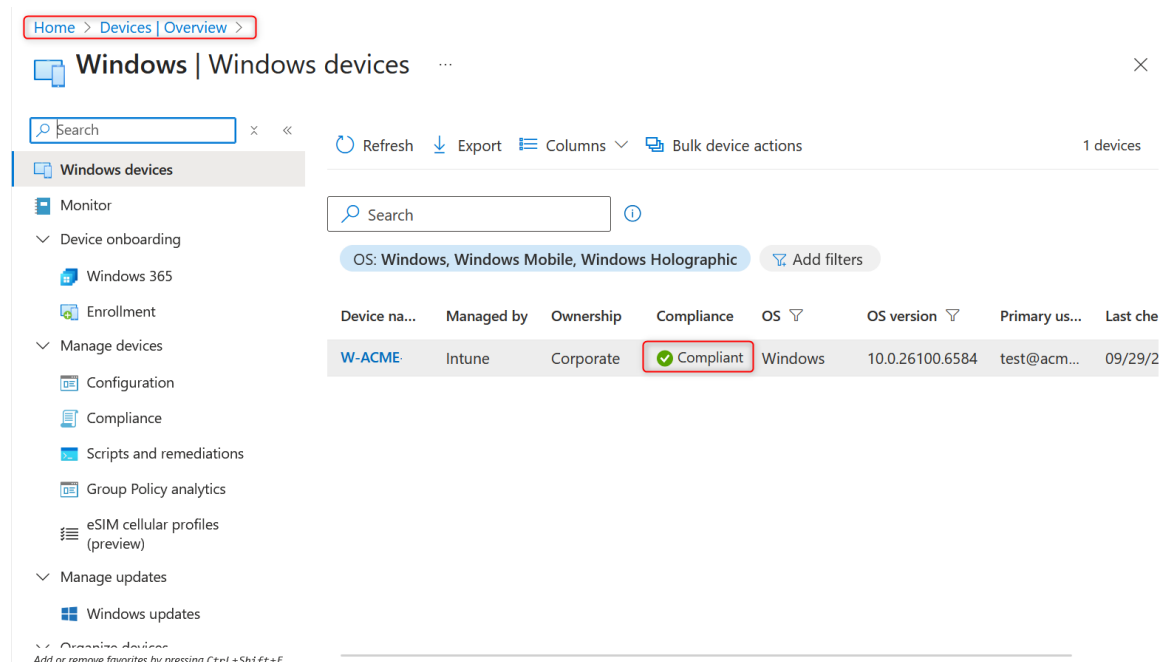
To confirm that your enrolled Windows device has synchronized with Intune and is reporting its compliance posture, check the device list inside the **Microsoft Intune admin center**.

Inside the Intune admin center go to:

Devices > Windows > Windows devices

Description

After enrollment, Windows devices may take **10–15 minutes** to appear in the Microsoft Endpoint Manager portal.



The screenshot shows the Microsoft Endpoint Manager portal interface. The breadcrumb navigation at the top reads 'Home > Devices | Overview >'. The main heading is 'Windows | Windows devices'. Below this is a search bar and a list of actions: Refresh, Export, Columns, and Bulk device actions. The left sidebar contains a list of navigation items: Monitor, Device onboarding, Windows 365, Enrollment, Manage devices, Configuration, Compliance, Scripts and remediations, Group Policy analytics, eSIM cellular profiles (preview), and Manage updates. The main content area displays a table of devices. The table has columns: Device name, Managed by, Ownership, Compliance, OS, OS version, Primary user, and Last checked. A single device is listed: 'W-ACME', managed by 'Intune', with 'Corporate' ownership. The 'Compliance' column for this device shows a green checkmark and the word 'Compliant', which is highlighted with a red box. The 'OS' is 'Windows', 'OS version' is '10.0.26100.6584', 'Primary user' is 'test@acm...', and 'Last checked' is '09/29/2021'.

Once the device is listed, the **Compliance** column will indicate whether the device is **Compliant** or **Non-compliant**, based on the compliance policy previously configured.

This allows you to verify that the device enrollment was successful and that Intune is evaluating the device correctly.

Apply Secure Access Rules for Intune-Managed Devices

In **Concerto**, go to:

Configure > Security Service Edge (SSE) > Secure Access > Client-based Access > Policy Rules

1. Configure Policy Rule Criteria

On the **Policy Rules** page, click + **Add** to create a new Secure Client Access rule, **or choose an existing rule from the list that you want to apply.**

This rule will control access for **compliant** and **non-compliant** devices.

VERSA ACME-ONE CONFIGURATION

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Client-based Access Rules

Below are all the rules for your Secure Client-based Access.

Rule Name	Operating System Versions	Users & Groups	Endpoint Posture		Traffic Action	VPN & Gateway Groups	Status	Last Modified By & Date
			EIP & Entity Risk Bands	Device Compliance Status				
<input type="checkbox"/> Secure_Access_Windows_Profile_LDAP_Us...er_Certificate	<input checked="" type="checkbox"/> Windows <input type="checkbox"/> Windows 10 <input type="checkbox"/> Windows 10 Mobile <input type="checkbox"/> Windows 11 More Details	<input checked="" type="checkbox"/> AD_Server_Acme...One <input type="checkbox"/> Users <input type="checkbox"/> Diego Chaves <input type="checkbox"/> lab@diegolab-versa.net <input type="checkbox"/> VIP1.vip1@acme-one.com	<input checked="" type="checkbox"/> Endpoint Information Profile (EIP) <input checked="" type="checkbox"/> User Defined <input type="checkbox"/> EIP_Profile_Windows_Re...gistry <input type="checkbox"/> Entity Risk Bands <input type="checkbox"/> All risk bands	<input checked="" type="checkbox"/> Managed Status of Devices <input type="checkbox"/> All Devices	<input type="checkbox"/> Action <input type="checkbox"/> Send Apps to Versa Cloud <input type="checkbox"/> No Client Applications selected <input checked="" type="checkbox"/> Exclude PreDefined Applications <input type="checkbox"/> Facebook	<input checked="" type="checkbox"/> VPN Name <input type="checkbox"/> ACME-ONE-Enterprise <input checked="" type="checkbox"/> Gateway Groups <input type="checkbox"/> Default <input checked="" type="checkbox"/> Gateways <input type="checkbox"/> SaseGWDiegolab	Enabled	11/21/2025, 11:53:34 AM Administrator
<input type="checkbox"/> Secure_Access_Windows_Profile	<input checked="" type="checkbox"/> Windows <input type="checkbox"/> Windows 10 <input type="checkbox"/> Windows 10 Mobile <input type="checkbox"/> Windows 11 More Details	<input checked="" type="checkbox"/> ENTRA-ID-SAML <input type="checkbox"/> Users <input type="checkbox"/> vip2@diegolab-versa.a.onmicrosoft.com <input type="checkbox"/> vip3@diegolab-versa.a.onmicrosoft.com <input type="checkbox"/> vip4@diegolab-versa.a.onmicrosoft.com	<input checked="" type="checkbox"/> Endpoint Information Profile (EIP) <input type="checkbox"/> All devices <input type="checkbox"/> Entity Risk Bands <input type="checkbox"/> All risk bands	<input checked="" type="checkbox"/> Managed Status of Devices <input type="checkbox"/> All Devices	<input type="checkbox"/> Action <input type="checkbox"/> Breakout to the Internet <input type="checkbox"/> No Client Applications selected <input type="checkbox"/> No Predefined Applications selected	<input checked="" type="checkbox"/> VPN Name <input type="checkbox"/> ACME-ONE-Enterprise <input checked="" type="checkbox"/> Gateway Groups <input type="checkbox"/> Default <input checked="" type="checkbox"/> Gateways <input type="checkbox"/> SaseGWDiegolab	Enabled	11/21/2025, 11:53:34 AM Administrator
<input type="checkbox"/> Secure_Access_Windows_MDM	<input checked="" type="checkbox"/> Windows <input type="checkbox"/> Windows 10 <input type="checkbox"/> Windows 10 Mobile <input type="checkbox"/> Windows 11 More Details	<input checked="" type="checkbox"/> AD_Server_Acme...One <input type="checkbox"/> Users <input type="checkbox"/> Diego Chaves <input type="checkbox"/> lab@diegolab-versa.net	<input checked="" type="checkbox"/> Endpoint Information Profile (EIP) <input type="checkbox"/> All devices <input type="checkbox"/> Entity Risk Bands <input type="checkbox"/> All risk bands	<input checked="" type="checkbox"/> Managed Status of Devices <input type="checkbox"/> Managed Devices <input checked="" type="checkbox"/> Device Compliance Status <input type="checkbox"/> compliance	<input type="checkbox"/> Action <input type="checkbox"/> Breakout to the Internet <input type="checkbox"/> No Client Applications selected <input type="checkbox"/> No Predefined Applications selected	<input checked="" type="checkbox"/> VPN Name <input type="checkbox"/> ACME-ONE-Enterprise <input checked="" type="checkbox"/> Gateway Groups <input type="checkbox"/> Default <input checked="" type="checkbox"/> Gateways <input type="checkbox"/> SaseGWDiegolab	Enabled	9/25/2025, 3:21:21 PM Administrator

Showing 1-4 of 4 results 10 Rows per Page Go to page 1 < Previous 1 Next >

In the Client-based Access Rule wizard, complete the following steps:

Step 1 – Operating System

Select the operating system platforms that this rule will apply to (Windows, macOS, iOS, Android, Linux).

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Create Client-based Access Rule

Operating System Users & Groups Endpoint Posture Source Geo Location & Source IP Address Traffic Action Gateways Client Configuration Agent Profile From EIP Review & Configure

Choose the operating system for this rule below.

If you prefer, you can customize which operating system options you would like to enable for the rule.

Windows

☐ All Windows Operating Systems

☐ User Defined

☐ Oper-1

☐ testGoWindows

☐ test-yin-rik

☐ test-yin-pa

☐ Predefined

☐ Windows 10

☐ Windows 10 Mobile

☐ Windows 11

☐ Windows 7

☐ Windows 8

☐ Windows 8.1

☐ Windows Server 2012

Apple

☐ All Apple Operating Systems

☐ User Defined

☐ testGo

☐ Predefined

☐ Mac OS X Server

☐ OS X

☐ Mac OS

☐ All Apple Mobile

☐ User Defined

☐ testGoIpad

☐ Predefined

☐ iOS

☐ iPadOS

Android

☐ All Android Operating Systems

☐ User Defined

☐ testGoAndroid

☐ testGoAndroid01

☐ Predefined

☐ Android

Linux

☐ All Linux Operating Systems

☐ User Defined

☐ testGoLinux

☐ testGoNew

☐ Predefined

☐ Fedora

☐ Linux

☐ Red Hat Enterprise Linux

☐ Ubuntu

Cancel Back Skip to Review Next

Step 2 – Users and Groups

Choose the users or groups that should be included in this access rule.

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Create Client-based Access Rule

Operating System **Users & Groups** Endpoint Posture Source Geo Location & Source IP Address Traffic Action Gateways Client Configuration Agent Profile From EIP Review & Configure

By default we have chosen all users and groups to apply your security enforcements
If you prefer, you can select the specific users or groups for the security posture.

Users & Groups

✓ Known Users

[Customize](#)

[Cancel](#) [Back](#) [Skip to Review](#) [Next](#)

Endpoint Posture

In the **Device Compliance Status** section, select:

- Managed Devices
- **Compliant** (to allow devices that pass Intune policies)

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure_Access_Windows_MDM

Operating System Users & Groups **Endpoint Posture** Source Geo Location & Source IP Address Traffic Action Gateways Client Configuration Agent Profile From EIP Review & Configure

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.
If you'd like, you can customize your options by choosing what to include or exclude below.

← Back

Device Compliance Status

If 3rd party UEM is used, select one or more device compliance status below

☐ All Devices
 ☒ **Managed Devices**
 ☐ Unmanaged Devices

☒ **Compliance**
 ☐ Non-Compliant
 ☐ Config-Manager
 ☐ Conflict
 ☐ In-Grace-Period
 ☐ Error
 ☐ Unknown

[Cancel](#) [Back](#) [Skip to Review](#) [Next](#)

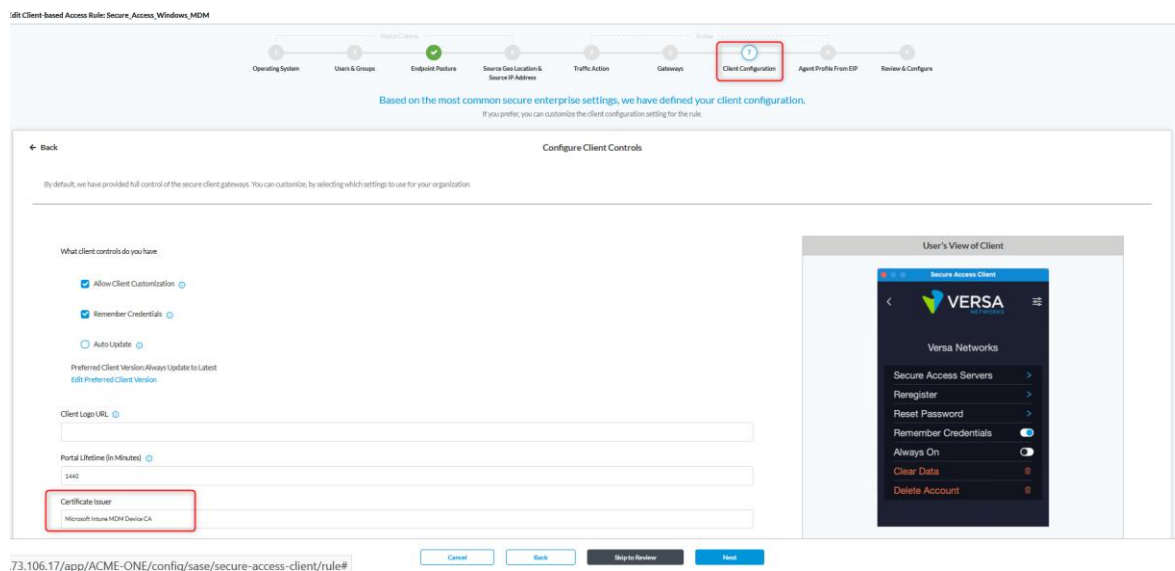
Steps 4–6 – Configure Source IP/Geo, Traffic Action, and Gateways as needed.

Client Configuration

- **Step 7** – Client Configuration → Click Customize to adjust client options.

Important Note:

Specify the **Certificate Issuer (Microsoft Intune MDM Device CA)** to validate enrolled devices. If the **Certificate Issuer** is not set, the SASE Client will **not send the device ID** when connecting to gateways, causing the policy match to fail.



Verification – How to Validate the Integration with Windows

Validation & Debugging > Once the configuration is pushed, the MDM/UEM module triggers API requests to **login.microsoftonline.com** and **graph.microsoftonline.com** using the **Directory ID, Client ID, and Client Secret** to fetch access tokens. You can also verify that the **Microsoft Intune MDM Device CA** certificate issuer parameter is present, ensuring correct device validation.

- Ensure that **DNS servers** are correctly configured to resolve the Microsoft API domains.
- You can **run Gateway debug commands** on the Sase Gateway to verify that Intune queries are being sent.

set debug captive-portal

set debug captive-portal level all

set debug captive-portal all-flags

set debug success

set debug success level all

set debug success all-flags

set debug dynamic-scale

set debug dynamic-scale level all

set debug dynamic-scale flags general

set debug mdm

set debug mdm level all

set debug mdm all-flags

After enabling the debug flags, review the logs:

Go to **Logs** then *run*

tail -f versa-service.log

When the configuration is applied and the device begins registration, the logs should show:

- The presence of **Microsoft Intune MDM Device CA** as the certificate issuer, confirming that the device certificate was detected and that the endpoint is presenting an Intune-issued certificate during registration. This indicates that VOS successfully extracted the device identity and can proceed with validating the device against Intune.

```
2025-09-29 20:28:52.128 DEBUG [0x101] saccess_service_process_response: resp_xml:
<?xml version="1.0" encoding="UTF-8"?>
<versa-secure-access version="2"><preregister><code>200</code><message>success</message><method>ldap</method></preregister><capabilities><actions><autoprerregister>autoprerregister</autoprerregister><preregister>preregister</preregister><register>register</register><otp-gen>register_otp_gen</otp-gen><otp-verify>register_otp_verify</otp-verify></actions><api-version>2</api-version></capabilities><device-id-request><certificate-issuer>Microsoft Intune MDM Device CA</certificate-issuer><uuid>4a73a59efb0dc8b2</uuid></device-id-request></versa-secure-access>
```

- API authentication requests **login.microsoftonline.com**, confirming that VOS is reaching Microsoft's OAuth endpoint to obtain an access token. This shows that the initial Intune authentication flow has been triggered correctly.
- The presence of **Client ID**, **Client Secret**, and **scope** referencing **graph.microsoft.com**, in the request payload confirms that the system is performing the token request using the configured Intune application credentials. This indicates that VOS is preparing to call Microsoft Graph and validate device compliance.

```
2025-09-29 20:28:52.326 DEBUG [0x101] mdm_get_access_token_request_data:158 form_data data len = 174
2025-09-29 20:28:52.326 DEBUG [0x101] mdm_get_access_token_request_data:159 out data len = 390
2025-09-29 20:28:52.326 DEBUG [0x101] mdm_get_access_token_request_data:171 Request query: POST https://login.microsoftonline.com/92896a25-7228-4f74-9bf4-fc31c21284be/oauth2/v2.0/token HTTP/1.1
Host: login.microsoftonline.com
Accept: */*
Content-Type: application/x-www-form-urlencoded
Content-Length: 174

client_id=18bea91a-611e-4108-b446-40a0902b764e&scope=https://graph.microsoft.com/.default&client_secret=fmU8Q~2XWLSAHAU7grb_IsNrA2GrCuaUHZ0rPdyJ&grant_type=client_credentials
2025-09-29 20:28:52.326 DEBUG [0x101] mdm_request_access_token:1352 len of data = 390
2025-09-29 20:28:52.511 DEBUG [0x101] mdm_access_token_cb:1252 resp_len = 3483
```



```

2025-09-29 20:28:52.970 DEBUG [0x101] mdm_request_resource_cb:1102 resp_len = 2494
2025-09-29 20:28:52.970 DEBUG [0x101] mdm_request_resource_cb:1105 response = HTTP/1.1 200 OK
Transfer-Encoding: chunked
Content-Type: application/json;odata.metadata=minimal;odata.streaming=true;IEEE754Compatible=false;charset=utf-8
Strict-Transport-Security: max-age=31536000
request-id: 2a542dfb-da93-4e77-a520-6d35ee5b0e5b
client-request-id: 2a542dfb-da93-4e77-a520-6d35ee5b0e5b
x-ms-ags-diagnostic: {"ServerInfo":{"DataCenter":"West US","Slice":"E","Ring":"4","ScaleUnit":"","004","RoleInstance":"B3Y3PEPFO0
799EF"}}
Odata-Version: 4.0
Date: Mon Sep 29 2025 20:28:51 GMT

7BD
{"@odata.context": "https://graph.microsoft.com/v1.0/$metadata#deviceManagement/managedDevices/$entity", "id": "5d7d35de-53c9-435
8-ae39-6d9dd8866254", "userId": "479990ec2-d1e9-40a4-a132-4b2ce4785417", "deviceName": "W-ACME-ONE-MDM", "managedDeviceOwnerType": "c
ompany", "managementState": "managed", "enrolledDateTime": "2025-09-10T21:12:20.3289877Z", "lastSyncDateTime": "2025-09-29T20:26:51.
281044Z", "operatingSystem": "Windows", "complianceState": "compliant", "jailBroken": "Unknown", "managementAgent": "mdm", "osVersion": "
0.0.26100.6584", "easActivated": false, "easDeviceId": null, "easActivationDateTime": "0001-01-01T00:00:00Z", "azureADRegistered": t
rue, "deviceEnrollmentType": "windowsAzureADJoin", "activationLockBypassCode": null, "emailAddress": "test@acmeonlab.onmicrosoft.co
m", "azureADDeviceId": "70d25038-8193-4238-8b52-7a394482108b", "deviceRegistrationState": "registered", "deviceCategoryDisplayName":
"", "isSupervised": false, "exchangeLastSuccessfulSyncDateTime": "0001-01-01T00:00:00Z", "exchangeAccessState": "none", "exchangeAcc
essStateReason": "none", "remoteAssistanceSessionUrl": "", "remoteAssistanceSessionErrorDetails": "", "isEncrypted": true, "userPrinci
palName": "test@acmeonlab.onmicrosoft.com", "model": "Standard PC (Q35 + ICH9, 2009)", "manufacturer": "OEMU", "imei": null, "complia
nceGracePeriodExpirationDateTime": "9999-12-31T23:59:9999999Z", "serialNumber": null, "phoneNumber": null, "androidSecurityPatchLe
vel": null, "userDisplayName": "test", "configurationManagerClientEnabledFeatures": null, "wifiMacAddress": null, "deviceHealthAttest
ationState": "null", "subscriberCarrier": "", "meid": null, "totalStorageSpaceInBytes": 160171032576, "freeStorageSpaceInBytes": 11023050
3424, "managedDeviceName": "test_Windows_9/10/2025_9:12 PM", "partnerRegistrationThreatState": "unknown", "requireUserEnrollmentApprova
l": null, "managementCertificateExpirationDate": "2026-05-05T00:00:00Z", "iccid": null, "udid": "", "notes": null, "ethernetMacAddress": "B
C2411A9E3D0", "physicalMemoryInBytes": 0, "enrollmentProfileName": "", "deviceActionResult": []}
sILvZXIUUmVhZCS5BgwILCEJZXPz2VNYW5H2ZtZW50029uZndXhdGJldl5SZZWFLKfSBjdLCJzdWIiOiI2ZmM1YmVnNS0yZjM3LTKRkZjItYTtYMyoNzFmI
GEtXNmYmW2EiLCJ0ZWNbnRfcmlvdWVnaW9uX3BiBGljaioiUEiLCJ0aWQoIiw3g5NMENYS903jT4LTRmNZQtOWJmNCImYmZmXyzIXmjoYmYuMjUjL2R2F6mpor
jREhWTATrKtkktUFIEFBFI iwdmYVjoiLSw4di iwd2LkClIgwyIwOTk3YTFKMzQWFDFLRhtY2tYj0wOCiLMWNWNmXzhXIjFlOTAiASwjbieX220Z2C6InXB0x2Wp
JREhWTtjV4UAxkUGtFEBCF0aaetFWgeJSuPz1TB2agvZq2M9r3bZCFH0miIpyTJBneFTYzXeIsInthe19ZHJibCI6lgmZAiLCJ4bXNfcm0iOiIwLjIyYj0pTpOzkw
pXzM4a0PiNXtUeMVRndG9UBjRKSTFSUTbjdyanRG6vFMHdkVDVBREZ05VLVCjNuX3VvY2Y1T3gtNT2VmYmZlF9mZVVUKURtSUNAOq7JTFtFAHkdICj4bXlndGnkdcIG6M
TCiMZmMTUjOX0". QyrdKJZCY5SPB1duK98SESNFPMMhke1Hyby7XdoMjUy1ghycRBHUOnPSy7hLBqGbqb3usuuK9kWUrU003PMatakDnkdic8CT0UbZCVcsukd
zb0PLuas0wYrmpefMW62CG9VI12XC87jiXUz5syupgkDXiLEtYUdo9yTNmeEqbv3eh2inCb2DVnSBPs3BZ2Sp5YoQgmjP24C8816xoqqeun6y9qnXkp-jnoELJ
FGxpHzq6WUpYl6ht8XguYubU6MRkvW6bt7tk7Trolv1zwIoh7HAkKN3R2HX0mYivrxZ70mdhLxe6EKygBo6qRd2IPxmxy8ZjdnEAIA"} end_flow = 0
2025-09-29 20:28:52.970 DEBUG [0x101] mdm_parse_chunk_response:719 sess_cfg->data_len = 0, sess_cfg->con_len = 0

```

These fields confirm that VOS successfully retrieved the device record and is receiving the correct compliance information from Intune.

All these logs are saved in the pre-register session logs, which are then used by the secure access policies to validate based on the different compliance states of a managed device.

To check the secure-access session logs, login to the vsmd and use the following commands:

- vsh connect vsmd
- show success session history all br
- show success session history all br | grep <user>
- show success session history id <no>

MACOS Enrollment

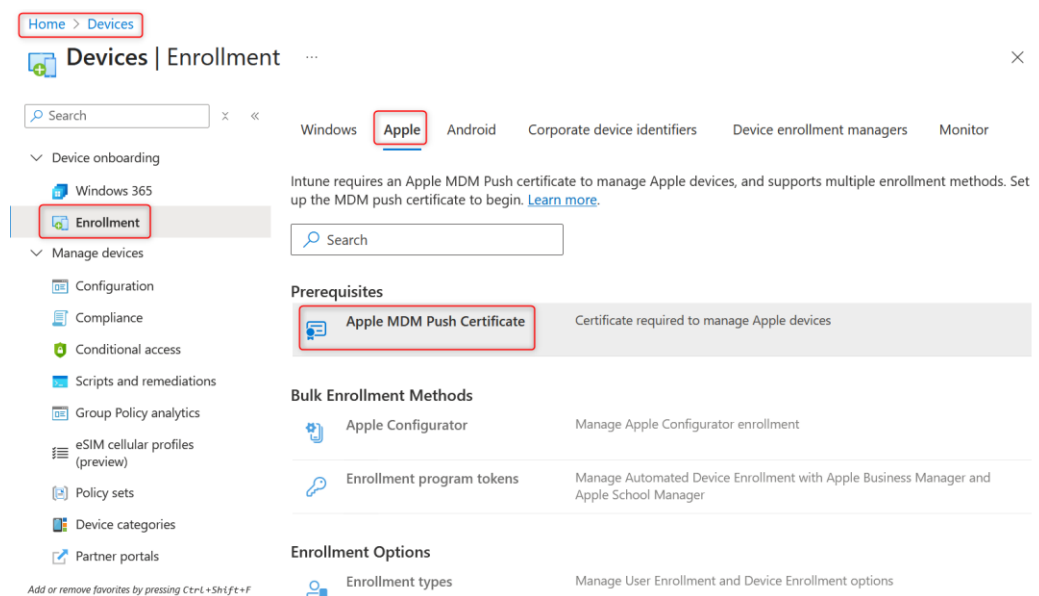
This walkthrough shows how to enroll a macOS device in Microsoft Intune and how its compliance state appears in VOS. It validates that the Intune integration behaves consistently across operating systems.

Generate the Apple MDM Push Certificate

To start macOS enrollment, you first need the Apple MDM Push certificate in Intune.

1. Download Apple MDM Push certificate in Intune for Mac enrollment

- Sign in to the Intune Admin Center:
<https://endpoint.microsoft.com>
- In the Intune Admin Center for Apple devices, go to:
Devices > Enroll devices > Apple enrollment > Apple MDM Push certificate



- In the **Apple MDM Push Certificate** area, review the permissions and select **I agree** to allow Microsoft to send device information to Apple.
- Click **Download your CSR** to download the Microsoft-signed .csr file.
 - Save this .csr file locally; you will use it later in Apple's portal when creating the actual Apple MDM Push certificate.

Home > Devices

Configure MDM Push Certificate

Delete

Not set up	Not available
Last updated	Expiration
Not available	Not available
Apple ID	Subject ID
Not set up	Not set up
Serial number	
Not set up	

You need an Apple MDM push certificate to manage Apple devices with Intune.

Steps:

- I grant Microsoft permission to send both user and device information to Apple. [More information on Microsoft permission.](#)
☒ I agree. *
- Download the Intune certificate signing request required to create an Apple MDM push certificate.
[Download your CSR](#)
- Create an Apple MDM push certificate. [More information on Apple MDM push certificate.](#)

2. Upload the CSR File in the Apple Push Certificates Portal

After downloading the **Intune CSR file**, use your **Apple ID** to request the MDM push certificate in the Apple portal.

- Go to the Apple Push Certificates Portal:
<https://identity.apple.com/pushcert>
- Sign in with your **Apple ID**.
- Click **Create a Certificate**, then accept the terms.

identity.apple.com/pushcert/

Apple Push Certificates Portal

Certificates for Third-Party Servers

Service	Vendor	Expiration Date*	Status	Actions
Mobile Device Management	Microsoft Corporation	Jun 26, 2026	Active	Review Download Revoke

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

About Apple Push Certificates Portal

Create and manage push certificates that enable your third-party server to work with the Apple Push Notification Service and your Apple devices.
[Learn more about Mobile Device Management](#)

MDM push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificate Portal.
[Learn more about MDM push certificate migration](#)

Contact Apple for assistance with the Apple Push Certificates Portal
 Enterprise-level customers with an AppleCare OS Support plan: 1-866-752-7753
 General inquiries and requests for assistance are handled by Deployment Programs Support.

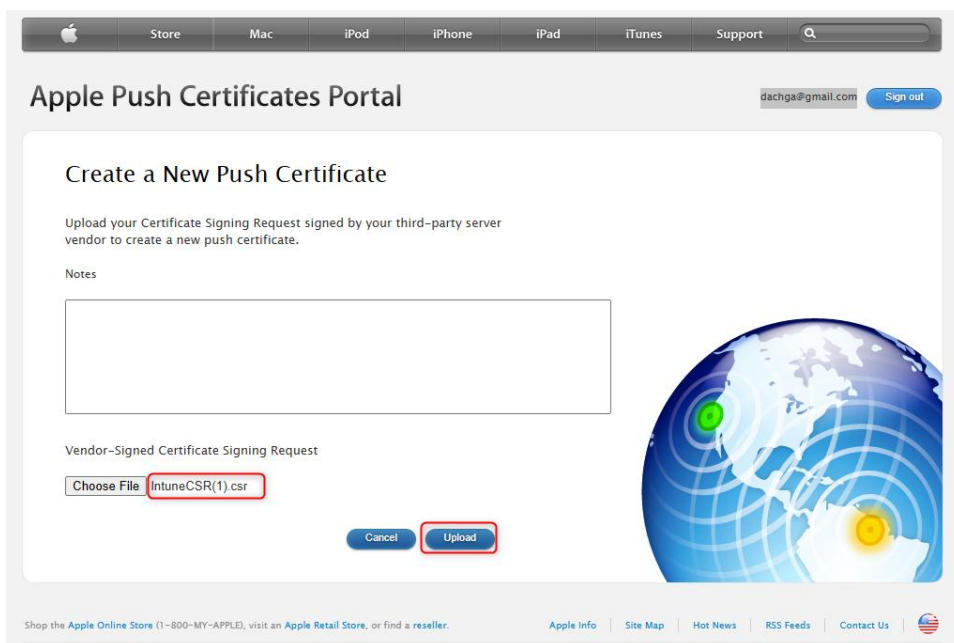
Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.

Apple Info | Site Map | Hot News | RSS Feeds | Contact Us

Copyright © 2017 Apple Inc. All rights reserved. [Terms of Use](#) [Privacy Policy](#)

On the Apple Push Certificates Portal, select the **correct .csr file** you previously downloaded from Intune (locate it on your laptop).

- After selecting the file, click **Upload** to submit the certificate signing request.



Apple Push Certificates Portal

dachga@gmail.com Sign out

Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

Vendor-Signed Certificate Signing Request

Choose File IntuneCSR(1).csr

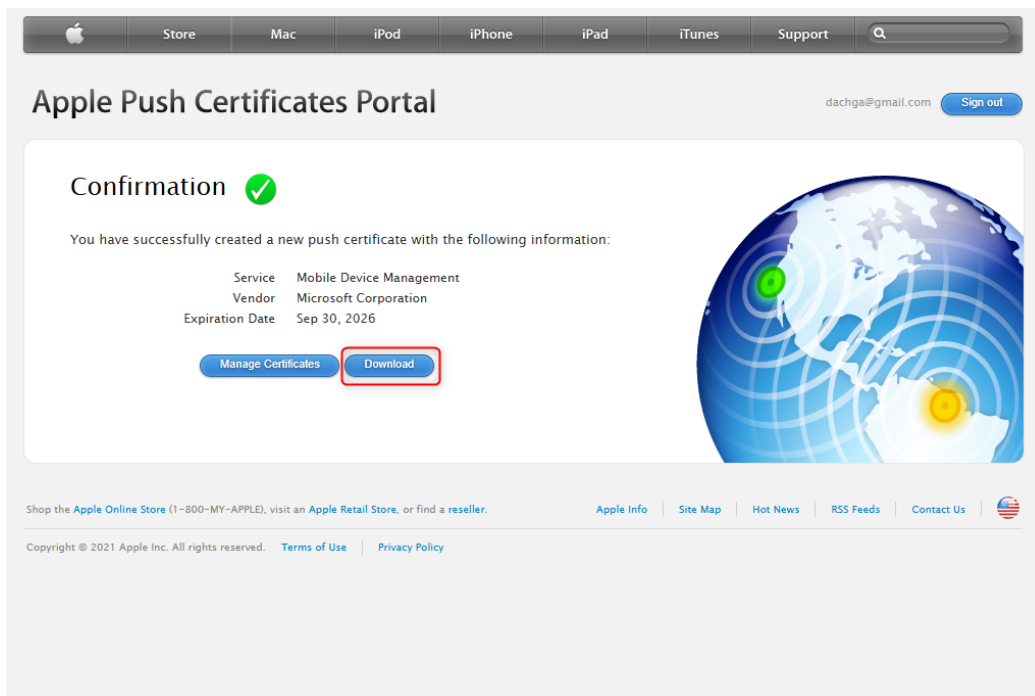
Cancel Upload

Shop the [Apple Online Store](#) (1-800-MY-APPLE), visit an [Apple Retail Store](#), or find a [reseller](#).

[Apple Info](#) | [Site Map](#) | [Hot News](#) | [RSS Feeds](#) | [Contact Us](#)

When the upload is completed, the portal will show a **confirmation screen**.

- Click Download to obtain the new **MDM Push Certificate (.pem)**.



Apple Push Certificates Portal

dachga@gmail.com Sign out

Confirmation

You have successfully created a new push certificate with the following information:

Service	Mobile Device Management
Vendor	Microsoft Corporation
Expiration Date	Sep 30, 2026

Manage Certificates Download

Shop the [Apple Online Store](#) (1-800-MY-APPLE), visit an [Apple Retail Store](#), or find a [reseller](#).

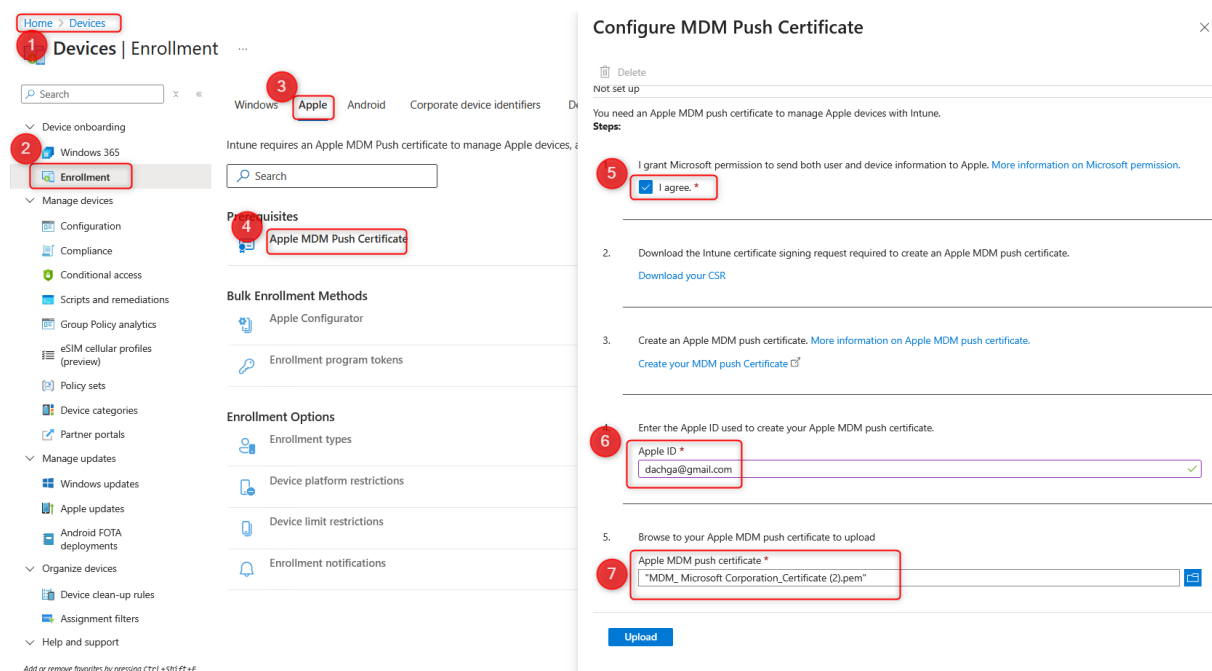
[Apple Info](#) | [Site Map](#) | [Hot News](#) | [RSS Feeds](#) | [Contact Us](#)

Copyright © 2021 Apple Inc. All rights reserved. [Terms of Use](#) | [Privacy Policy](#)

3. Upload the New Apple MDM Push Certificate in Microsoft Intune

Return to the Intune Admin Center.

- Navigate to:
Devices > Enroll devices > Apple enrollment > Apple MDM Push certificate
- Click **Upload your APNs certificate**, then browse and select the **.pem** file you downloaded from the Apple Push Certificates Portal.
- Enter the **Apple ID** used to generate the certificate.
- **Save** the changes.



Note: Although this procedure was completed using a regular Apple ID, corporate environments use a company-managed Apple ID. The process for generating the MDM Push Certificate is the same in both cases.

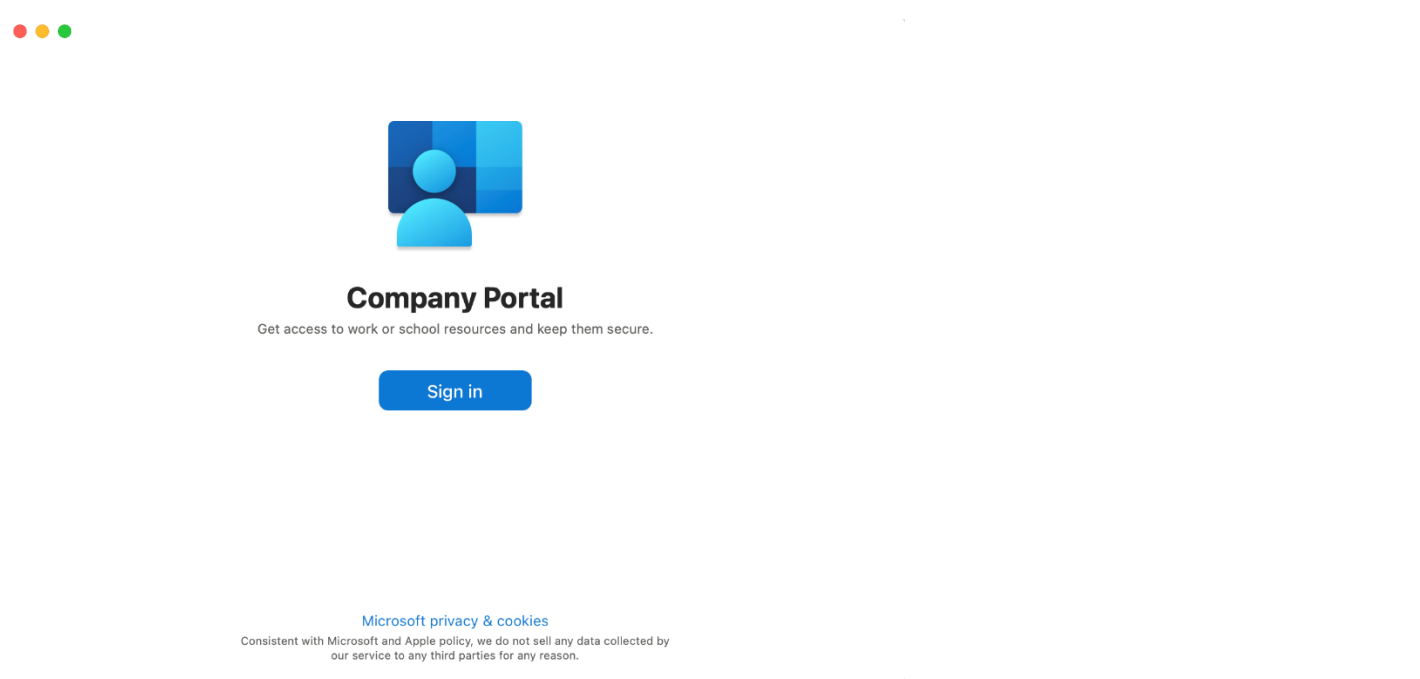
Install Company Portal on macOS

To begin enrollment on macOS, download and install the **Microsoft Intune Company Portal**

application.

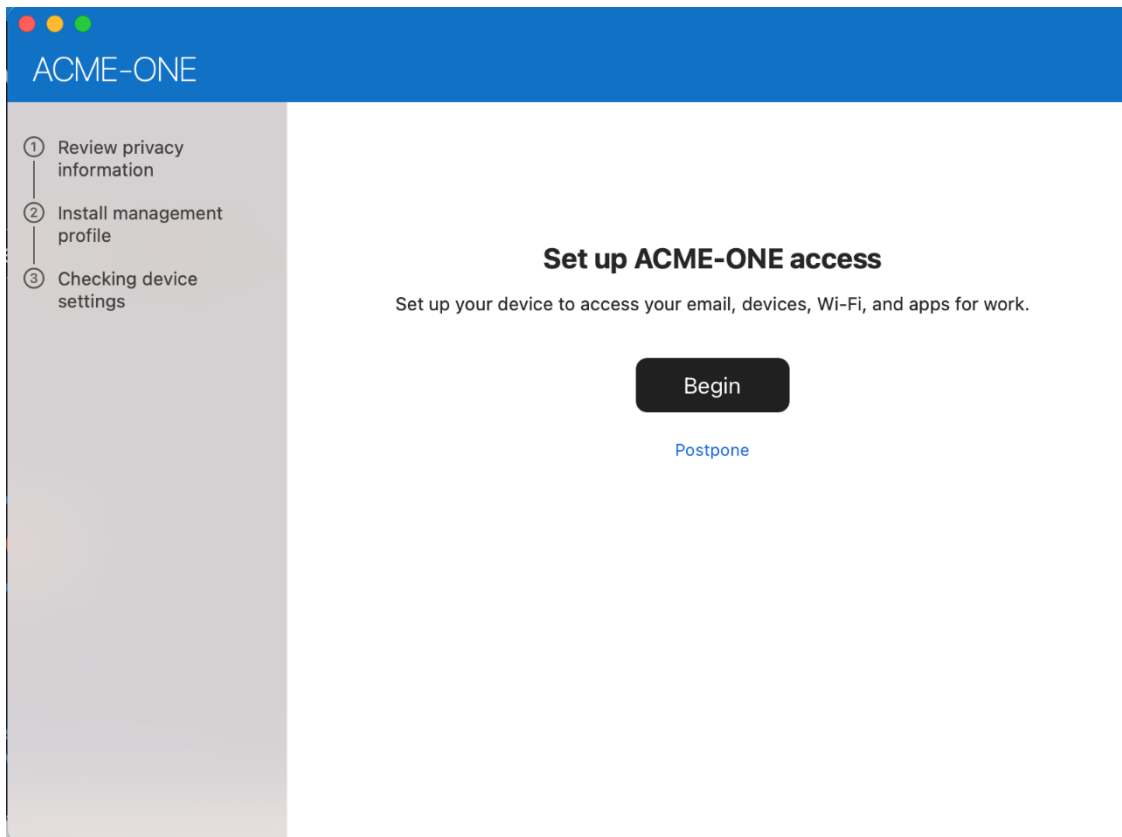
1. Install and sign in Microsoft Company Portal

Open the **App Store** search for **Microsoft Company Portal** and click **Get** to install (you may also download it from Microsoft's official site).



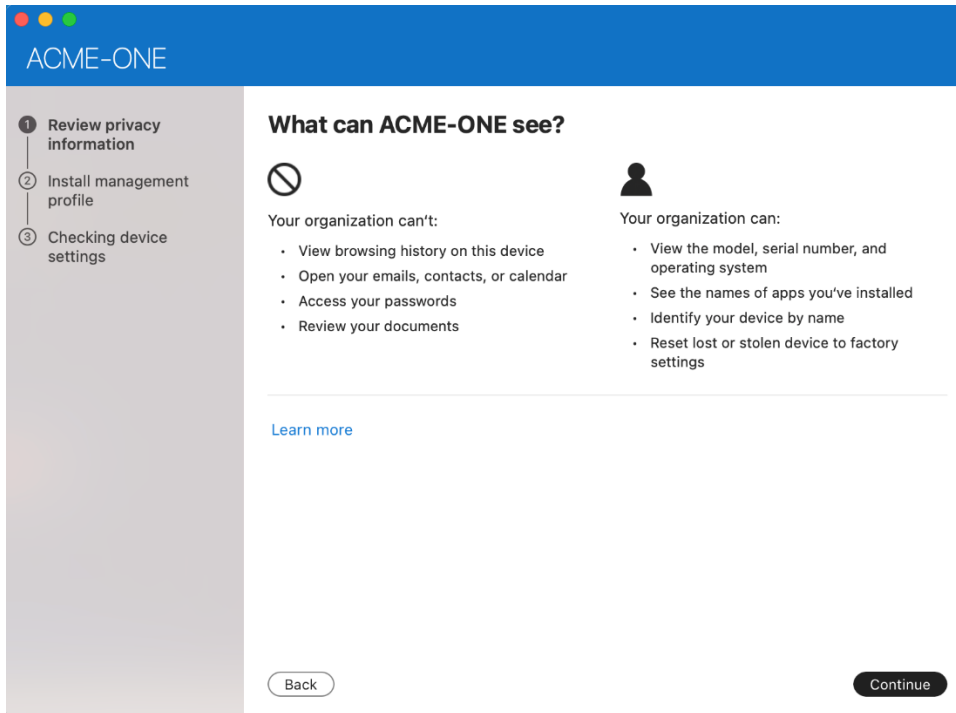
After installation, **sign in using your Intune corporate account** with your work or school email and password to start the enrollment process.

Once logged in to **Company Portal** on macOS, click **Begin** to start the setup process.

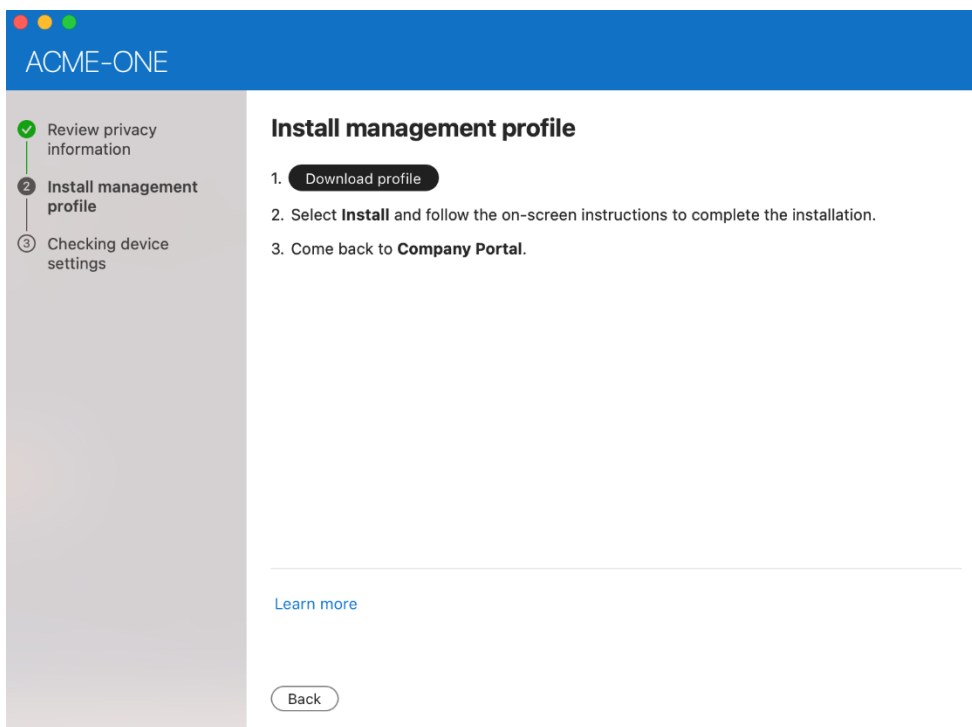


macOS will then display the **privacy information**, showing what your organization *can* and *cannot* see on the device.

- Review the details and click **Continue** to proceed with installing the management profile.



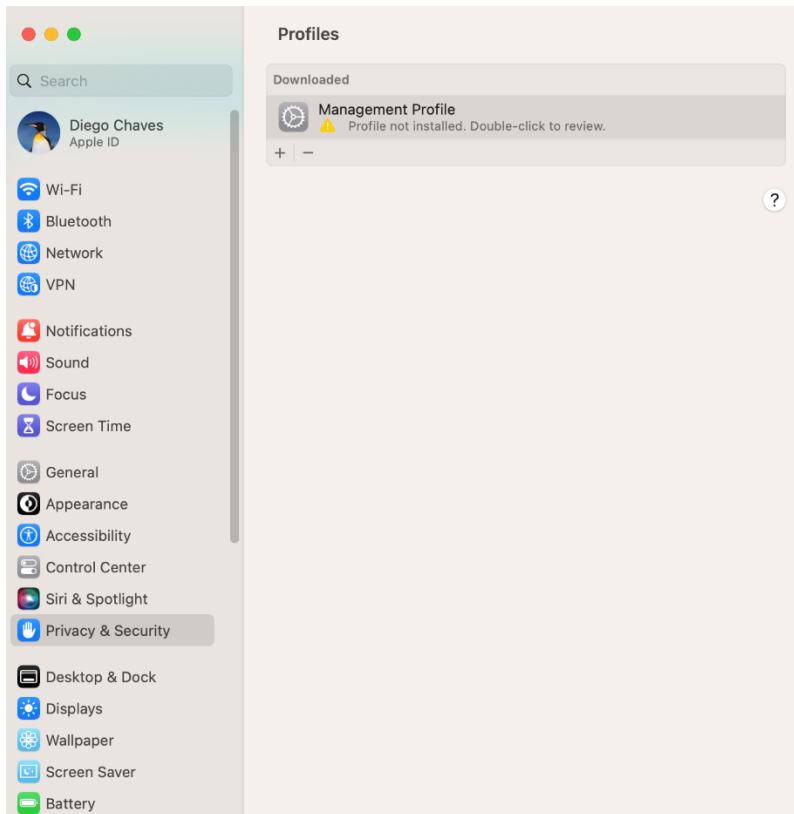
Install the management profile > Click **Download profile**, open the downloaded file, select **Install**, and follow the on-screen instructions.



2. Install the downloaded profile in macOS

Open System Settings > Privacy & Security > Profiles.

- Select the **Management Profile** that was downloaded from the Company Portal.



- Click **Install** and follow the on-screen instructions to complete the profile installation.

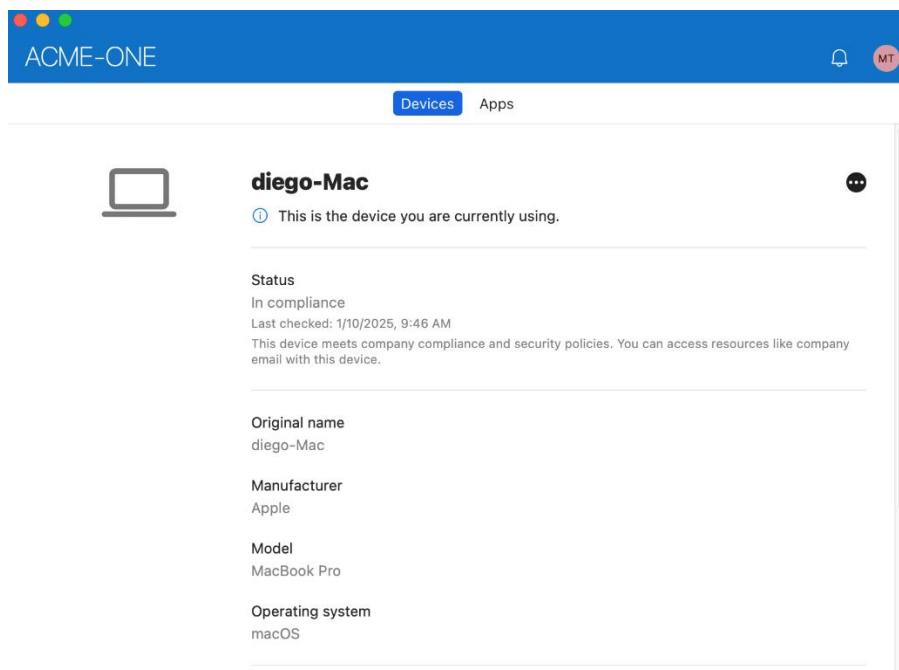
Once the profile installation is complete, **return to the Company Portal** to continue the enrollment process.

Complete Enrollment > After the management profile is installed, Intune validates the device and updates its status.

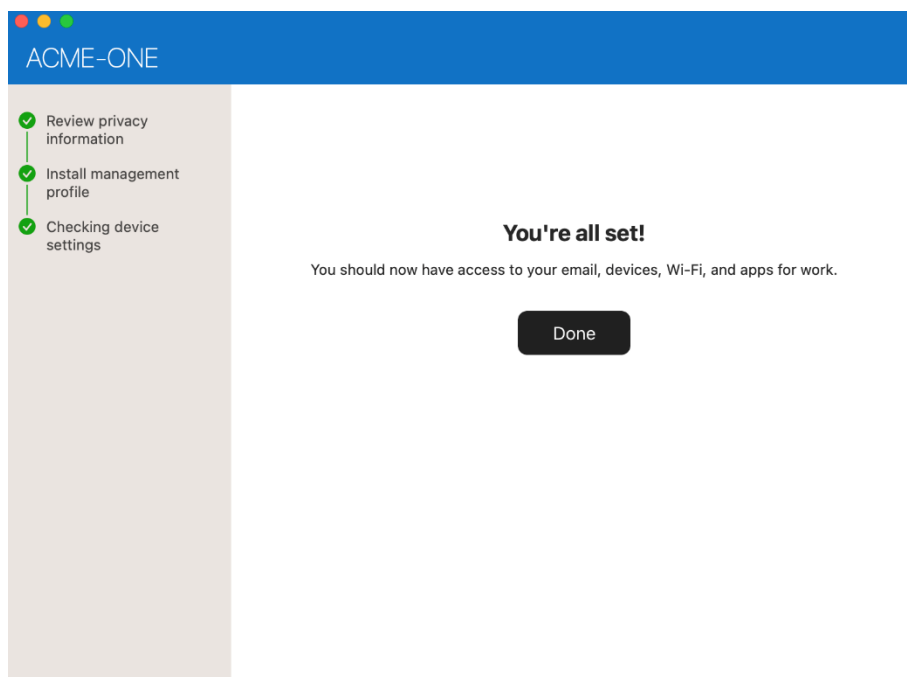
If everything is successful, the Mac will appear as **"In compliance"** in the Company Portal.

Note

Since no macOS-specific compliance policy was created, the device is evaluated using Intune's **default compliance policy**. Administrators may later define a dedicated macOS compliance policy, as we did for Windows in the previous section..



Click **Done** to finish the setup and gain access to corporate apps, email, and resources.



3. Review Device Visibility in Intune

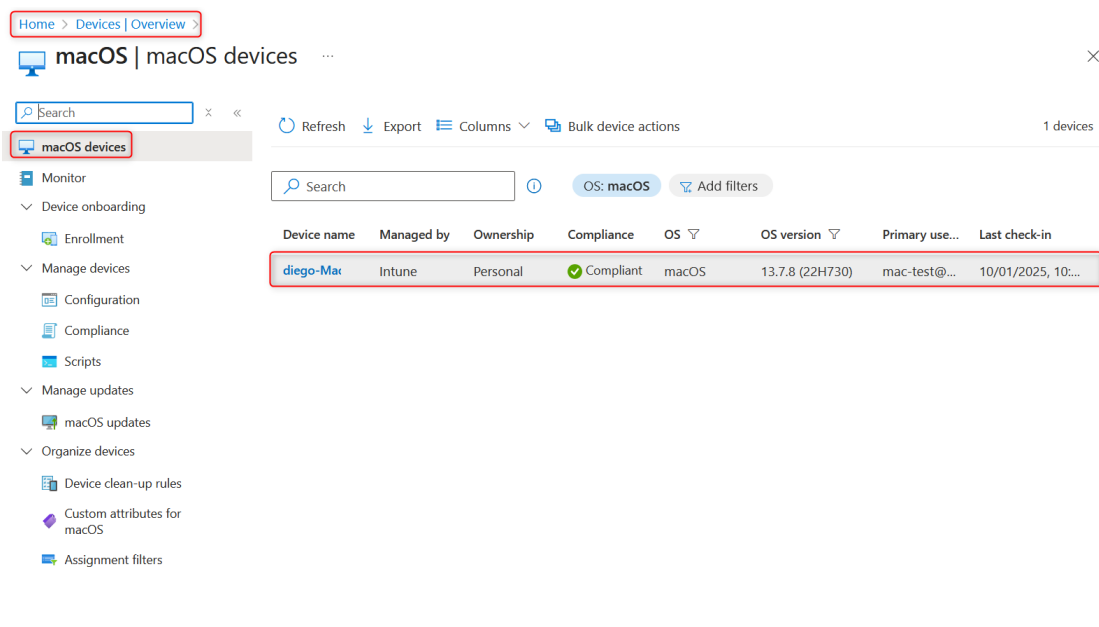
After enrollment, the Mac may take **10–15 minutes** to appear in the Microsoft Endpoint Manager portal.

Once it appears, check the **Compliance** column to confirm whether the device is **Compliant** or **Non-compliant**.

Go to Microsoft Intune admin center.

Inside the Intune admin center go to:

Devices > macOS> macOS devices



Apply Secure Access Rules for Intune-Managed Devices

In Concerto, go to:

Configure > Security Service Edge (SSE) > Secure Access > Client-based Access > Policy Rules

1. Configure Policy Rule Criteria

On the **Policy Rules** page, click + **Add** to create a new Secure Client Access rule, **or choose an existing rule from the list that you want to apply.**

This rule will control access for **compliant** and **non-compliant** devices.

VERSA | ACME-ONE | CONFIGURATION | Administrator Service Provider Administrator

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Client-based Access Rules

Below are all the rules for your Secure Client-based Access.

Rule Name	Operating System Versions	Users & Groups	Endpoint Posture		Traffic Action	VPN & Gateway Groups	Status	Last Modified By & Date
			EIP & Entity Risk Bands	Device Compliance Status				
<input type="checkbox"/> Secure_Access_Windows_Profile_LDAP_Us... More Details	Windows Windows 10 Windows 10 Mobile Windows 11	AD_Server_Acme_One Users Diego Chaves diego@diegolab-versa.net VIP1.vip1@acme-one.com	Endpoint Information Profile (EIP) User Defined EIP_Profile_Windows_Re... Entity Risk Bands All risk bands	Managed Status of Devices All Devices	Action Send Apps to Versa Cloud No Client Applications selected Exclude PreDefined Applications Facebook	VPN Name ACME-ONE-Enterprise Gateway Groups Default Gateways SaseGWDiego-lab	Enabled	11/21/2025, 11:53:34 AM Administrator
<input type="checkbox"/> Secure_Access_Windows_Profile More Details	Windows Windows 10 Windows 10 Mobile Windows 11	ENTRA-ID-SAML Users vip2@diegolab-versa.a.onmicrosoft.com vip3@diegolab-versa.a.onmicrosoft.com vip4@diegolab-versa.a.onmicrosoft.com	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Managed Status of Devices All Devices	Action Breakout to the Internet No Client Applications selected No Predefined Applications selected	VPN Name ACME-ONE-Enterprise Gateway Groups Default Gateways SaseGWDiego-lab	Enabled	11/21/2025, 11:53:34 AM Administrator
<input type="checkbox"/> Secure_Access_Windows_MDM More Details	Windows Windows 10 Windows 10 Mobile Windows 11	AD_Server_Acme_One Users Diego Chaves diego@diegolab-versa.net	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Managed Status of Devices Managed Devices Device Compliance Status compliance	Action Breakout to the Internet No Client Applications selected No Predefined Applications selected	VPN Name ACME-ONE-Enterprise Gateway Groups Default Gateways SaseGWDiego-lab	Enabled	9/25/2025, 3:21:21 PM Administrator

Showing 1-4 of 4 results | 10 Rows per Page | Go to page 1 | Previous | Next

In the Client-based Access Rule wizard, complete the following steps:

Step 1 – Operating System

Select the macOS operating system platforms that this rule will apply.

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Create Client-based Access Rule

1 Operating System | 2 Users & Groups | 3 Endpoint Posture | 4 Source Geo Location & Source IP Address | 5 Traffic Action | 6 Gateways | 7 Client Configuration | 8 Agent Profile From EIP | 9 Review & Configure

Choose the operating system for this rule below.

If you prefer, you can customize which operating system options you would like to enable for the rule.

Windows

☐ All Windows Operating Systems

☐ User Defined

- ☐ Oper-1
- ☐ testGoWindows
- ☐ test-yin-ok
- ☐ test-yin-pa

☐ Predefined

- ☐ Windows 10
- ☐ Windows 10 Mobile
- ☐ Windows 11
- ☐ Windows 7
- ☐ Windows 8
- ☐ Windows 8.1
- ☐ Windows Server 2012

Apple

☐ All Apple Operating Systems

☐ User Defined

- ☐ testGo
- ☐ Predefined

 - ☐ Mac OS X Server
 - ☐ OS X
 - ☐ Mac OS

☐ All Apple Mobile

☐ User Defined

- ☐ testGoIpad

☐ Predefined

- ☐ iOS
- ☐ iPadOS

Android

☐ All Android Operating Systems

☐ User Defined

- ☐ testGoAndroid
- ☐ testGoAndroid01

☐ Predefined

- ☐ Android

Linux

☐ All Linux Operating Systems

☐ User Defined

- ☐ testGoLinux
- ☐ testGoNew

☐ Predefined

- ☐ Fedora
- ☐ Linux
- ☐ Red Hat Enterprise Linux
- ☐ Ubuntu

Cancel | Back | Skip to Review | Next

Step 2 – Users and Groups


Choose the users or groups that should be included in this access rule.

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Create Client-based Access Rule

1 Operating System 2 **Users & Groups** 3 Endpoint Posture 4 Source Geo Location & Source IP Address 5 Traffic Action 6 Gateways 7 Client Configuration 8 Agent Profile From EIP 9 Review & Configure

By default we have chosen all users and groups to apply your security enforcements
If you prefer, you can select the specific users or groups for the security posture.


Users & Groups ⓘ
 ✓ Known Users
[Customize](#)

Cancel Back Skip to Review Next

Endpoint Posture

In the **Device Compliance Status** section, select:

- Managed Devices
- **Compliant** (to allow devices that pass Intune policies)

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure_Access_Windows_MDM

1 Operating System 2 Users & Groups 3 **Endpoint Posture** 4 Source Geo Location & Source IP Address 5 Traffic Action 6 Gateways 7 Client Configuration 8 Agent Profile From EIP 9 Review & Configure

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.
If you'd like, you can customize your options by choosing what to include or exclude below.

← Back

Device Compliance Status

If 3rd party UEM is used, select one or more device compliance status below

☐ All Devices
 ☒ **Managed Devices**
☐ Unmanaged Devices

☒ **Compliance**
☐ Non-Compliant
 ☐ Config-Manager
 ☐ Conflict
 ☐ In-Grace-Period
 ☐ Error
 ☐ Unknown

Cancel Back Skip to Review Next

Steps 4–6 – Configure Source IP/Geo, Traffic Action, and Gateways as needed.

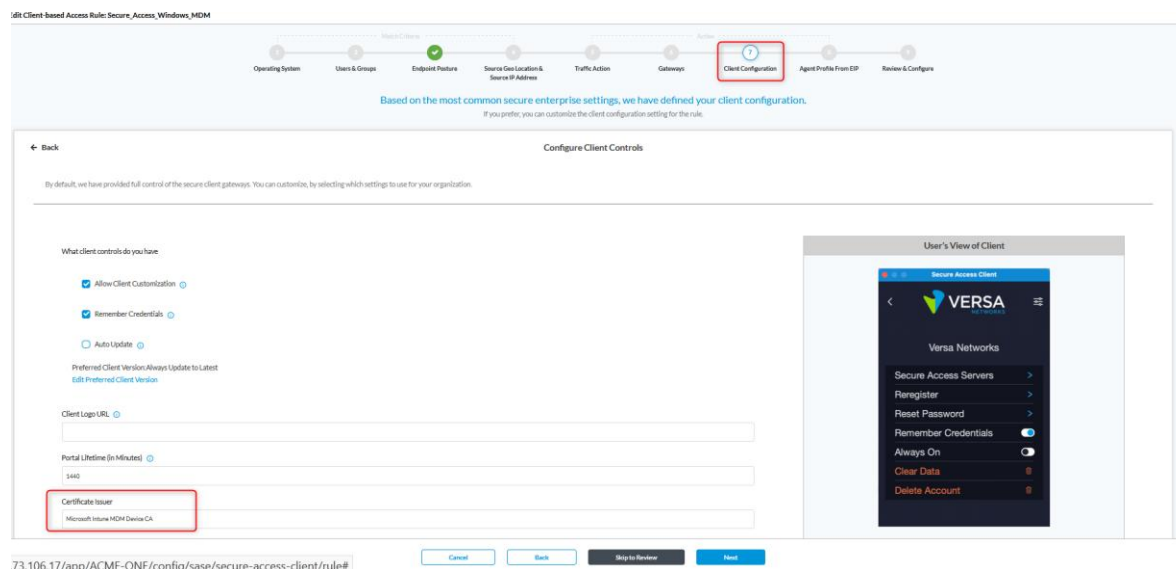
Client Configuration

- Step 7 – Client Configuration → Click Customize to adjust client options.

Important Note:

Specify the **Certificate Issuer (Microsoft Intune MDM Device CA)** to validate enrolled devices.

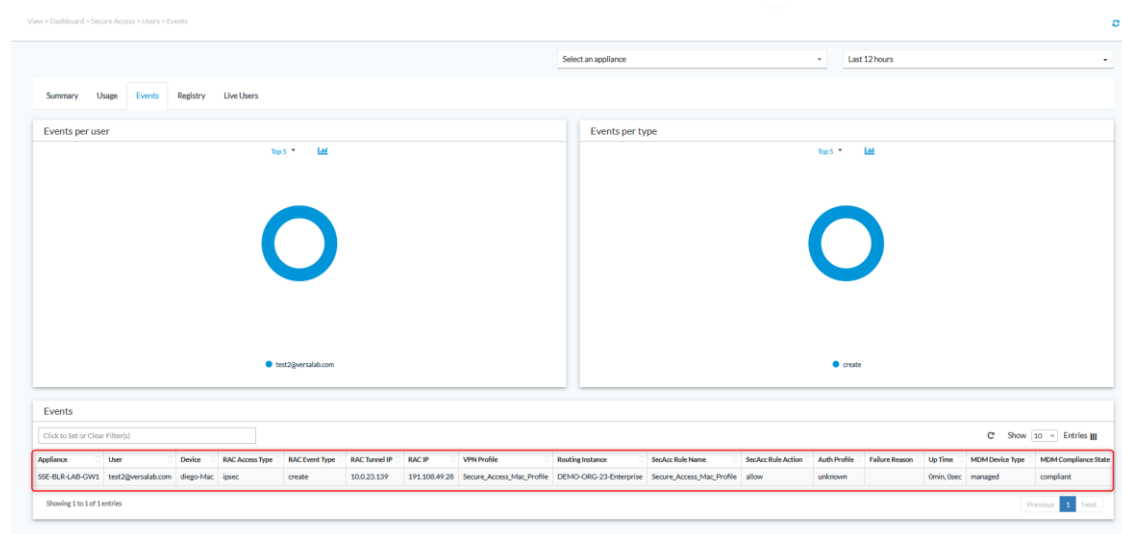
If the **Certificate Issuer** is not set, the SASE Client will **not send the device ID** when connecting to gateways, causing the policy match to fail.



Verification – How to validate the integration with macOS Compliance

After logging in with the SASE Client, In Concerto navigate to:

View > Dashboard > Secure Access > Users > > Events.



In the event logs, verify that the Mac device appears with **MDM Device Type: managed** and **MDM**

Compliance State: compliant

You can apply the **same debug and log validation steps** described in the earlier ***"Verification – How to Validate the Integration with windows"*** section to confirm that macOS devices are correctly registered with Intune. This includes checking the **versa-service.log** on the SASE Gateway (with UEM debug enabled) to verify Intune API requests, observing the **Microsoft Intune MDM Device CA** certificate issuer, token requests to **login.microsoftonline.com** and **graph.microsoft.com**, and validating returned fields such as **device name, management state, OS version, and compliance state**. These checks confirm that VOS is successfully retrieving the macOS compliance status from Intune.

About Versa

Versa, the global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the [VersaONE Universal SASE Platform](#) delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users, trust Versa with their mission critical networks and security. Versa is privately held and funded by investors such as Sequoia Capital, Mayfield, and BlackRock. For more information, visit <https://www.versa-networks.com> and follow Versa on [LinkedIn](#) and X (Twitter) [@versanetworks](#).