VERSA

IMPLEMENTATION GUIDE

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)

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

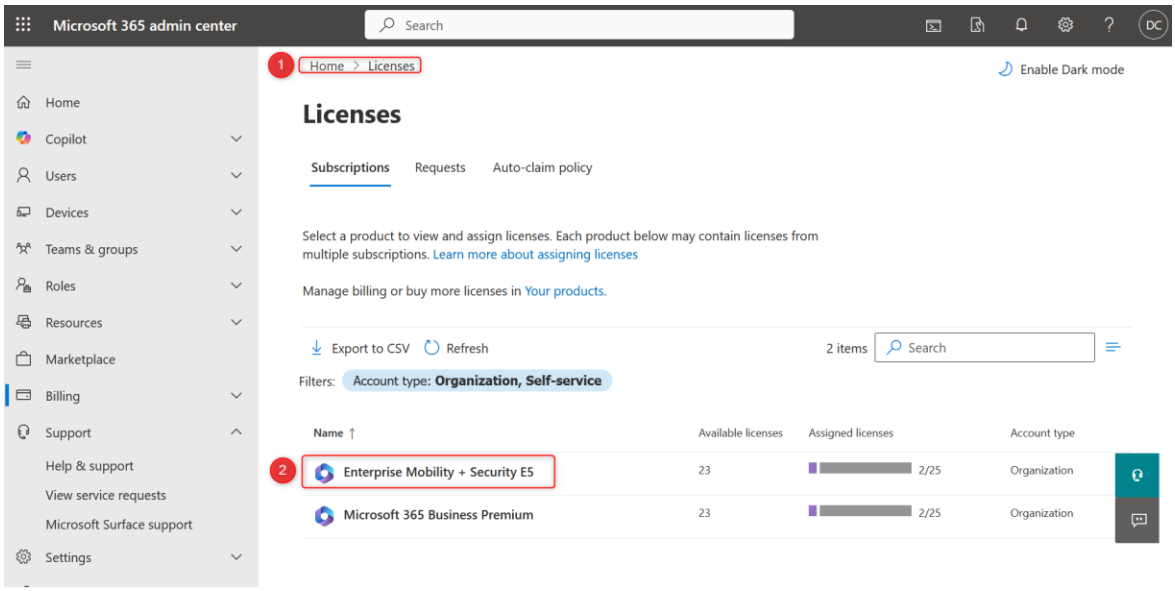
Ensure your Microsoft tenant includes one of the following subscriptions:

- **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:

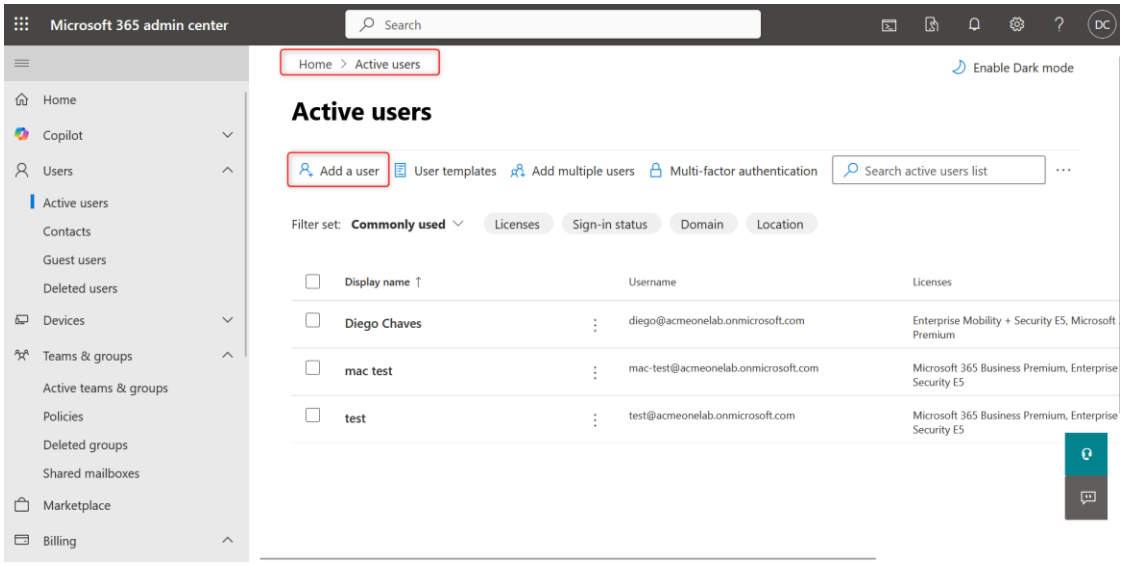
1. Creating a New User

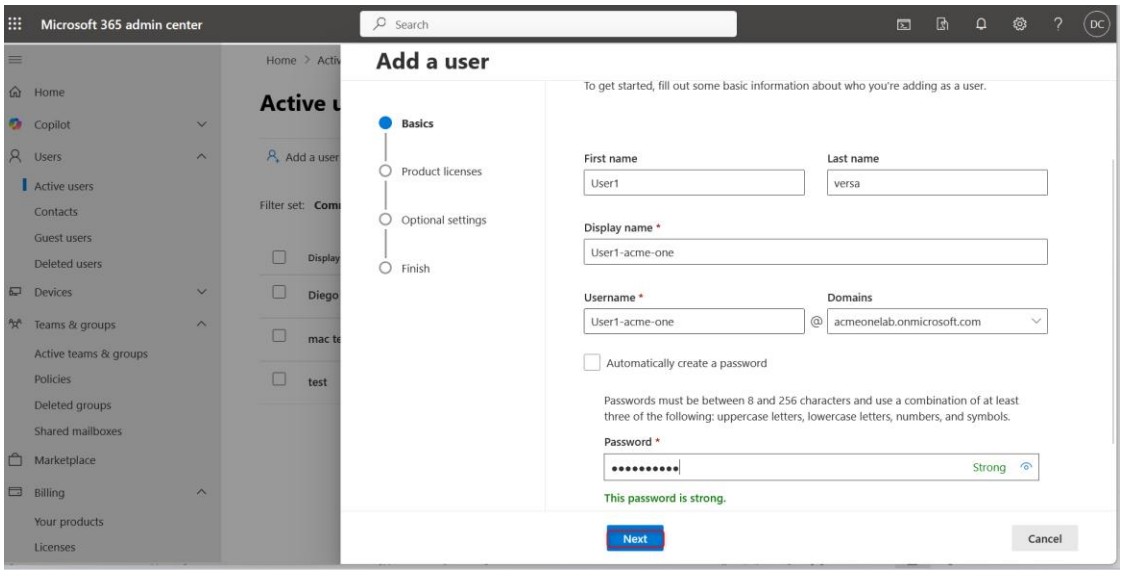
Navigate to **Users** → **Active users** inside the Admin Center.

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

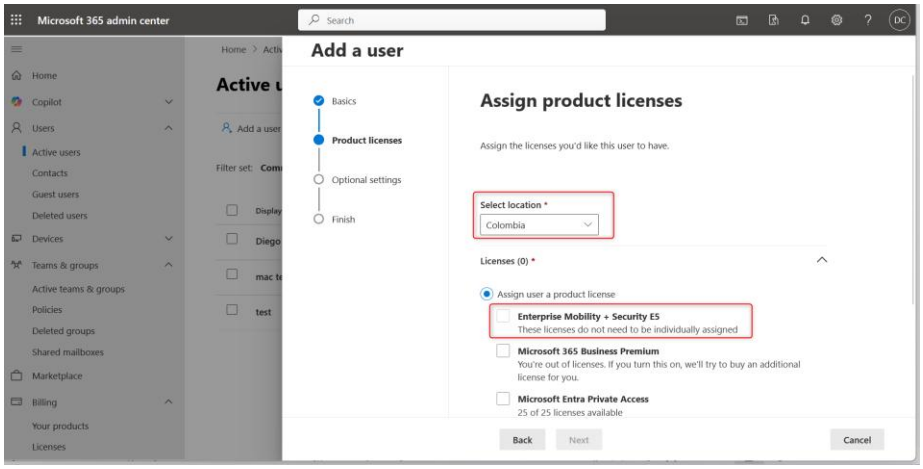
From here you can add new users who will be managed through Intune and later evaluated by Versa SASE Gateway.

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

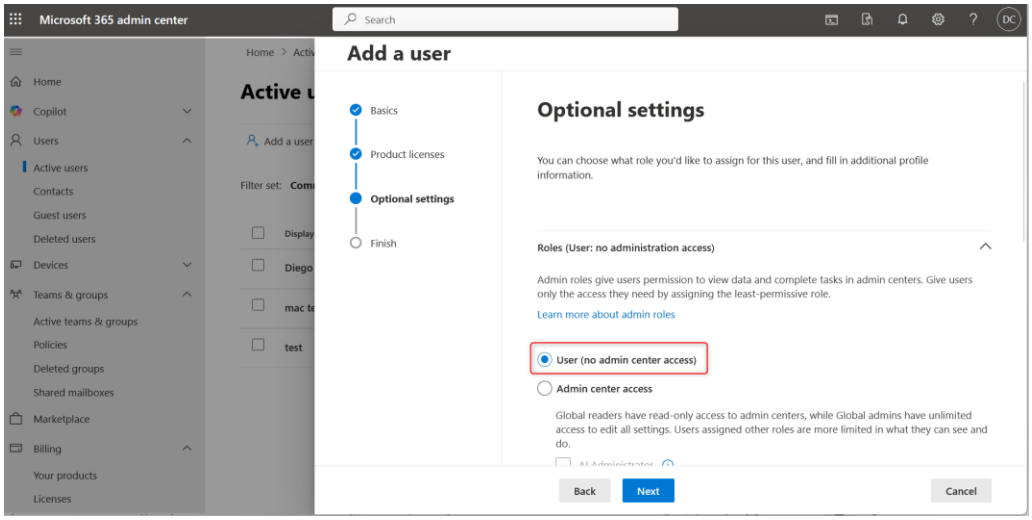




Then select **location** and assign the specific **license**.



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.

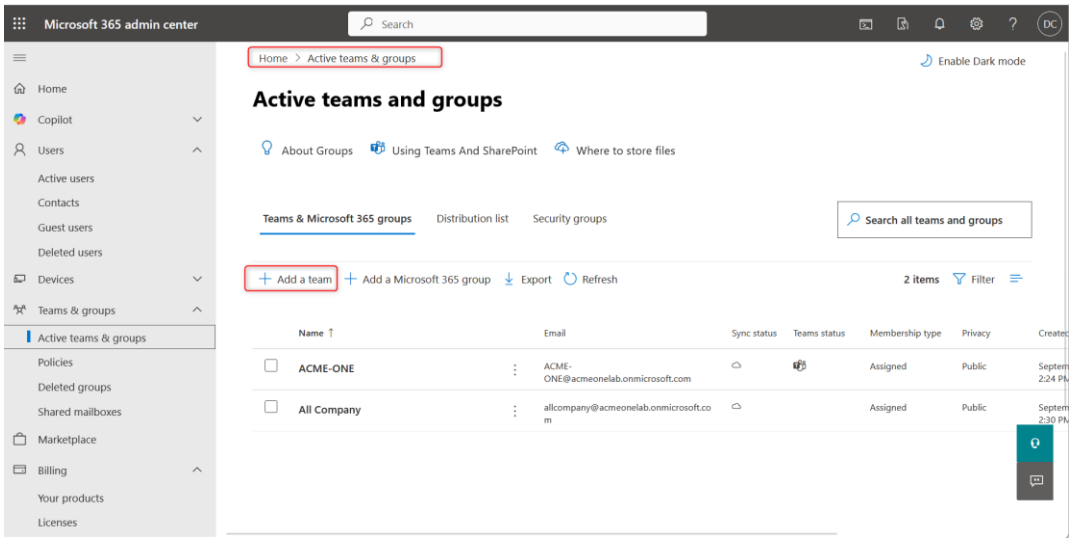
2. Creating a Group

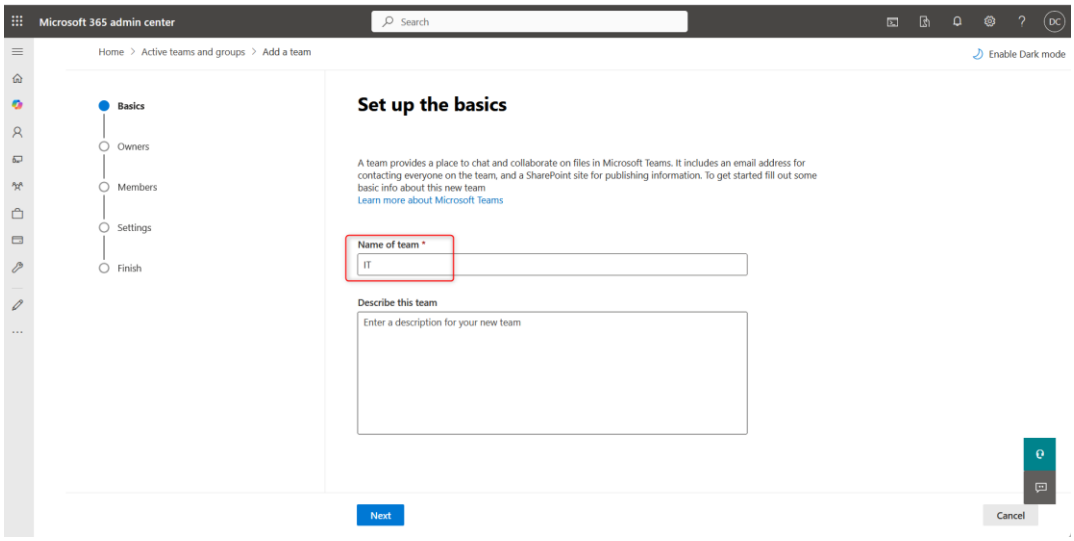
To create a group that can be used for Intune policy targeting or license assignment, go to:

Teams & groups → Active teams & groups

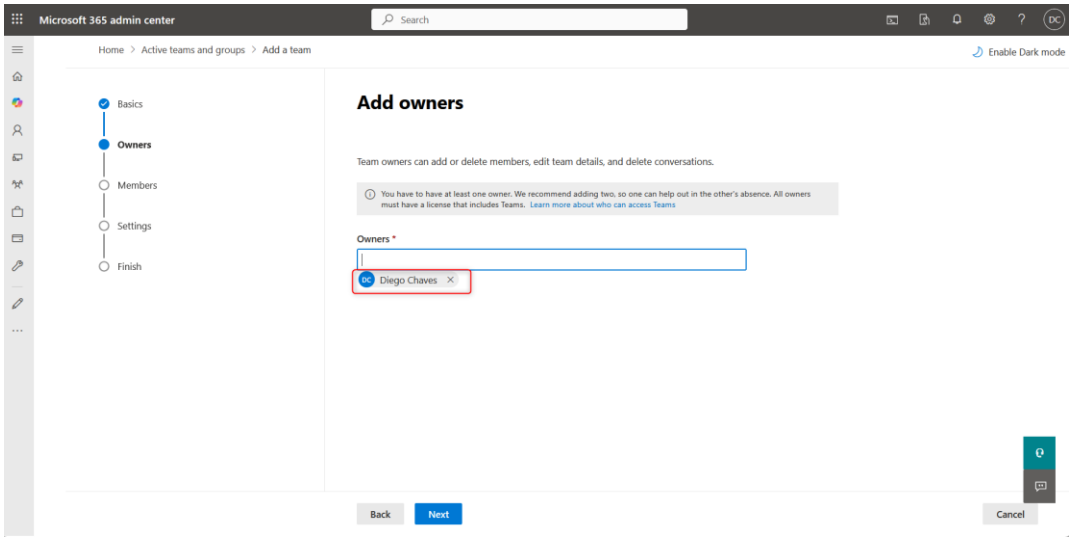
This section allows you to view and create Microsoft 365 groups, security groups, and distribution lists. Groups may be used to organize users for easier license assignment or compliance policy targeting.

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.

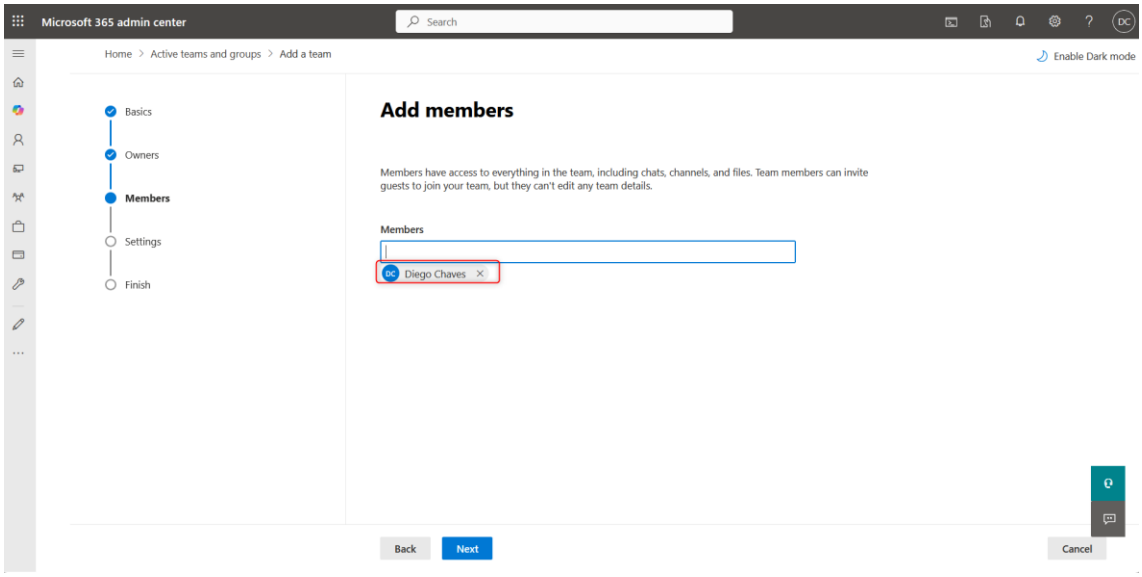




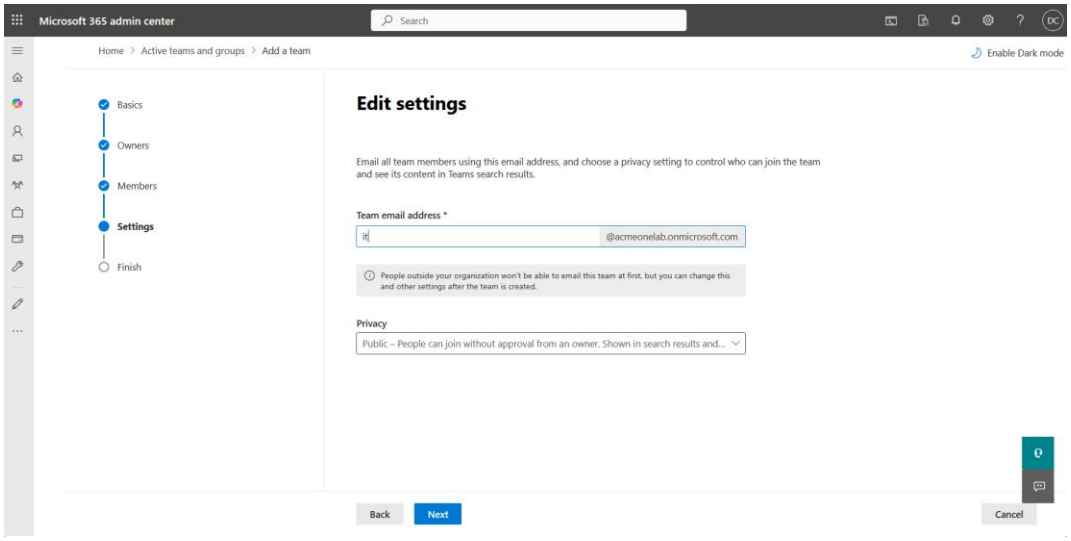
Assing at least on owner to the Group



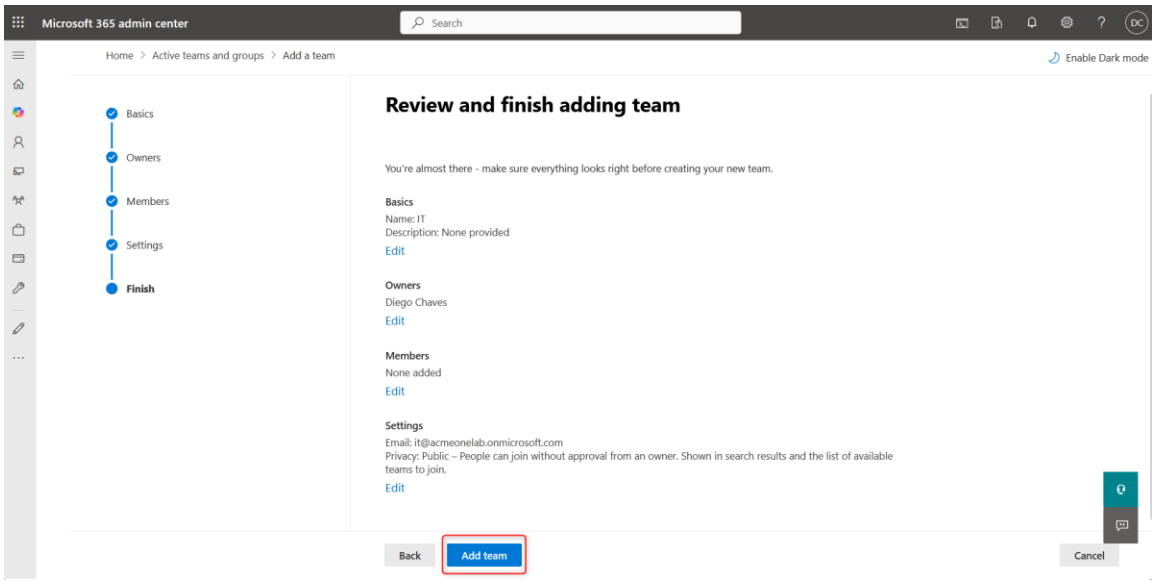
You can add members to the group now or add them later.



Choose an email to all team members.



Then **Review** and Add Team

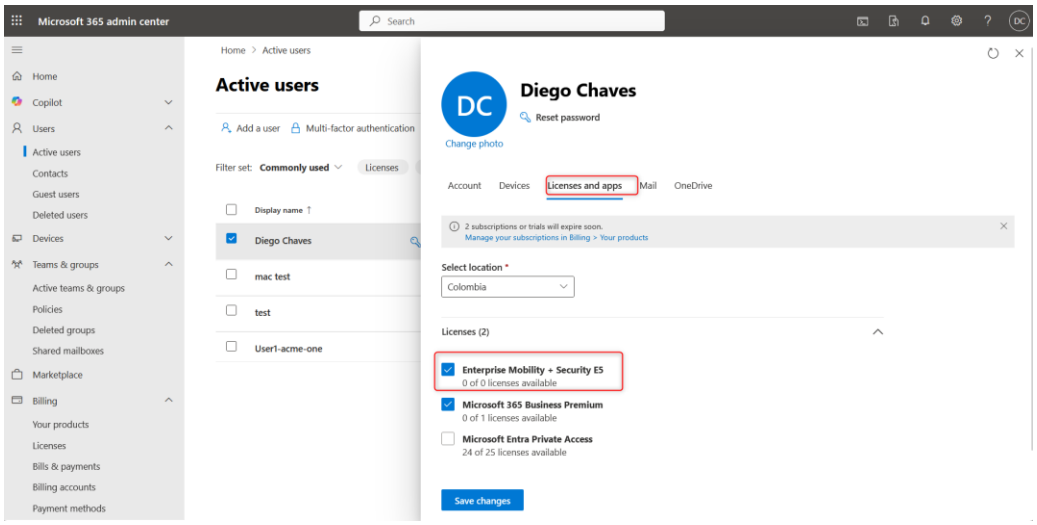


3. Assigning Licenses to Users or Groups

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.

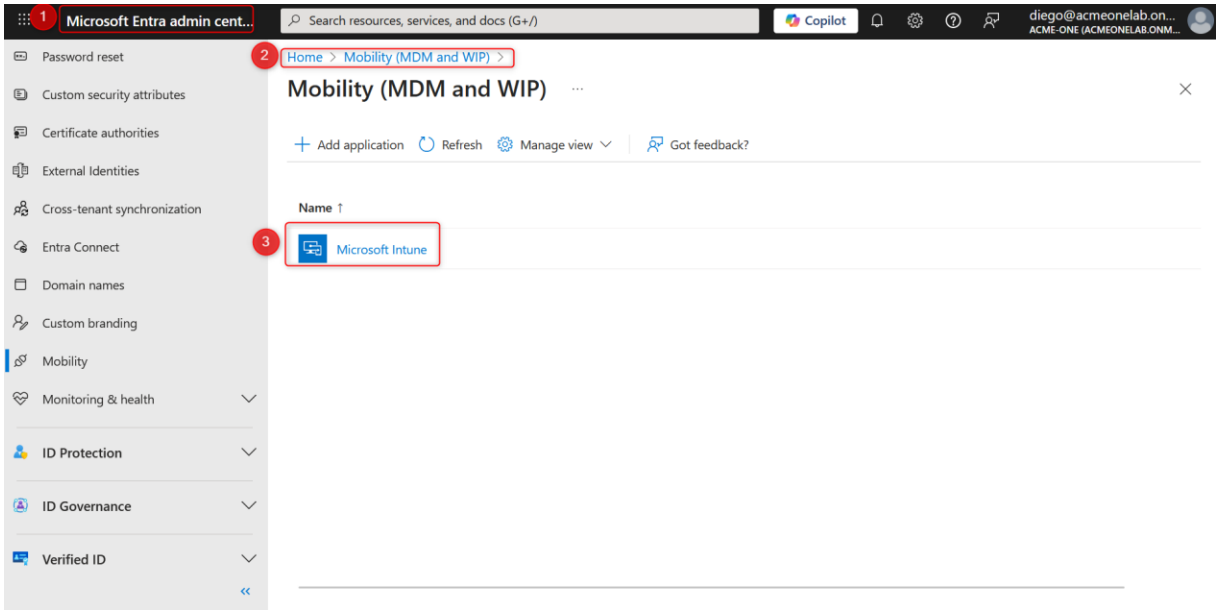
Access Microsoft Entra

- Log in to the Microsoft Entra admin portal:

https://entra.microsoft.com

Navigate to Mobility (MDM and WIP)

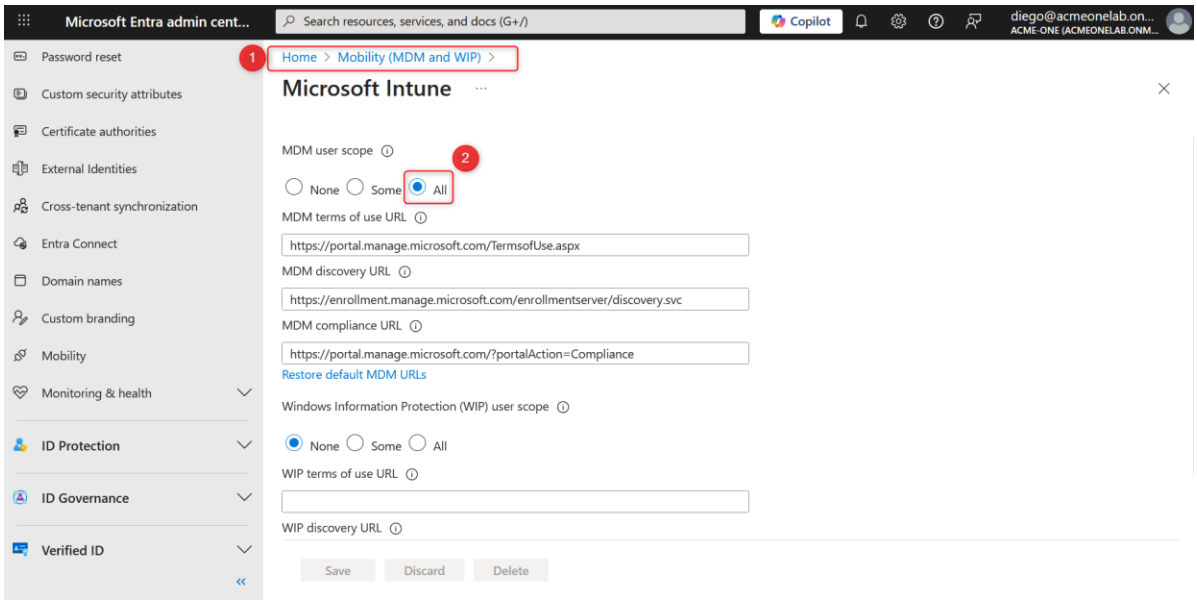
- In the left navigation panel, go to **Home**.
- Select Mobility (MDM and WIP).
- Open the **Microsoft Intune** application.



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

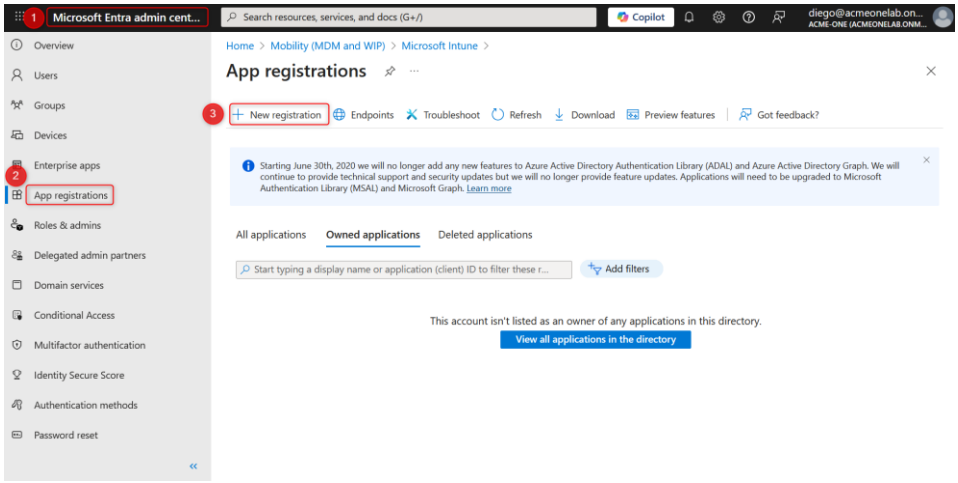
Inside the Microsoft Entra Admin Center, go to:

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:

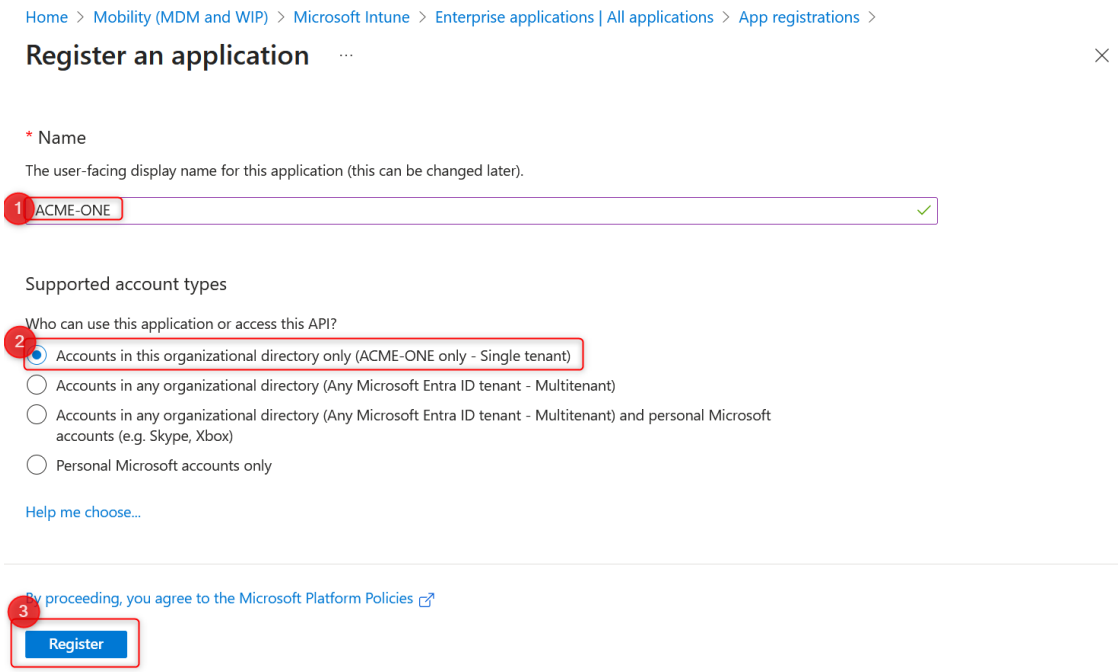
Accounts in this organizational directory only (Single-tenant)

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

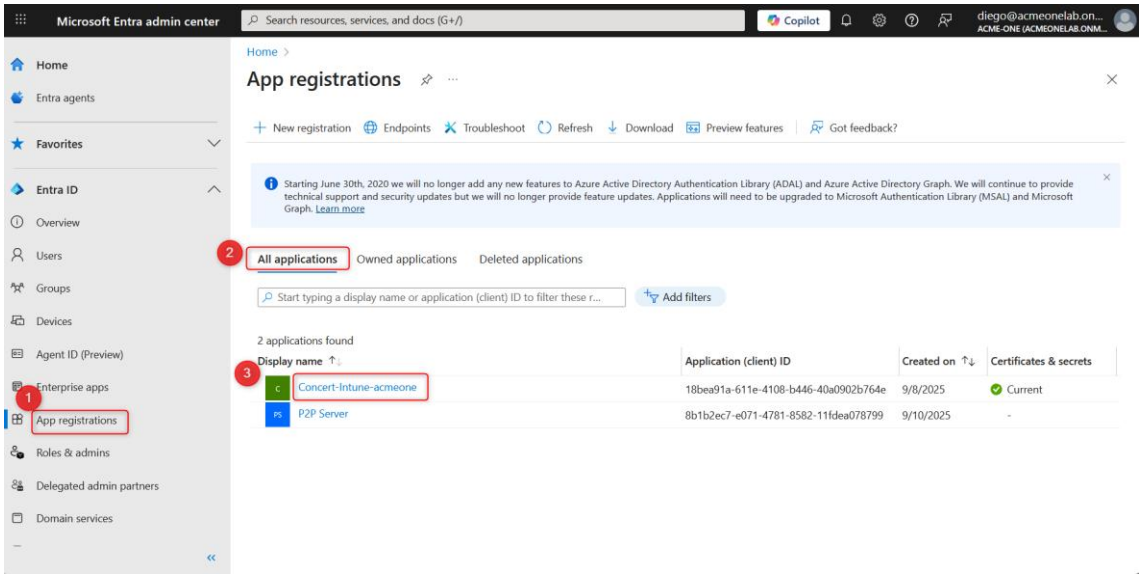
Register the Application

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.



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



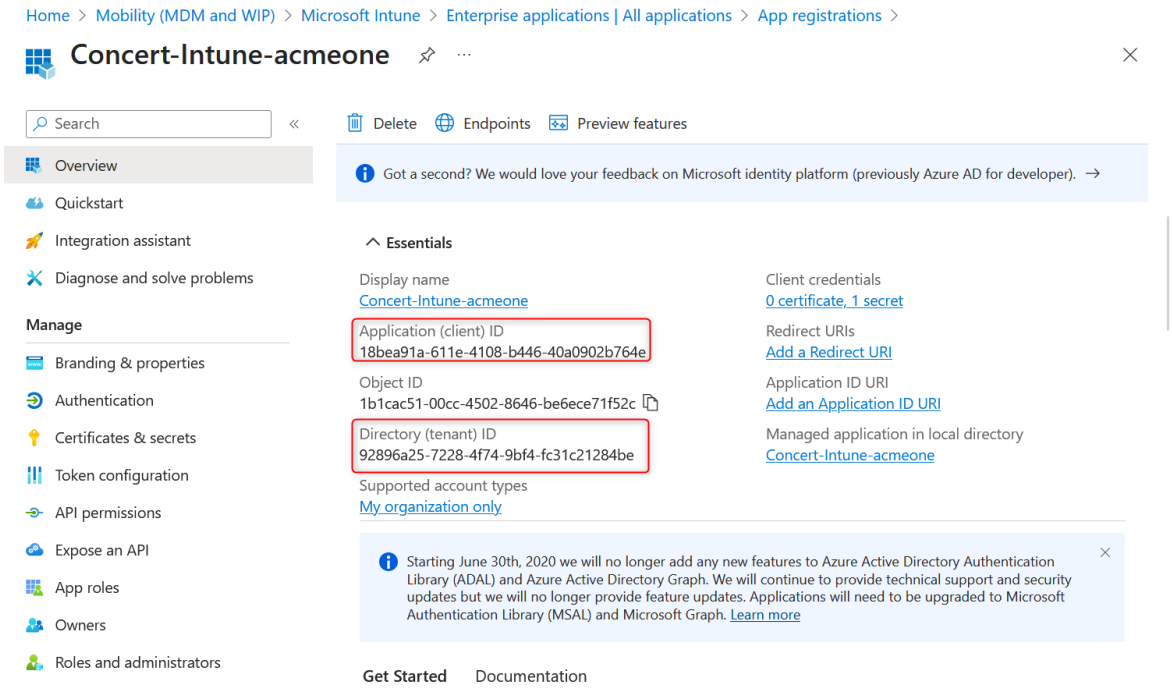
3. Retrieve Required Identifiers

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.

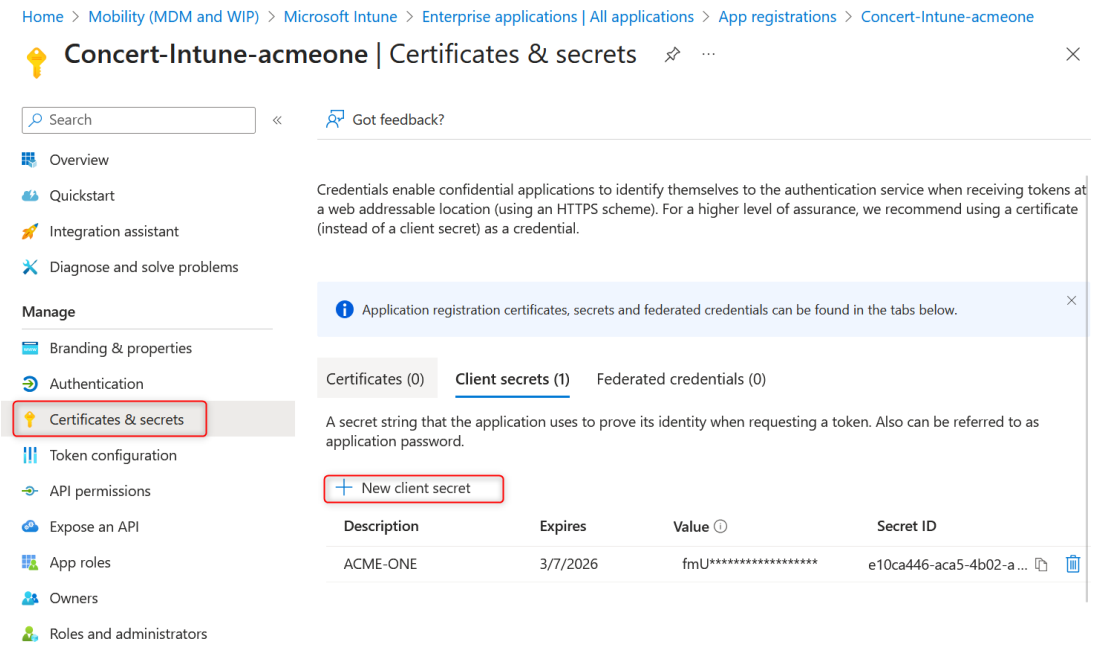


4. Generating a Client Secret

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.



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**.

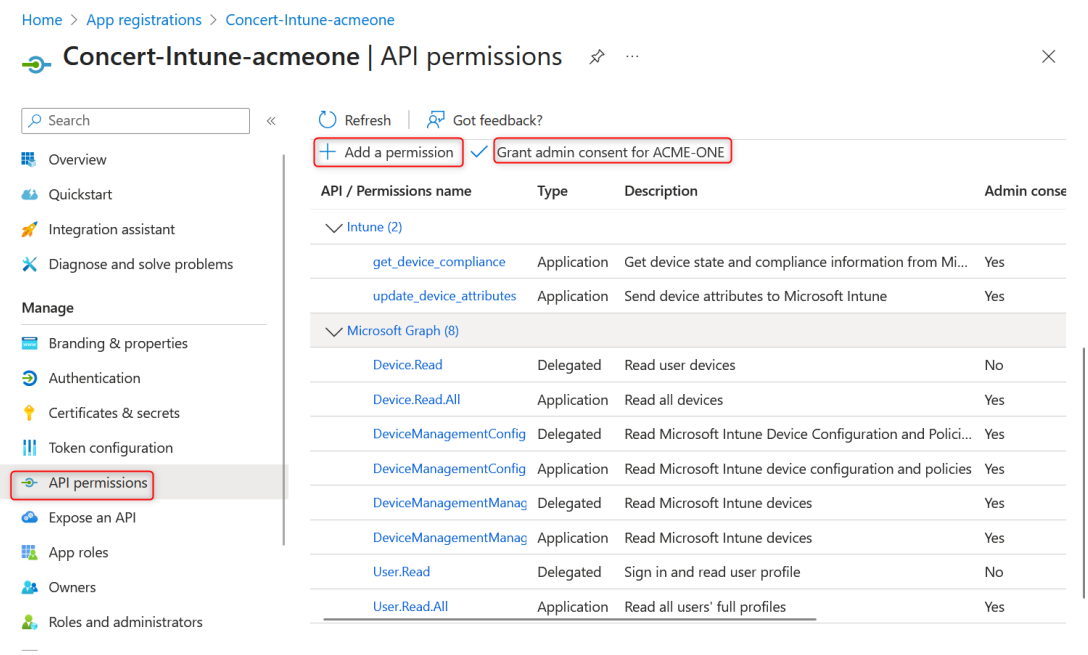
Add Required Permissions

- 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.



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**.

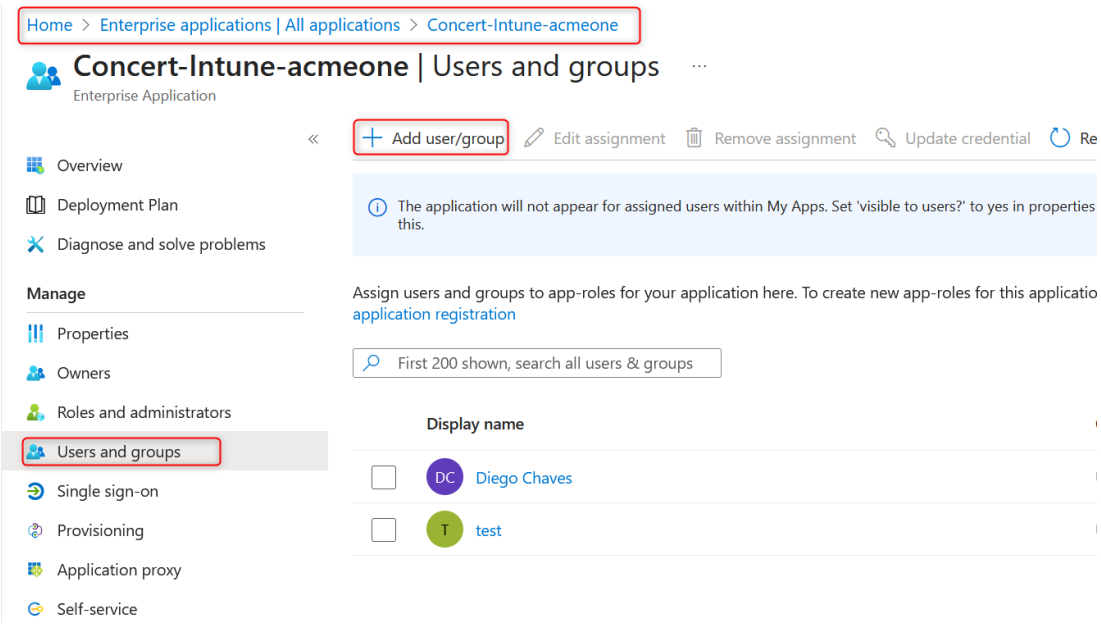
From the Microsoft Entra admin center:
Enterprise applications > All applications > Select your Intune app > Users and groups

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

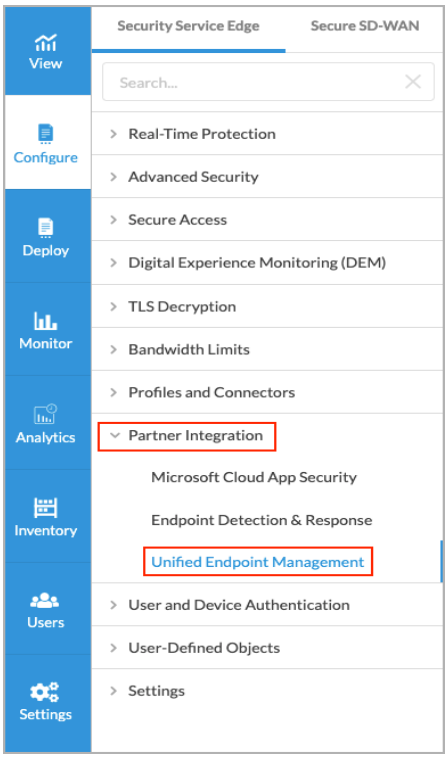


Configuration in Concerto

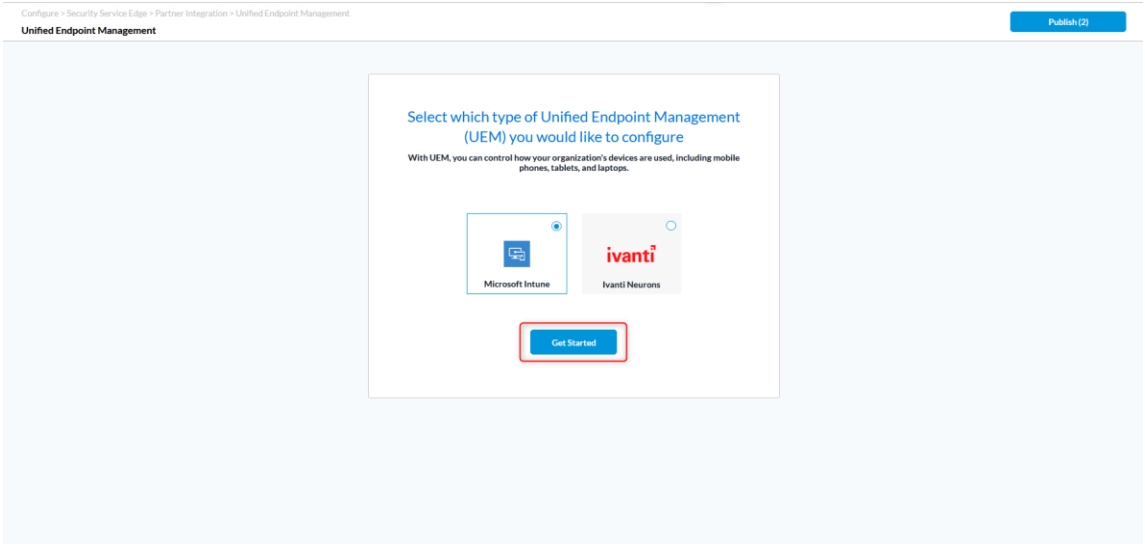
Integration with Accessing Unified Endpoint Management

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

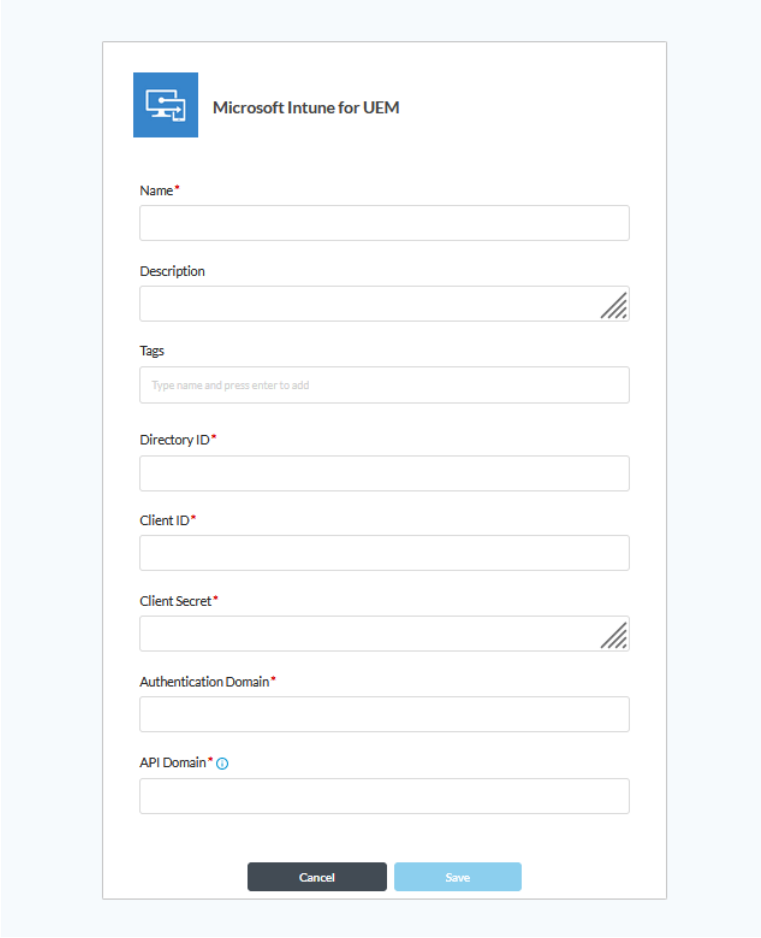
Configure > Security Service Edge (SSE) > Partner Integration > Unified Endpoint Management



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.



\

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.

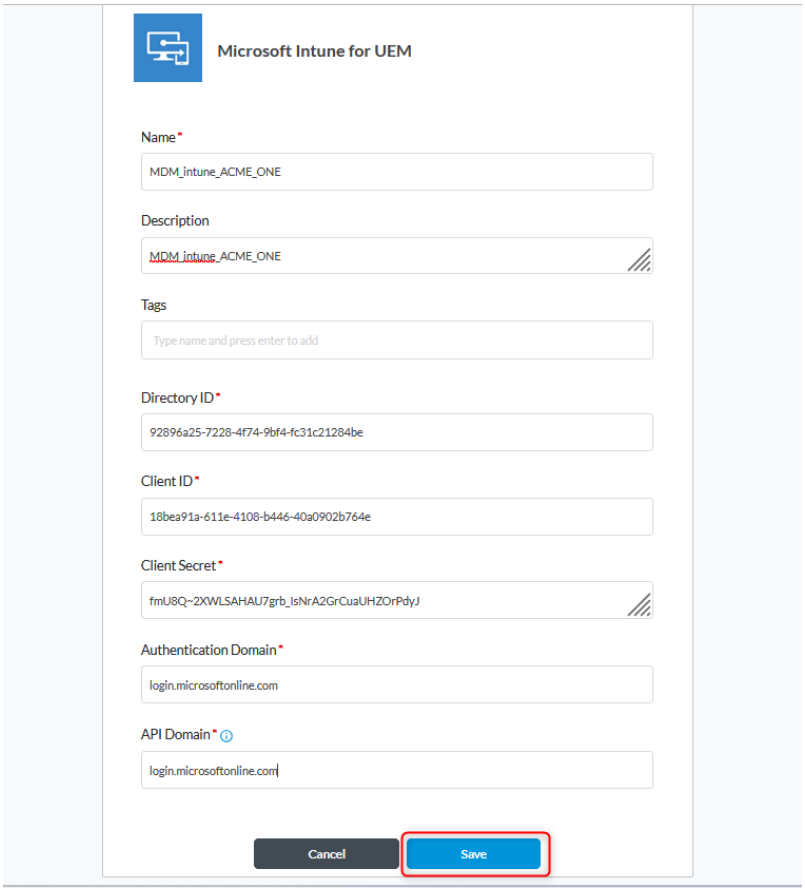
Client Secret **(Required)**	Enter the client secret provided by the graph (Intune) server, in string format.
Authentication Domain **(Required)**	Enter the domain name to use for authentication. login.microsoftonline.com
API Domain **(Required)**	Enter the domain name to use for APIs. graph.microsoft.com

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

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

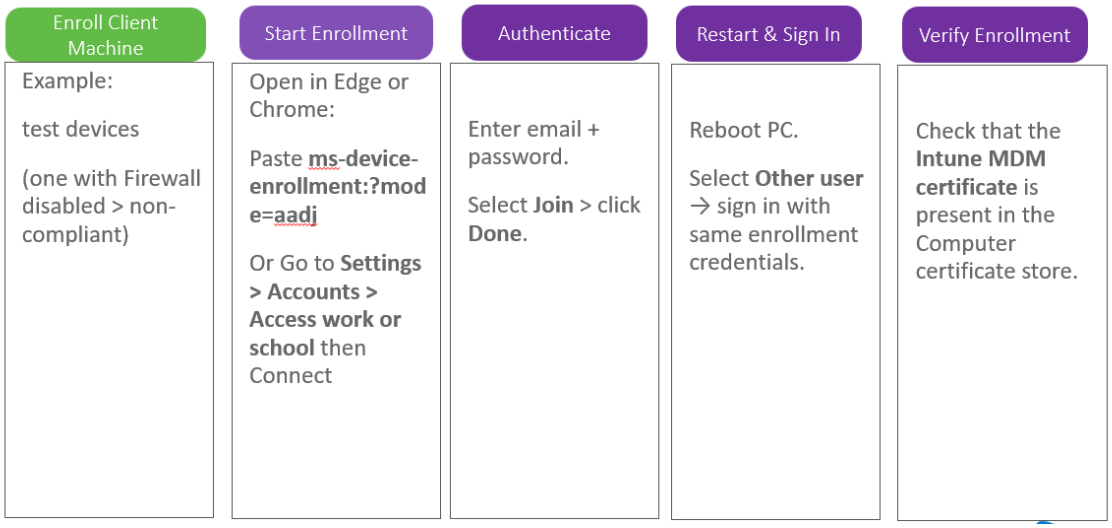
Note: The **Authentication Domain** and **API Domain** values shown on table represent the standard default values used in most **Microsoft Intune integrations**. These values apply to regular commercial tenants. Environments using sovereign clouds or specialised infrastructure may require different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

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



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.



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:

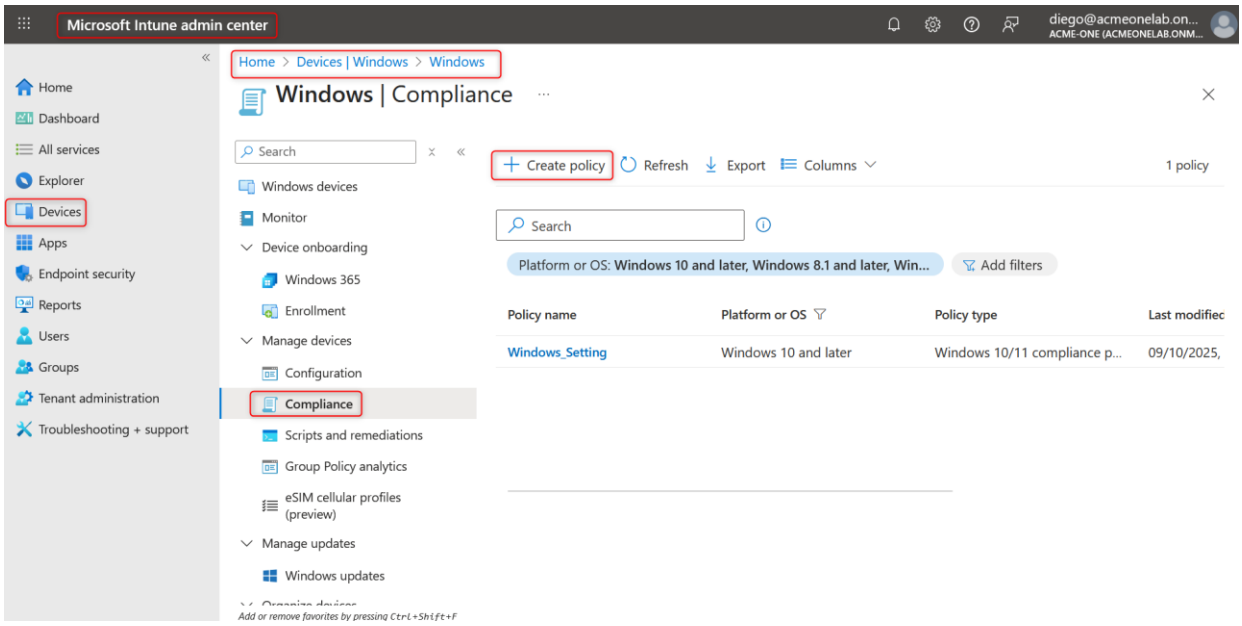
https://endpoint.microsoft.com

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

Devices > Windows > Compliance > Create policy

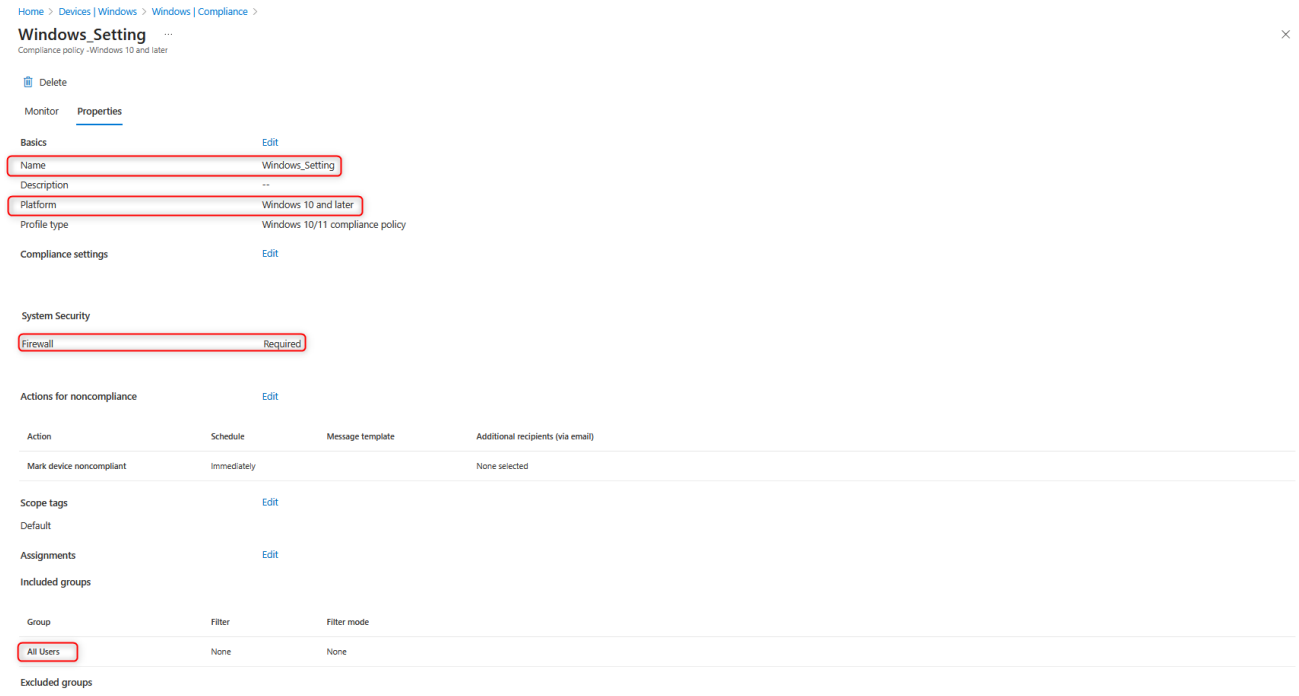
Description

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

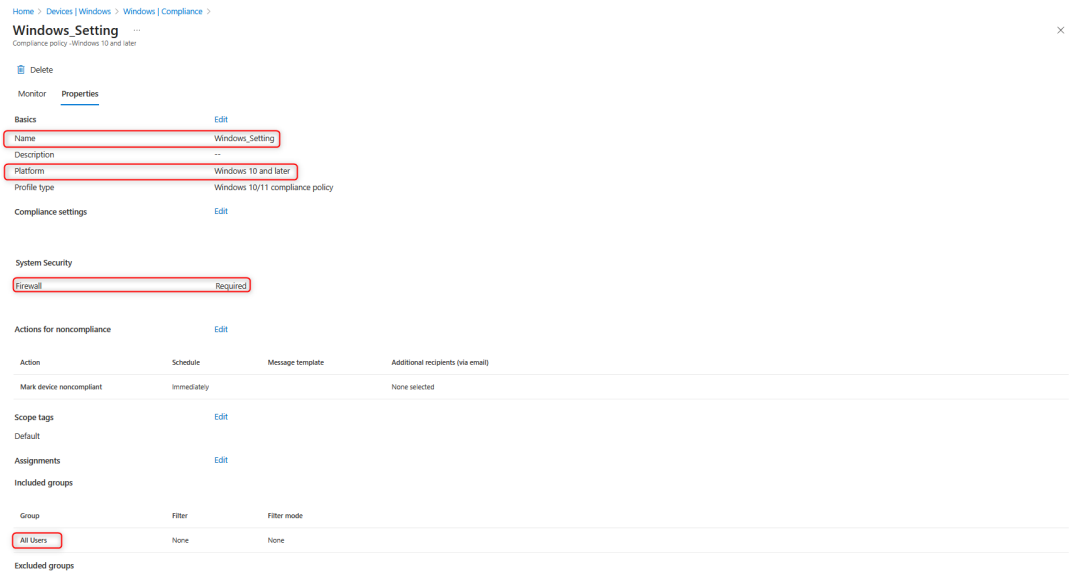
As an example in policy, the requirement is set for the **Firewall** to be enabled, and the policy is assigned to the **All Users** group. The slide illustrates how a basic Windows compliance rule appears once created.



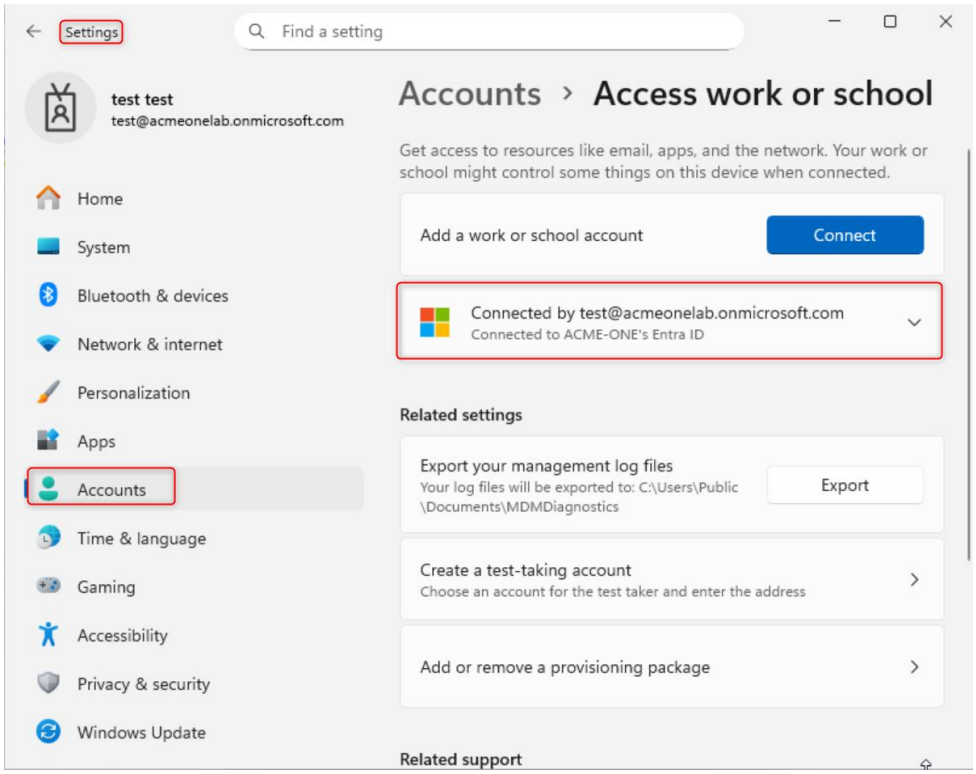
2. Review Compliance Policy Example

Device Enrollment (Compliance Policy Example)

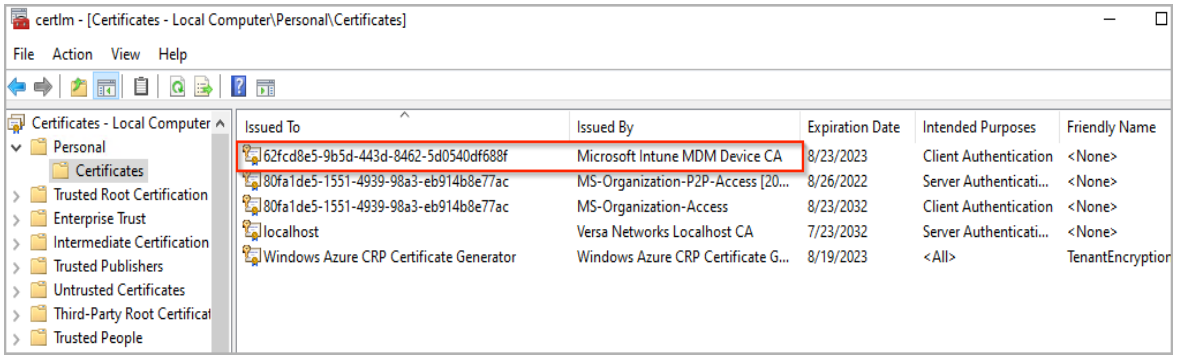
This example shows how a Windows compliance policy appears once configured in Microsoft Intune. The policy named **Windows_Setting** is applied to **Windows 10 and later** devices and includes a requirement for the **Firewall** to remain enabled. The policy is assigned to **All Users**, ensuring that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



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

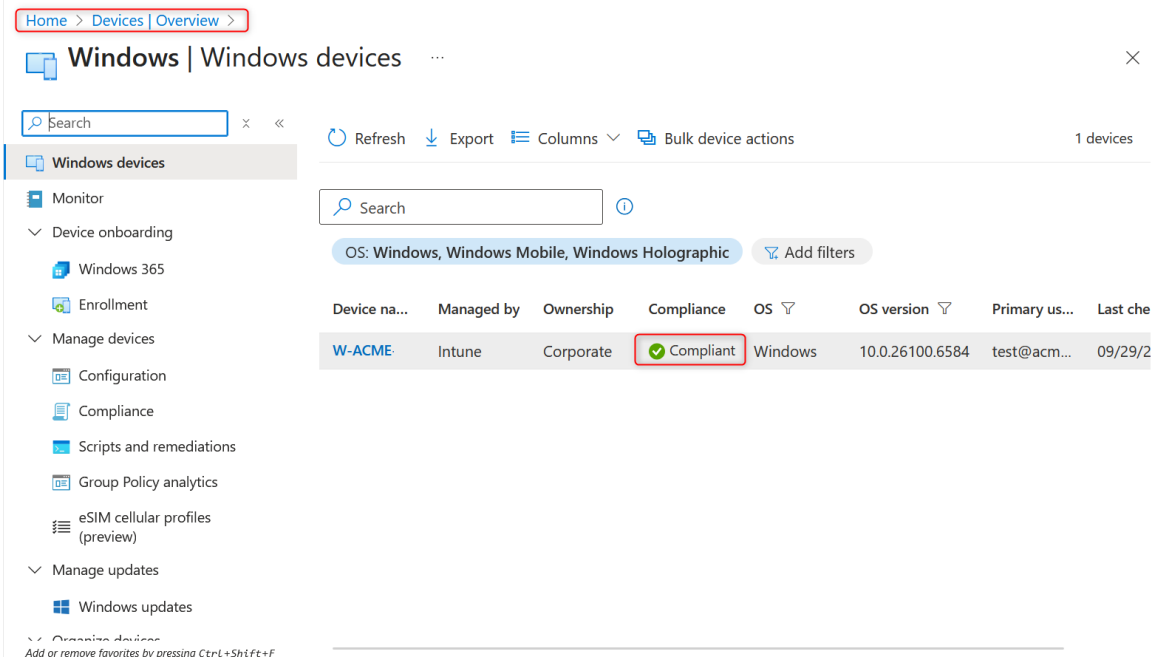
To confirm that your enrolled Windows device has synchronized with Intune and is reporting its compliance posture, check the device list inside the **Microsoft Intune admin center**.

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.



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

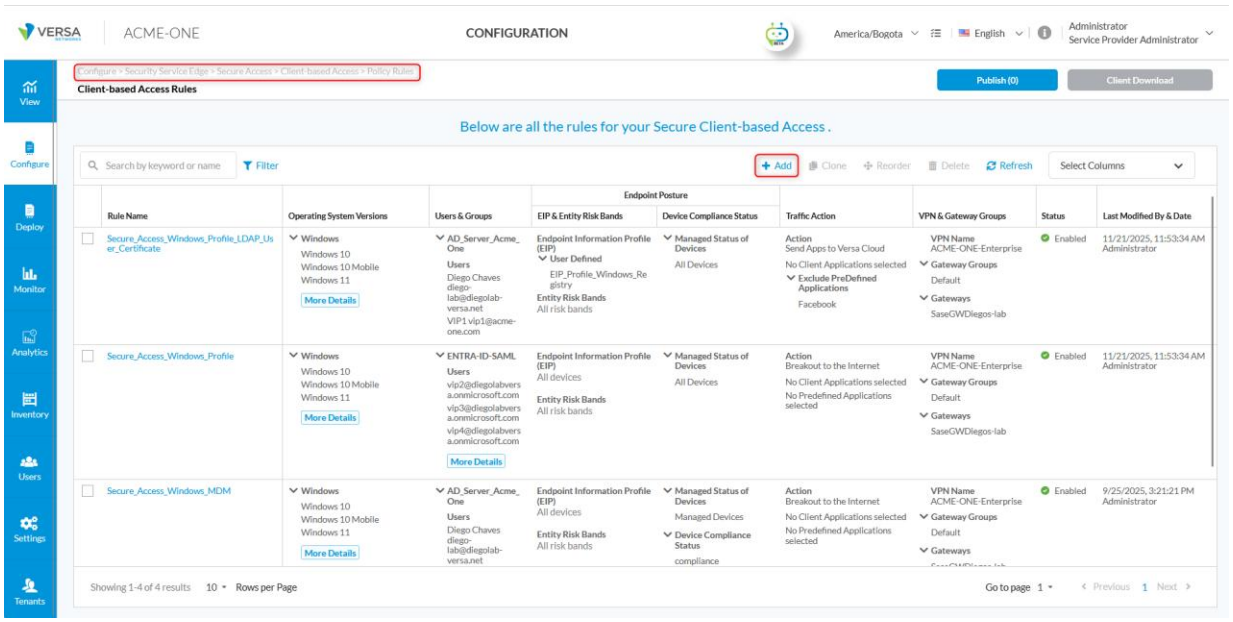
In **Concerto,** go to:

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**.

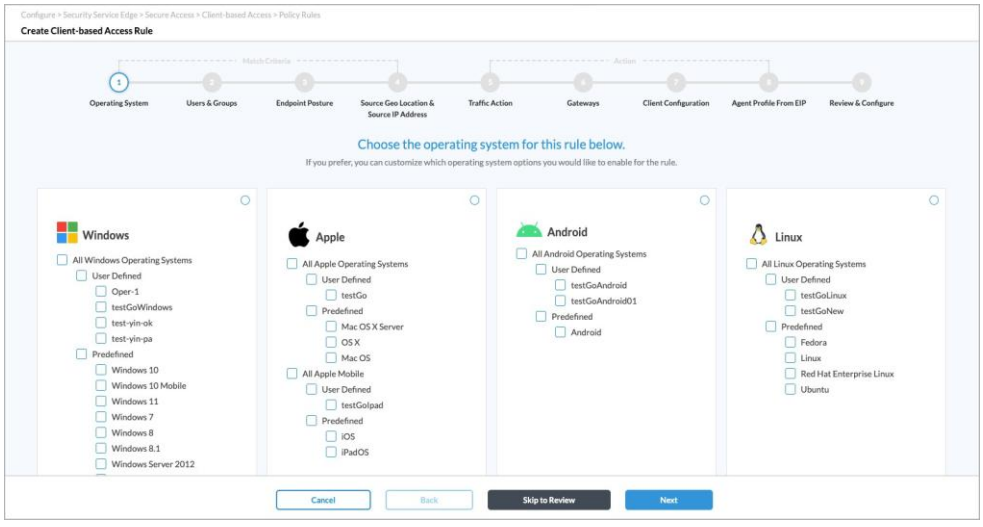
This rule will control access for **compliant** and **non-compliant** devices.



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

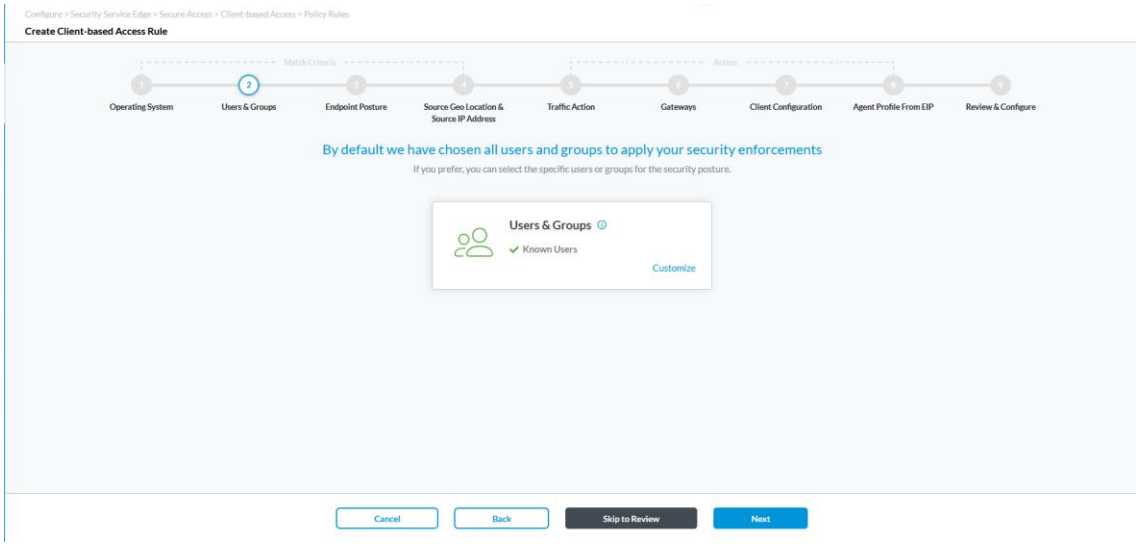
Step 1 – Operating System

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



Step 2 – Users and Groups

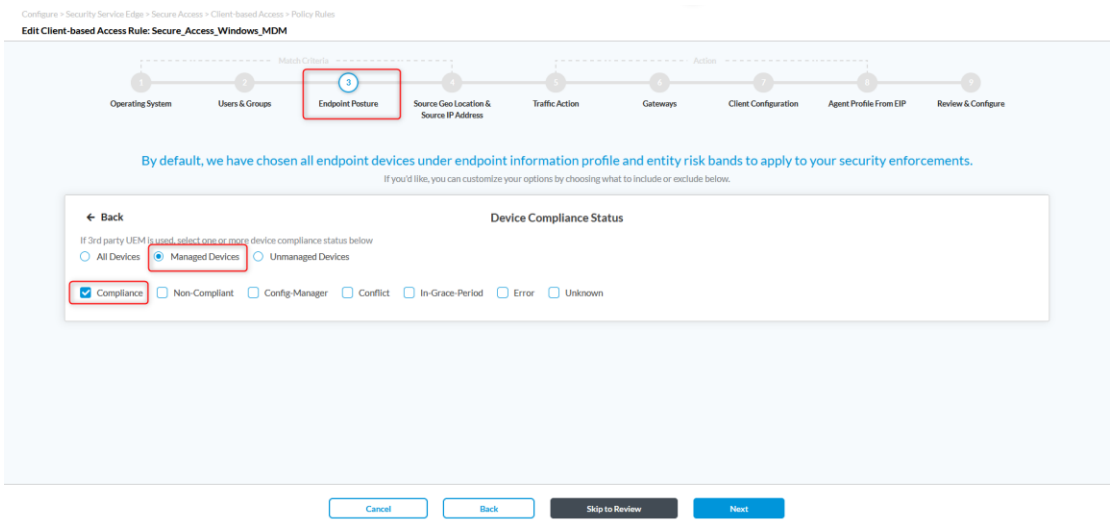
Choose the users or groups that should be included in this access rule.



Endpoint Posture

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

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



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

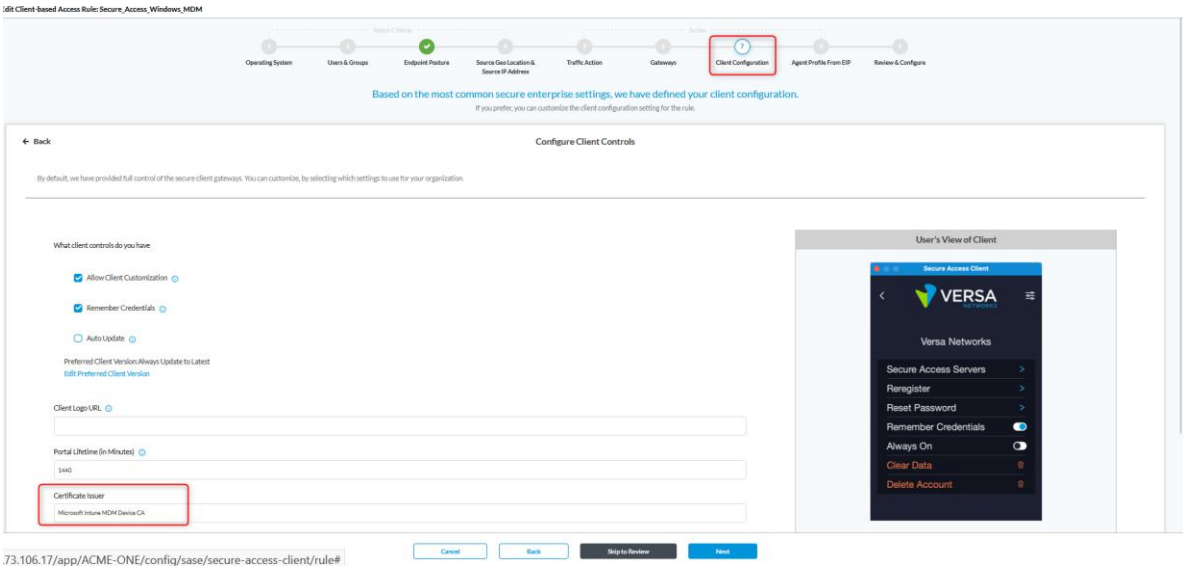
Client Configuration

- **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 saccess

set debug saccess level all

set debug saccess 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

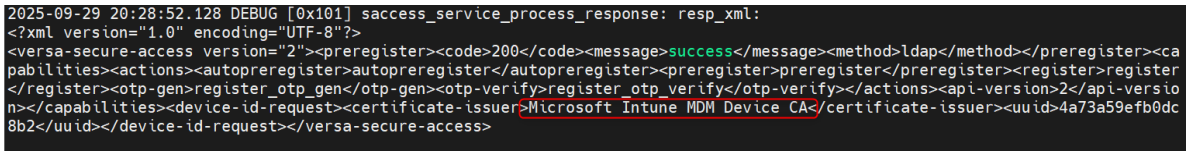
After enabling the debug flags, review the logs:

Go to **Logs** then *run*

tail -f versa-service.log

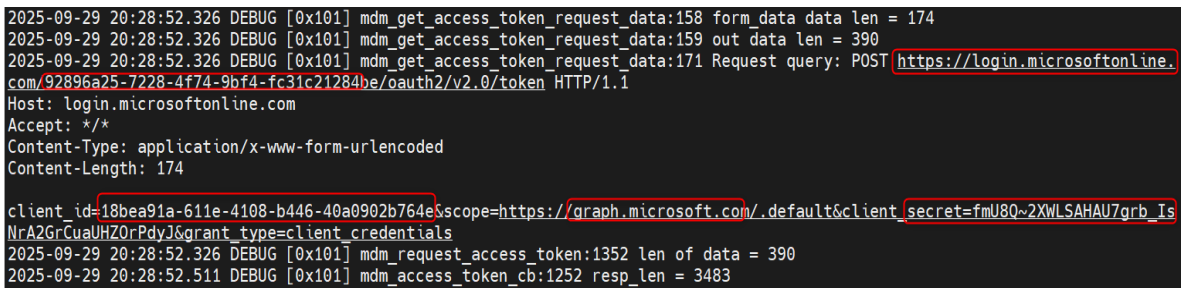
When the configuration is applied and the device begins registration, the logs should show:

- 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.



- 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.

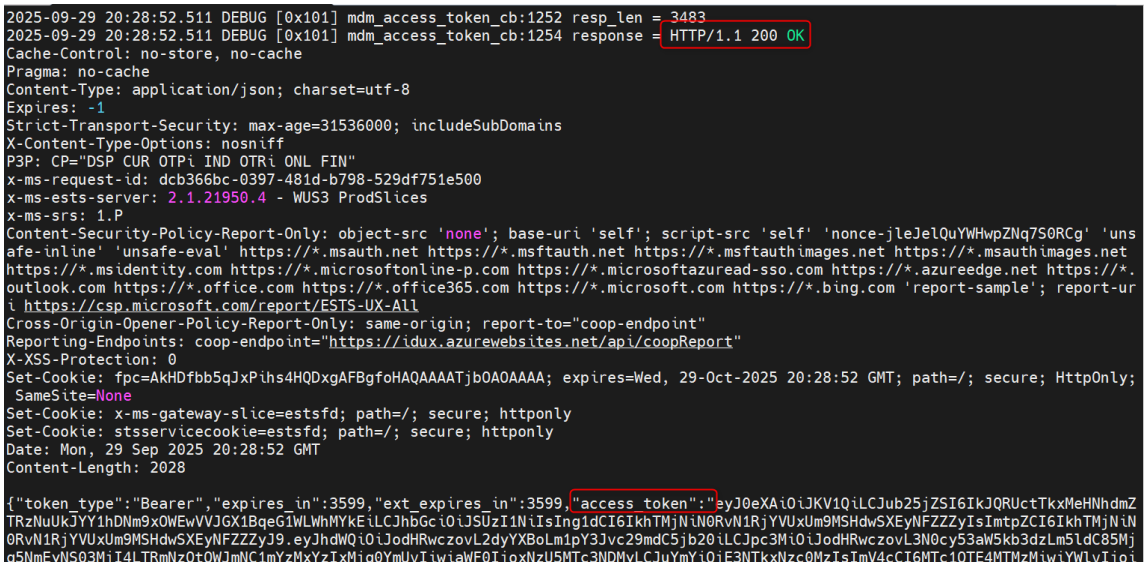


- Verification – Token Response Validation

A successful query to Microsoft should return:

- **HTTP/1.1 200 OK**, confirming that Microsoft's OAuth service accepted the request and returned a valid response.
- An **access_token value in the response payload**, showing that Intune authentication succeeded and VOS now has the token required to query Microsoft Graph for device compliance.

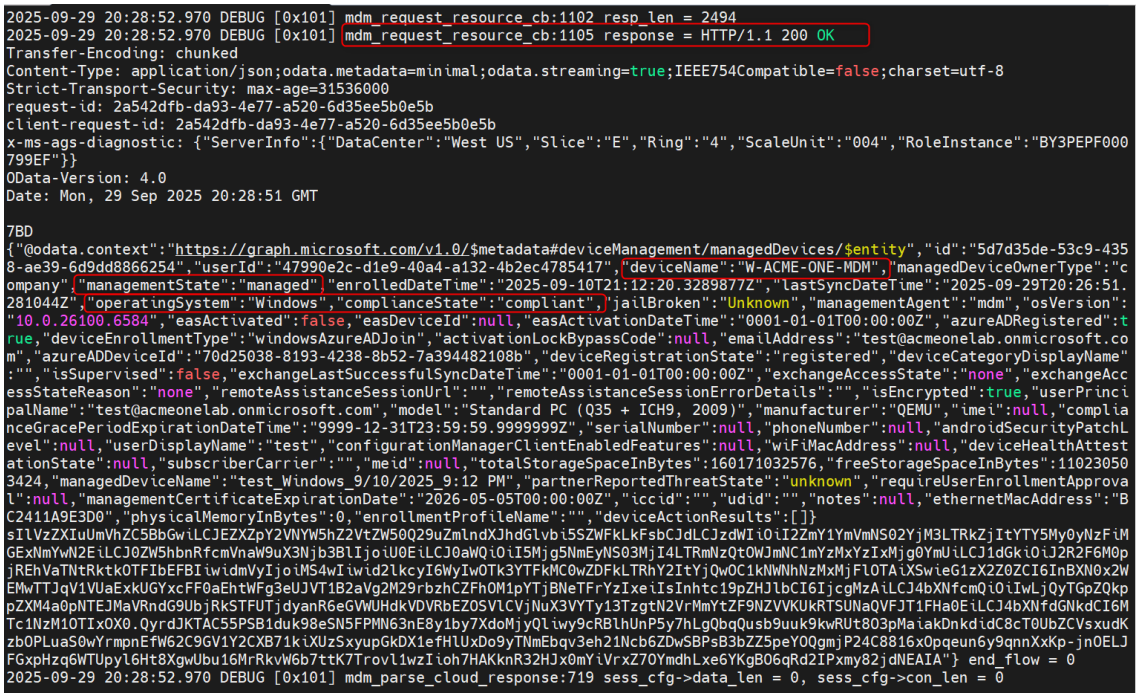
Important Note: VOS stores this token internally. Any further API communications to fetch the compliance details are generated using the saved access tokens.



All these log entries indicate that Secure Access Gateway is requesting Intune tokens and validating the enrolled device as expected.

Additionally in the debug logs, you should verify key fields returned by Microsoft Graph, such as:

- **Device ID / Device Name** (for example, *W-ACME-ONE-MDM*)
- **Management State** (e.g., *managed*)
- Operating System & OS Version
- **Compliance State** (e.g., *compliant* or *non-compliant*)



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 saccess session history all br
- show saccess session history all br | grep <<user>>
- show saccess session history id <<no>>

MACOS Enrollment

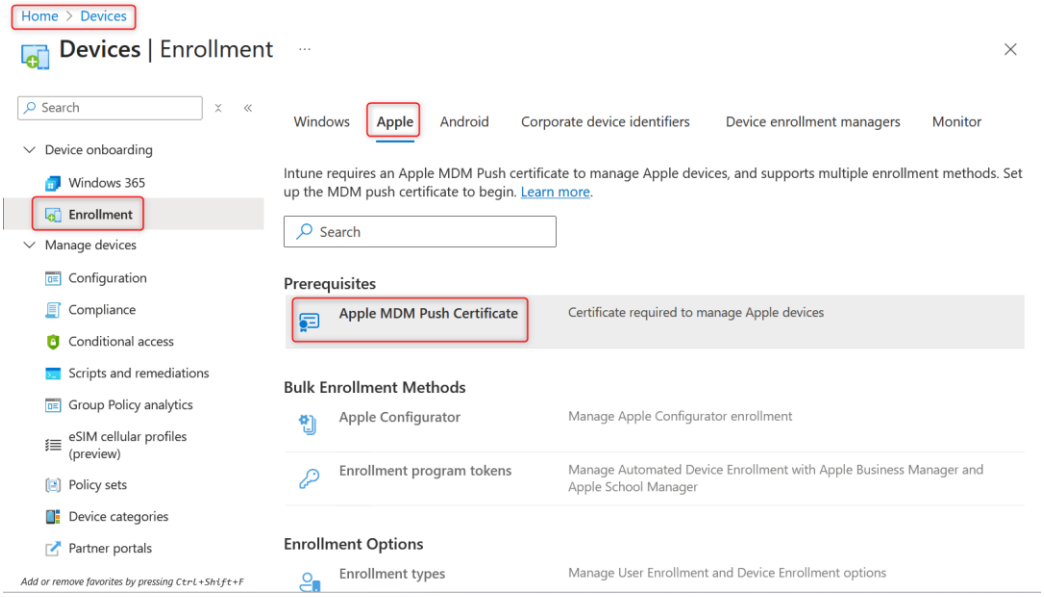
This walkthrough shows how to enroll a macOS device in Microsoft Intune and how its compliance state appears in VOS. It validates that the Intune integration behaves consistently across operating systems.

Generate the Apple MDM Push Certificate

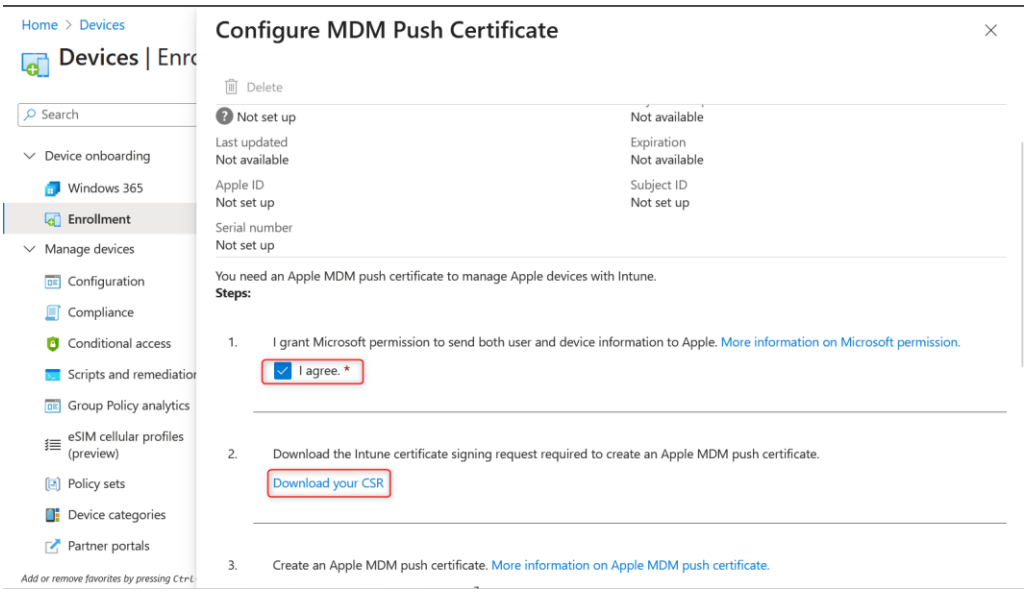
To start macOS enrollment, you first need the Apple MDM Push certificate in Intune.

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



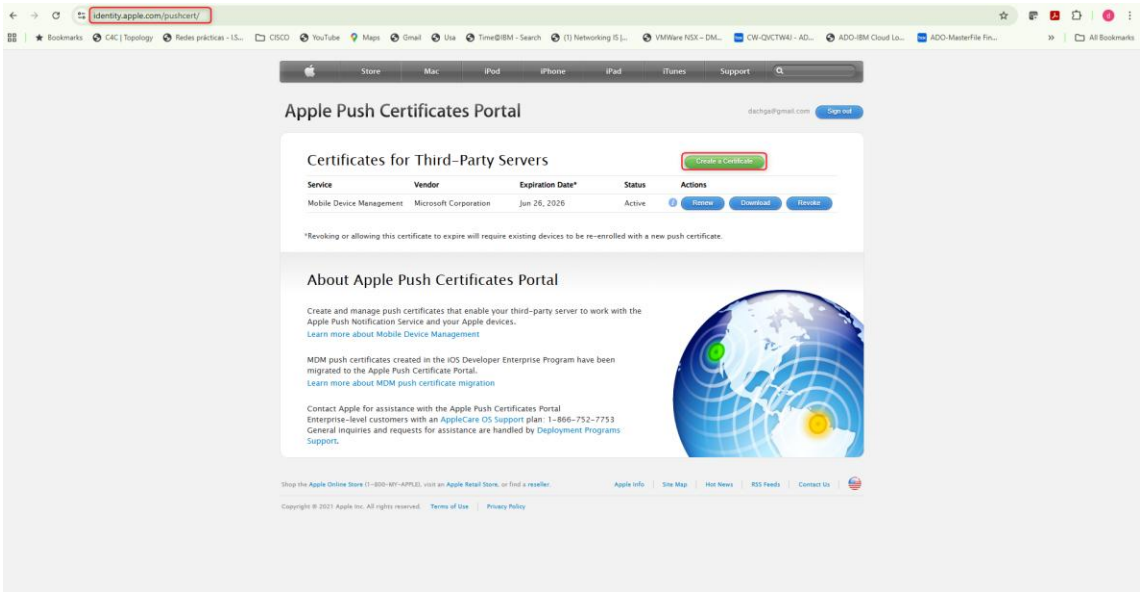
- In the **Apple MDM Push Certificate** area, review the permissions and select **I agree** to allow Microsoft to send device information to Apple.
- Click **Download your CSR** to download the Microsoft-signed .csr file.
    - Save this .csr file locally; you will use it later in Apple's portal when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



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

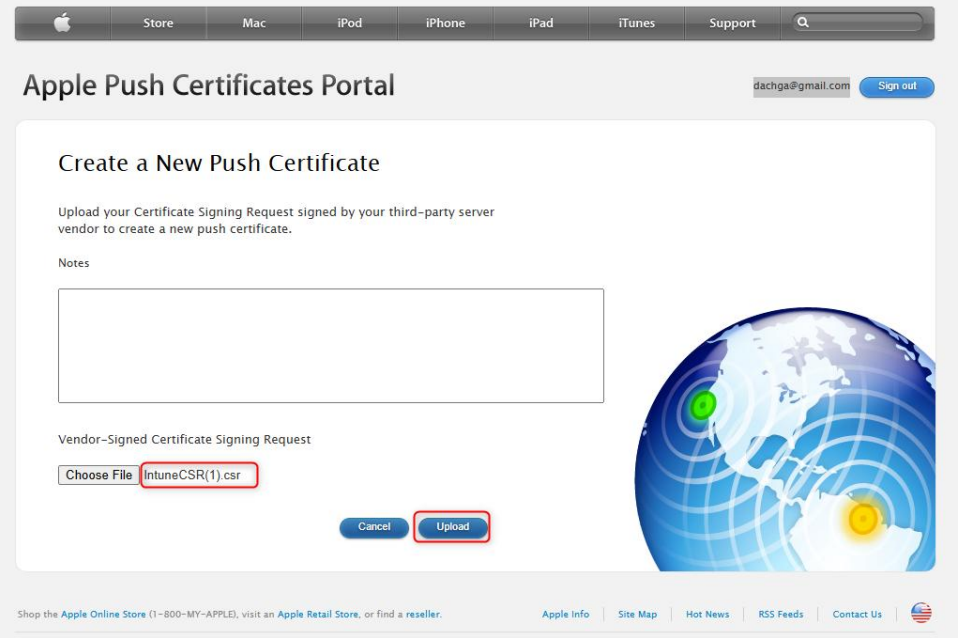
After downloading the **Intune CSR file**, use your **Apple ID** to request the MDM push certificate in the Apple portal.

- 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.



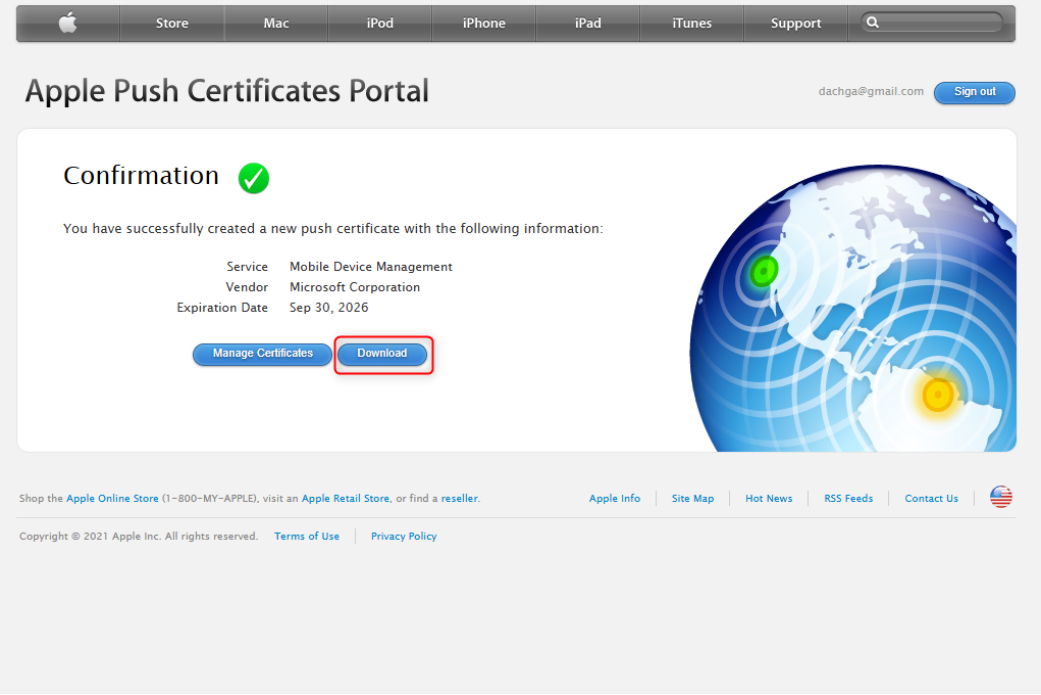
On the Apple Push Certificates Portal, select the **correct .csr file** you previously downloaded from Intune (locate it on your laptop).

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



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

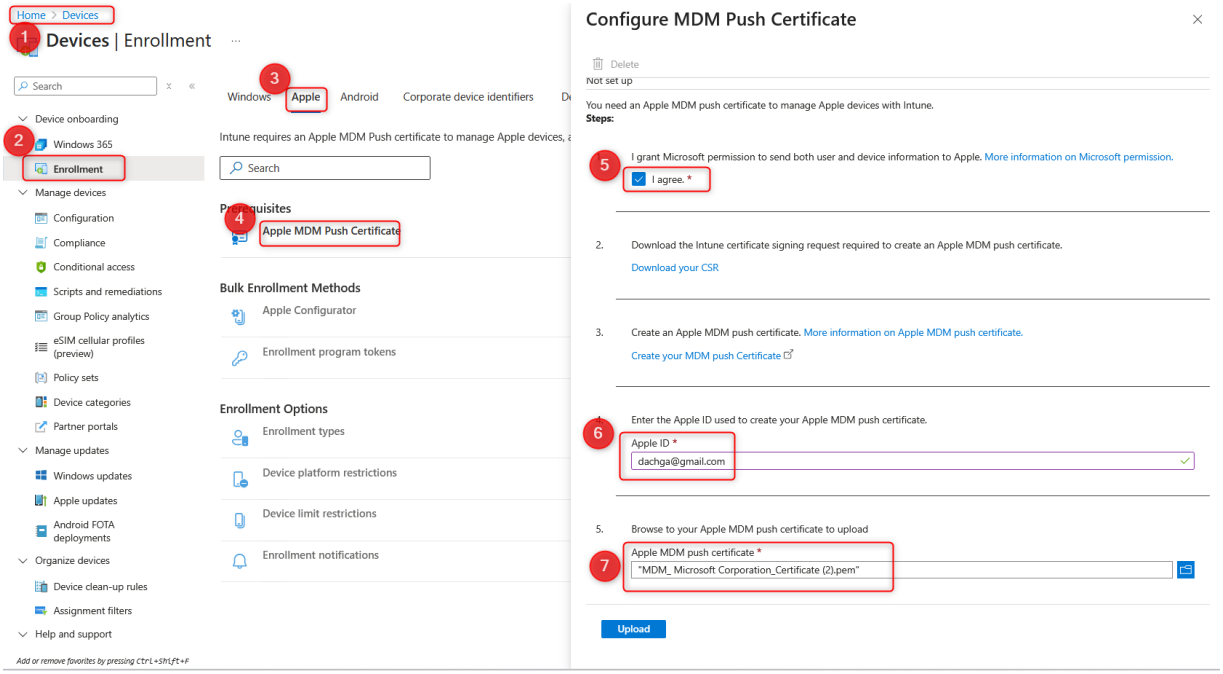
- Click Download to obtain the new **MDM Push Certificate (.pem).**



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.

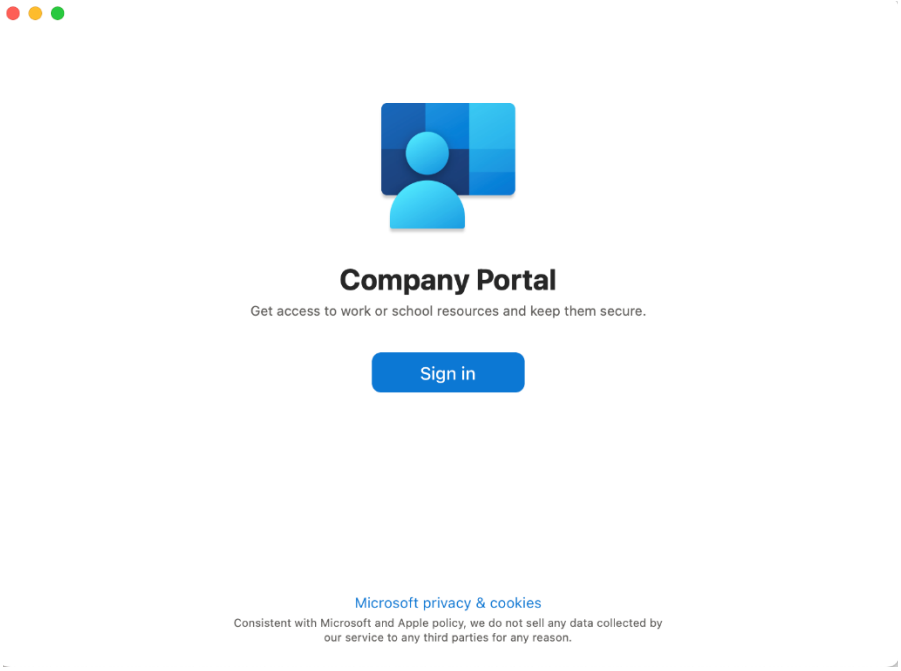
Install Company Portal on macOS

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

application.

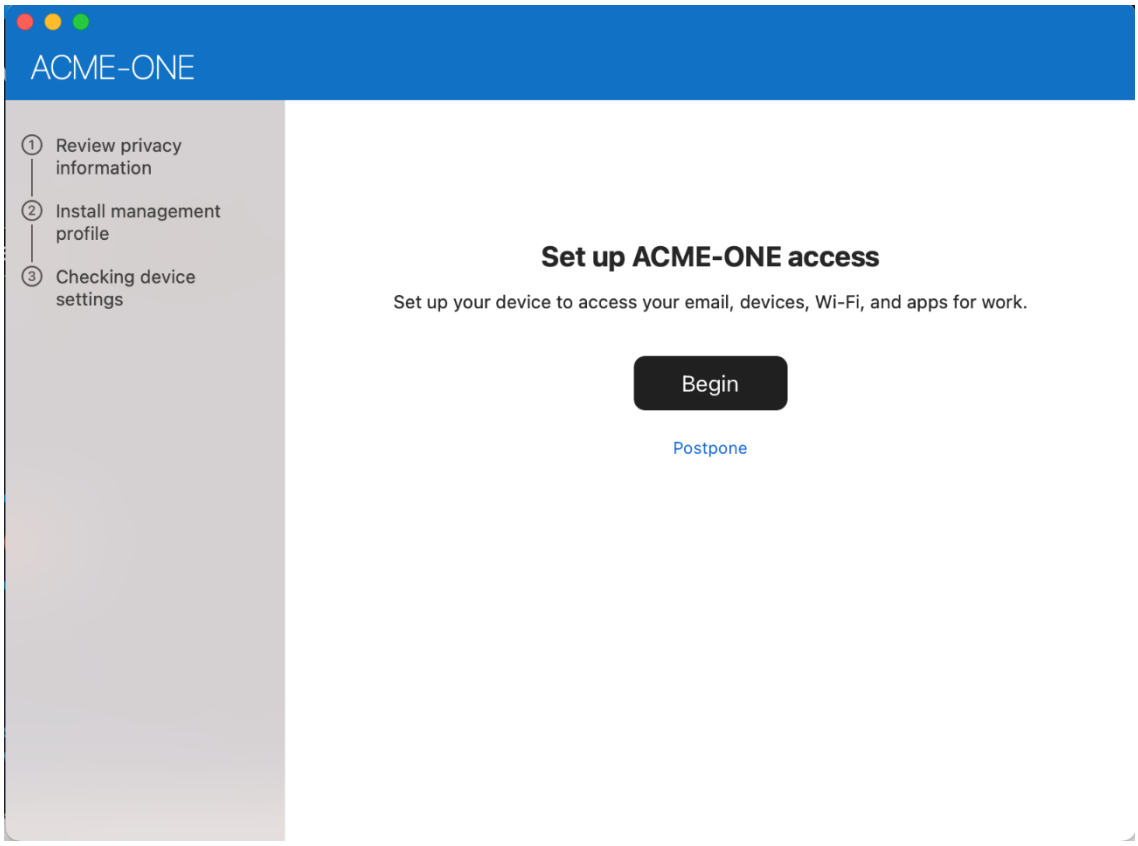
1. Install and sign in Microsoft Company Portal

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



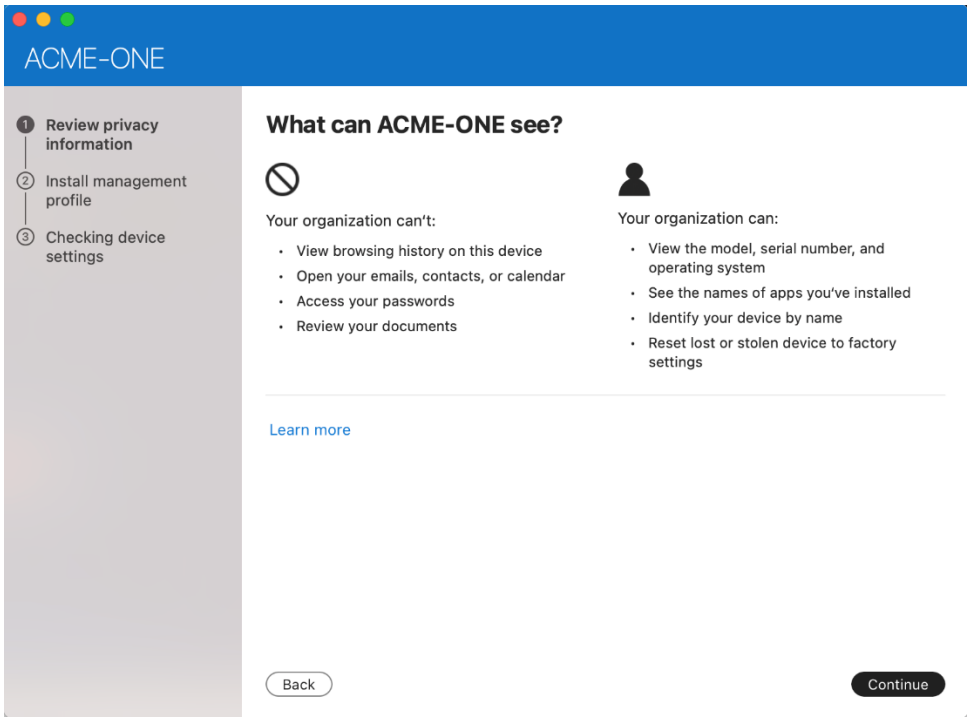
After installation, **sign in using your Intune corporate account** with your work or school email and password to start the enrollment process.

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

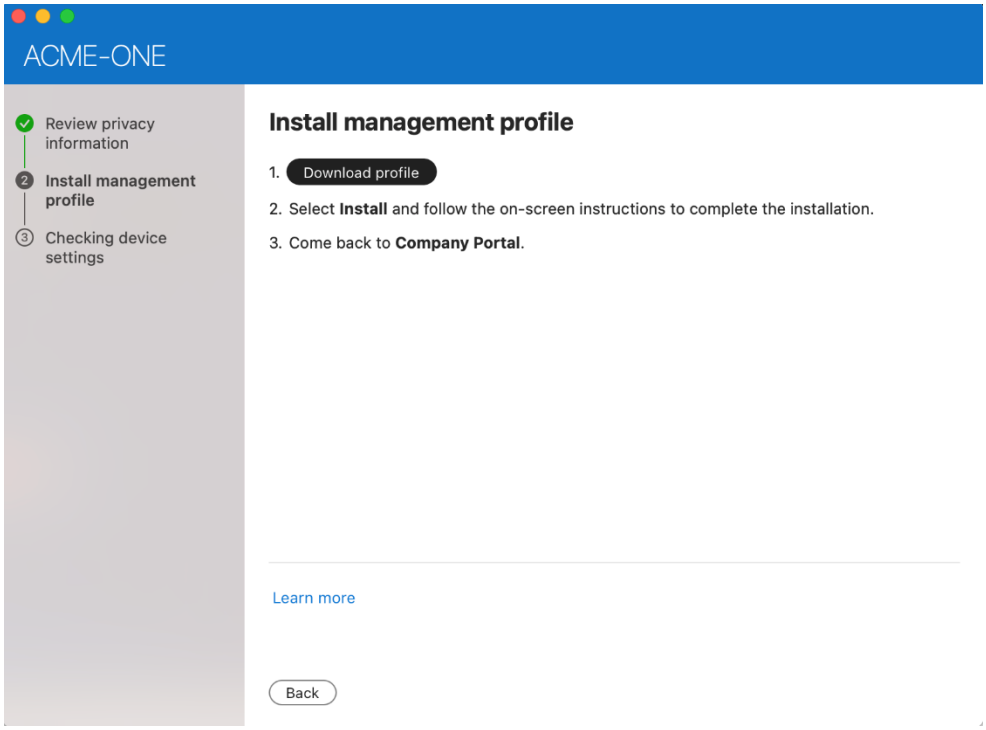


macOS will then display the **privacy information**, showing what your organization *can* and *cannot* see on the device.

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



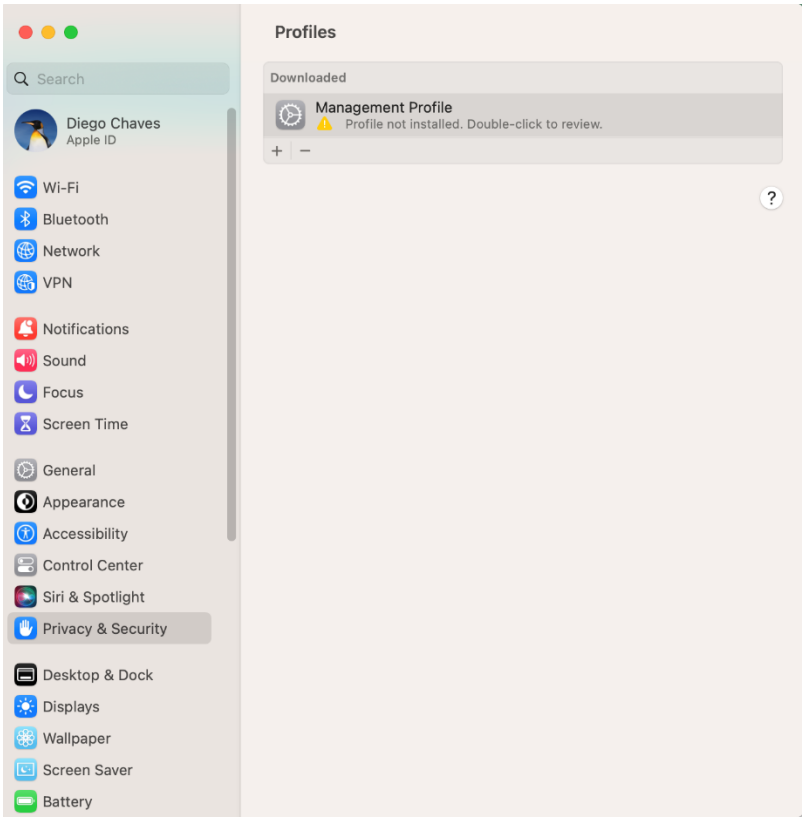
Install the management profile > Click **Download profile**, open the downloaded file, select **Install**, and follow the on-screen instructions.



2. Install the downloaded profile in macOS

Open System Settings > Privacy & Security > Profiles.

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



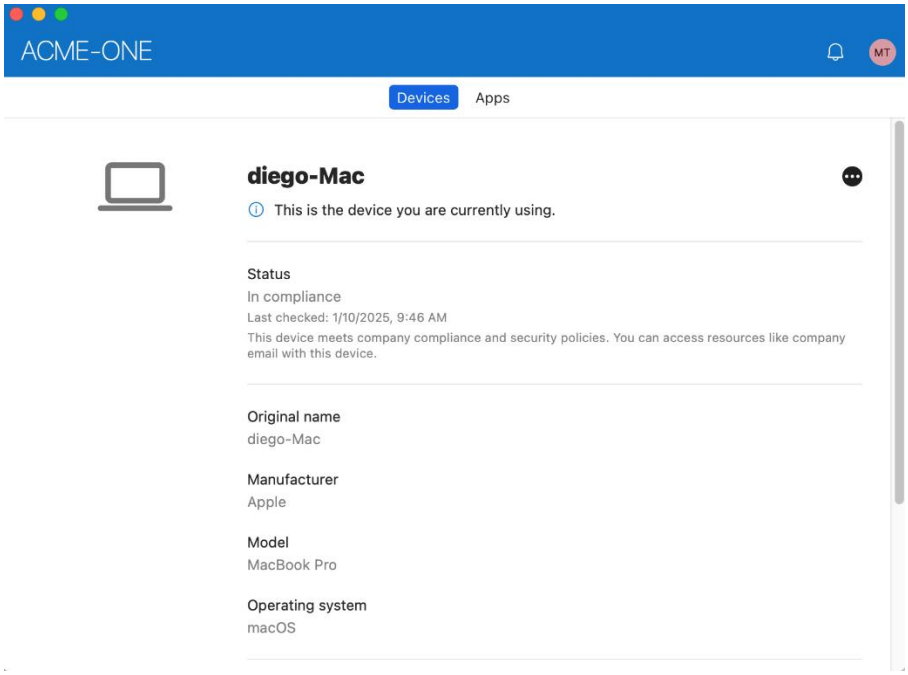
- Click **Install** and follow the on-screen instructions to complete the profile installation.

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

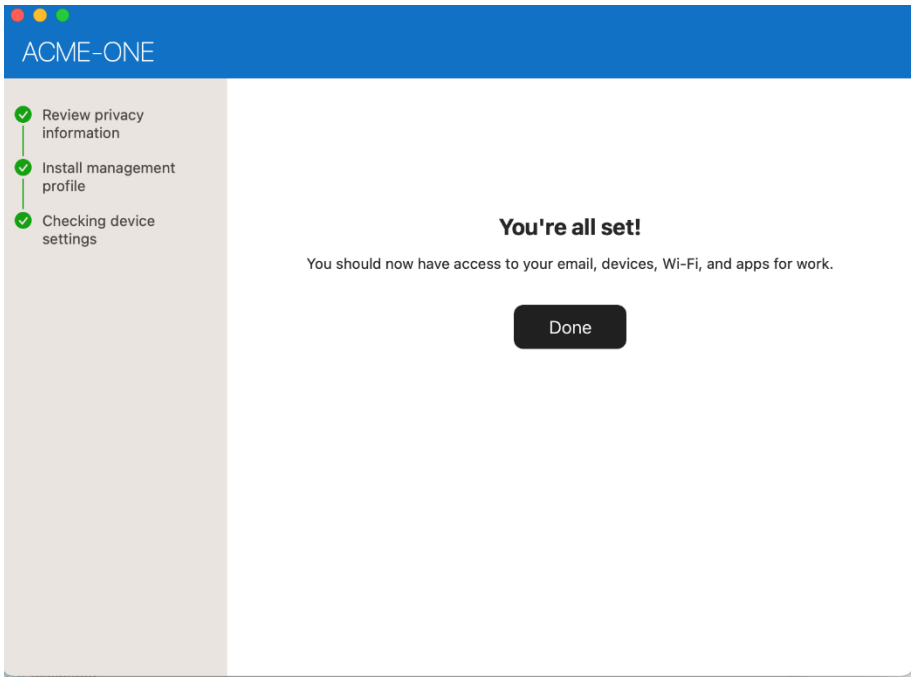
Complete Enrollment > After the management profile is installed, Intune validates the device and updates its status.
If everything is successful, the Mac will appear as **"In compliance"** in the Company Portal.

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

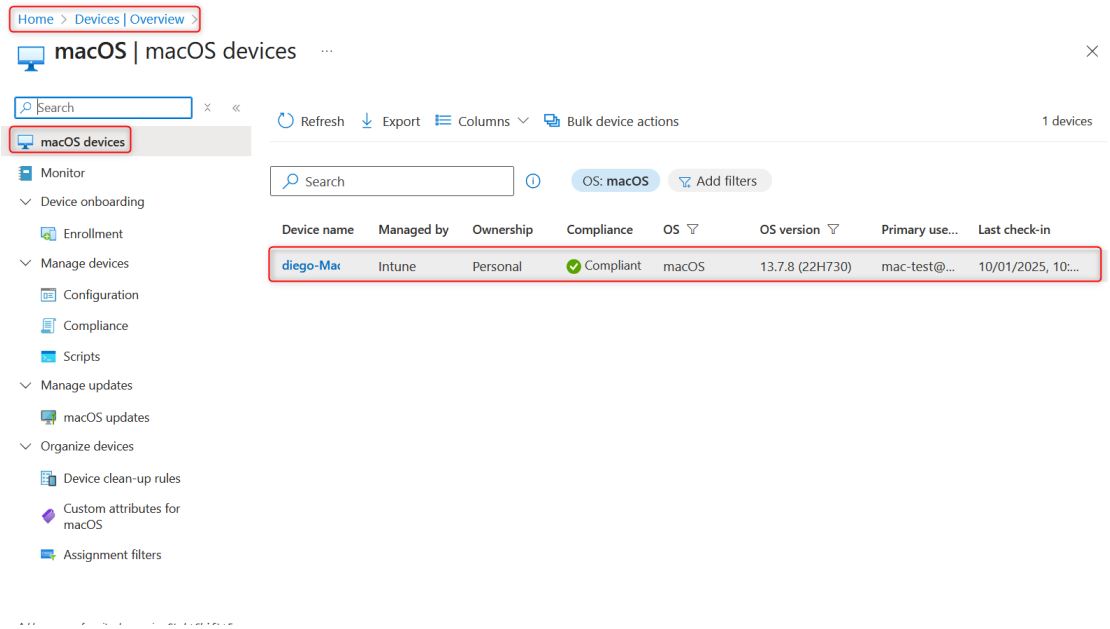
After enrollment, the Mac may take **10–15 minutes** to appear in the Microsoft Endpoint Manager portal.

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

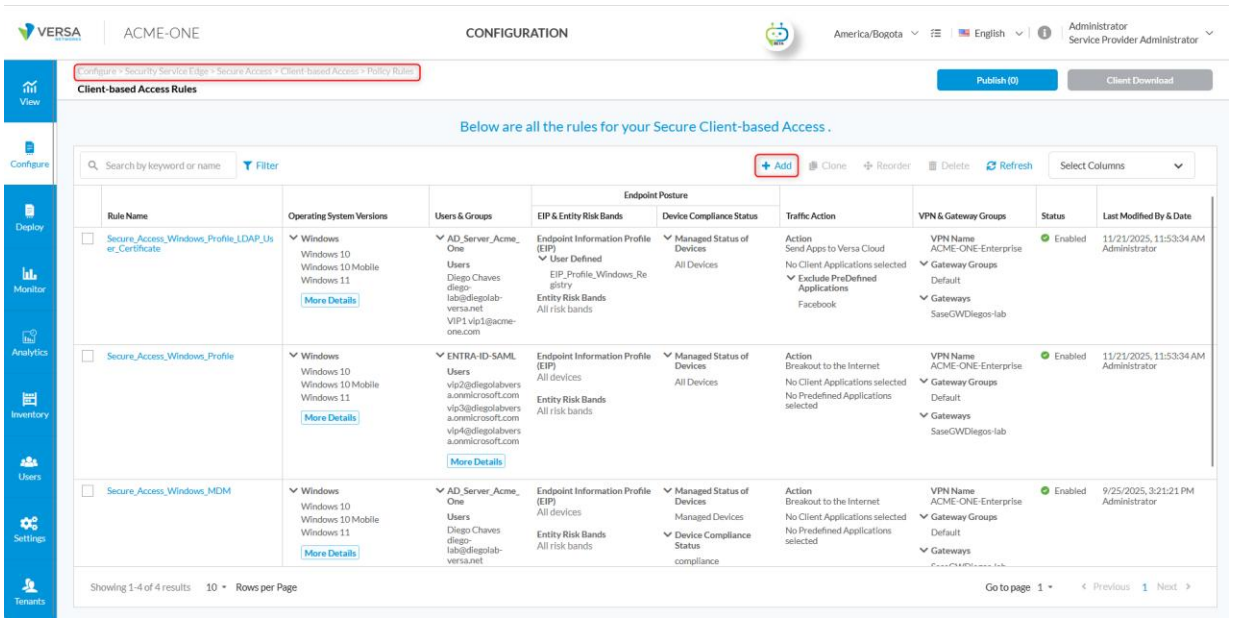
In Concerto, go to:

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**.

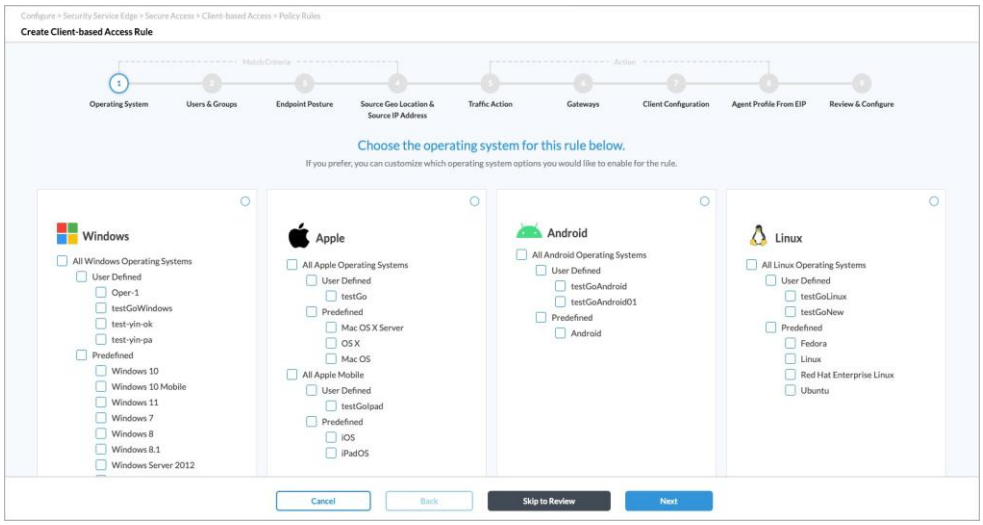
This rule will control access for **compliant** and **non-compliant** devices.



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

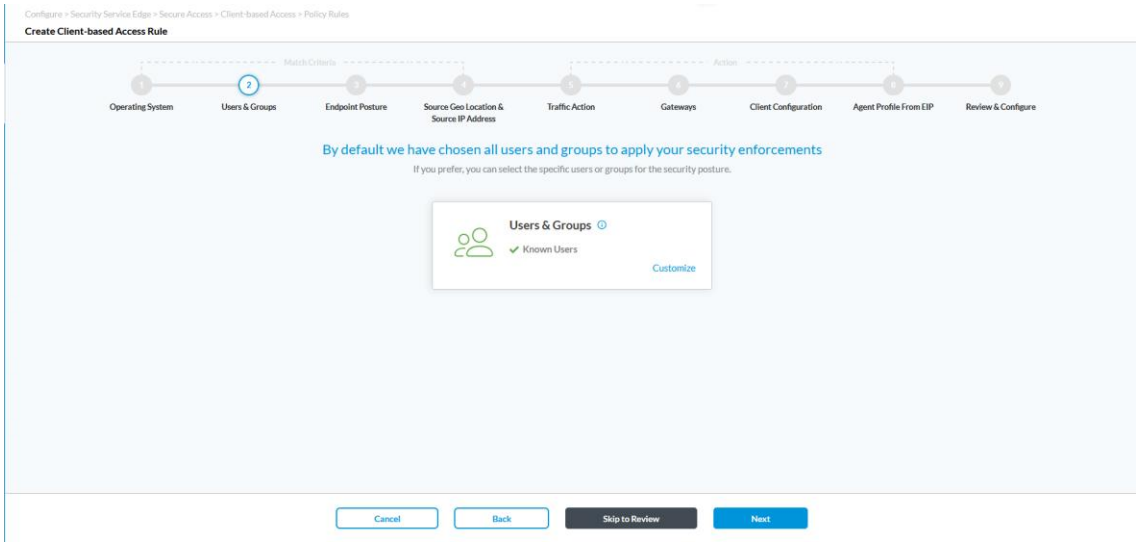
Step 1 – Operating System

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



Step 2 – Users and Groups

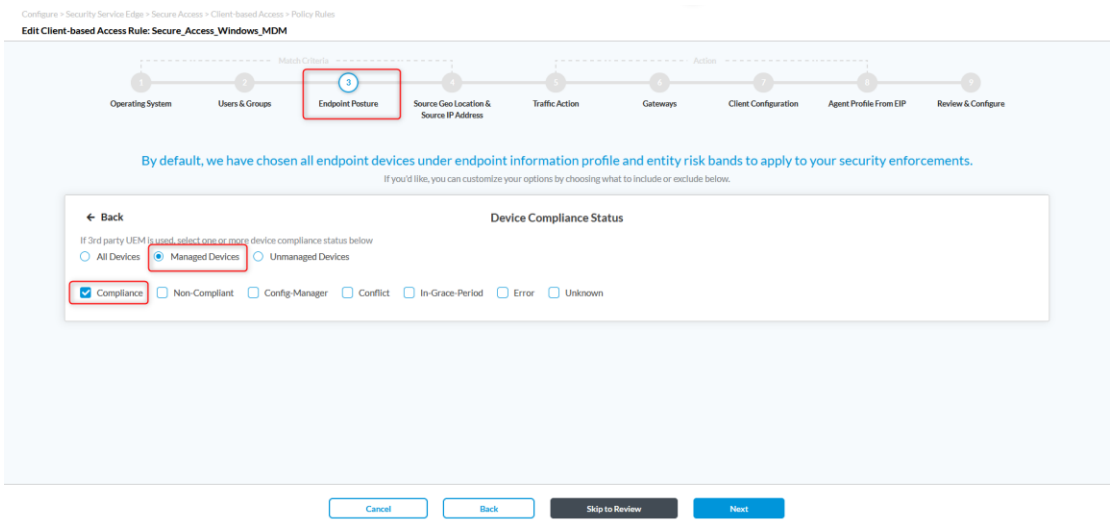
Choose the users or groups that should be included in this access rule.



Endpoint Posture

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

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



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

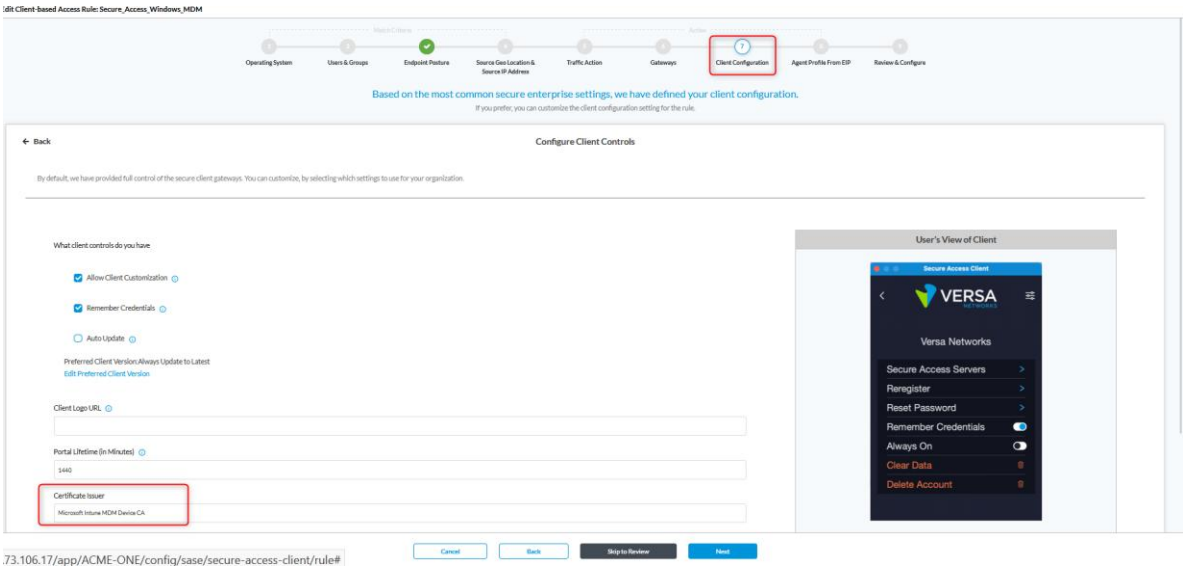
Client Configuration

- 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.

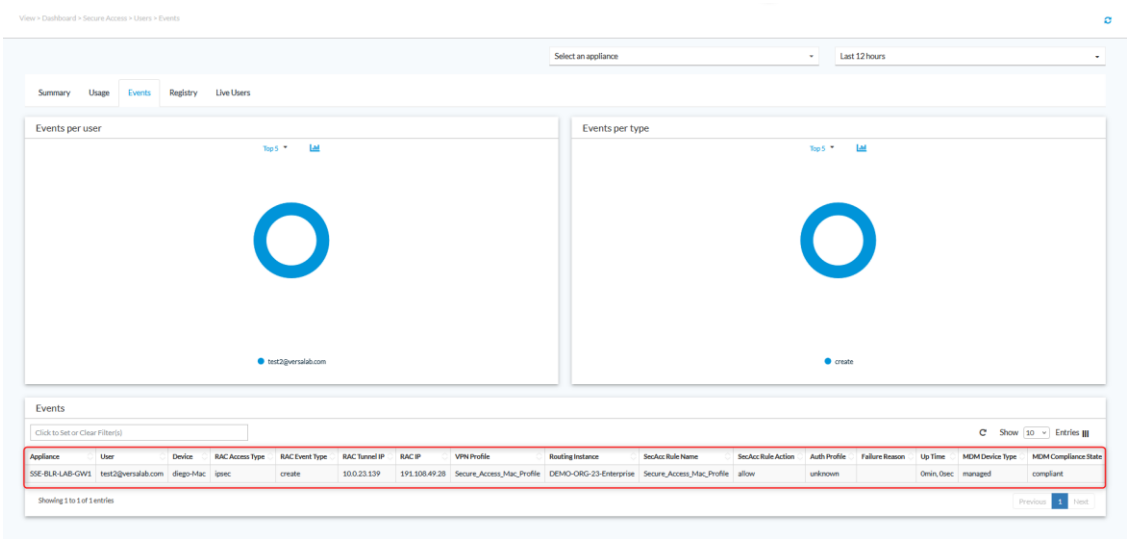
If the **Certificate Issuer** is not set, the SASE Client will **not send the device ID** when connecting to gateways, causing the policy match to fail.



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.