

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:
 - o Device ID
 - o 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.

Microsoft 365 admin center

Home > Licenses

Subscriptions Requests Auto-claim policy

Select a product to view and assign licenses. Each product below may contain licenses from multiple subscriptions. [Learn more about assigning licenses](#)

Manage billing or buy more licenses in [Your products](#).

Export to CSV Refresh 2 items Search

Filters: Account type: Organization, Self-service

Name	Available licenses	Assigned licenses	Account type
Enterprise Mobility + Security E5	23	2/25	Organization
Microsoft 365 Business Premium	23	2/25	Organization

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.

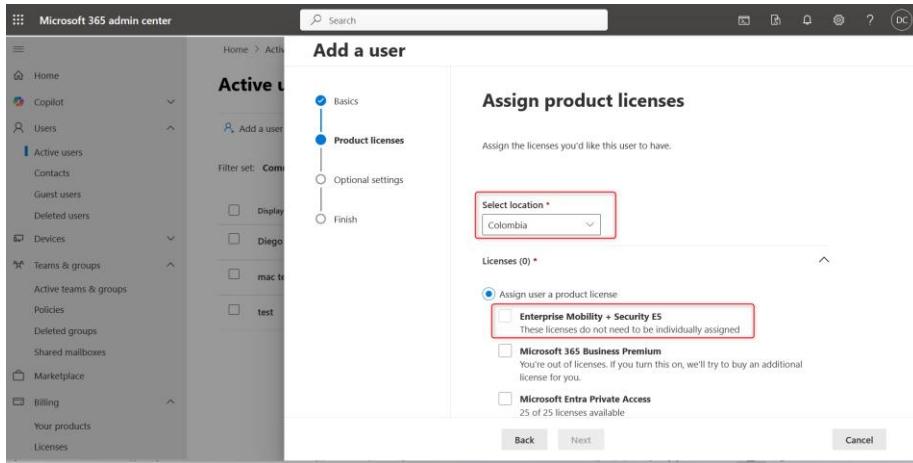
This page displays all users currently registered in your Microsoft tenant.

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

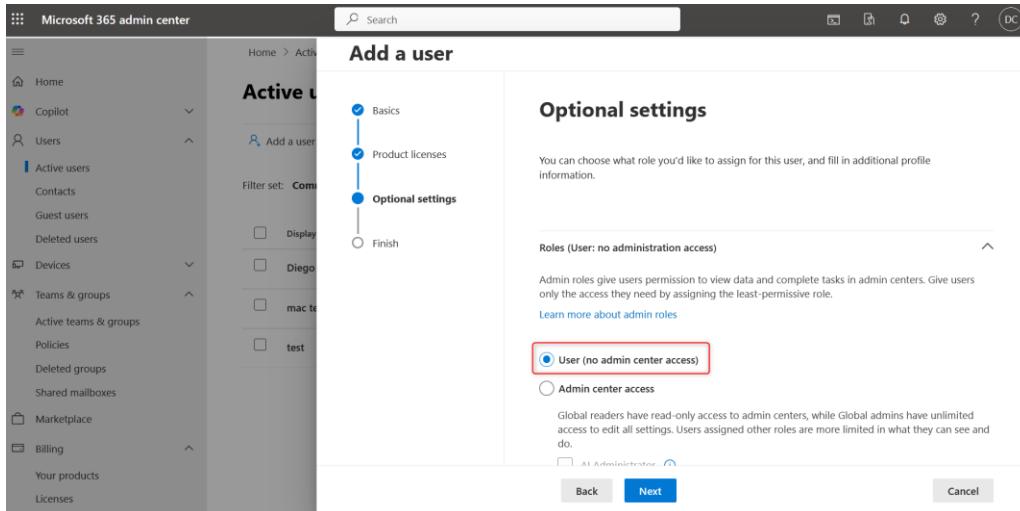
When creating a user, ensure that the account is assigned an appropriate usage location, as licensing availability depends on this attribute.

Display name	Username	Licenses
Diego Chaves	diego@acmeonelab.onmicrosoft.com	Enterprise Mobility + Security E5, Microsoft Premium
mac test	mac-test@acmeonelab.onmicrosoft.com	Microsoft 365 Business Premium, Enterprise Security E5
test	test@acmeonelab.onmicrosoft.com	Microsoft 365 Business Premium, Enterprise Security E5

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 & groups

Active teams and groups

About Groups Using Teams And SharePoint Where to store files

Teams & Microsoft 365 groups Distribution list Security 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@acmeone.lab.onmicrosoft.com	Syncing	Active	Assigned	Public	September 2, 2023, 2:24 PM
All Company	allcompany@acmeone.lab.onmicrosoft.com	Syncing	Active	Assigned	Public	September 2, 2023, 2:30 PM

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 *

Describe this team
 Enter a description for your new team

Next Cancel

Assing at least on owner to the Group

Microsoft 365 admin center

Home > Active teams and groups > Add a team

Add owners

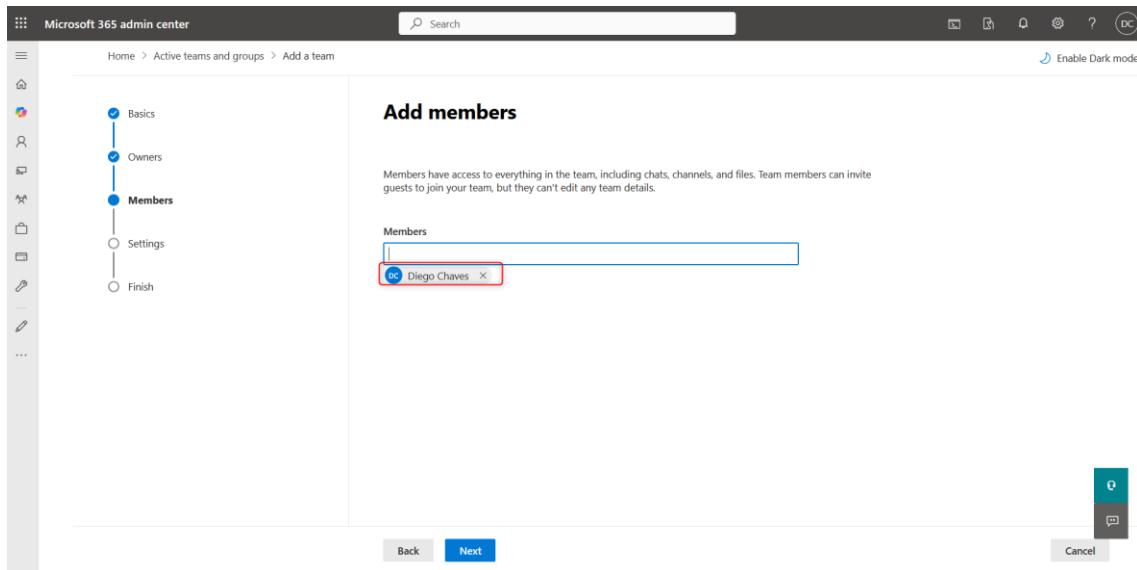
Team owners can add or delete members, edit team details, and delete conversations.

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 *

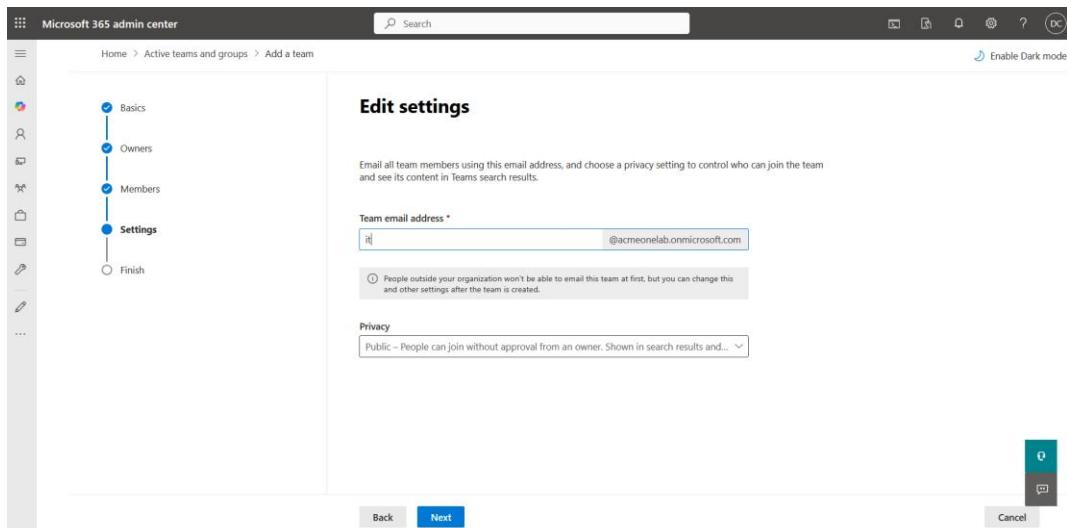
Back Next Cancel

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



The screenshot shows the 'Add members' step of the 'Add a team' wizard in the Microsoft 365 admin center. The sidebar on the left shows a progress bar with 'Basics', 'Owners', and 'Members' completed, and 'Settings' and 'Finish' remaining. The main area is titled 'Add members' and contains a sub-instruction: 'Members have access to everything in the team, including chats, channels, and files. Team members can invite guests to join your team, but they can't edit any team details.' Below this is a 'Members' list box containing 'Diego Chaves' with a red-bordered 'X' button to its right. At the bottom are 'Back' and 'Next' buttons, and a 'Cancel' button on the right.

Choose an email to all team members.



The screenshot shows the 'Edit settings' step of the 'Add a team' wizard. The sidebar shows 'Basics', 'Owners', 'Members', and 'Settings' completed, and 'Finish' remaining. The main area is titled 'Edit settings' and contains a sub-instruction: 'Email all team members using this email address, and choose a privacy setting to control who can join the team and see its content in Teams search results.' Below this are fields for 'Team email address *' (containing 'id@acmeonelab.onmicrosoft.com') and 'Privacy' (set to 'Public – People can join without approval from an owner. Shown in search results and...'). At the bottom are 'Back' and 'Next' buttons, and a 'Cancel' button on the right.

Then **Review** and Add Team

The screenshot shows the Microsoft 365 Admin Center interface. On the left, a navigation pane lists 'Active teams and groups' with a sub-menu: 'Basics' (selected), 'Owners', 'Members', 'Settings', and 'Finish'. The main content area is titled 'Review and finish adding team' and contains sections for 'Basics' (Name: IT, Description: None provided, Edit), 'Owners' (Diego Chaves, Edit), 'Members' (None added, Edit), and 'Settings' (Email: it@acmeonelab.onmicrosoft.com, Privacy: Public, Edit). At the bottom are 'Back', 'Add team' (highlighted with a red box), and 'Cancel' buttons.

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

The screenshot shows the Microsoft 365 Admin Center 'Active users' page. The left sidebar shows 'Active users' selected. The main area shows 'Diego Chaves' with a blue 'DC' profile picture. The 'Licenses and apps' tab is selected (highlighted with a red box). A sub-menu shows 'Enterprise Mobility + Security E5' (selected with a checked checkbox), 'Microsoft 365 Business Premium' (unchecked), and 'Microsoft Entra Private Access' (unchecked). At the bottom are 'Save changes' and 'X' buttons.

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.

The screenshot shows the Microsoft Entra admin center interface. The left navigation panel is open, showing various administrative sections like Password reset, Custom security attributes, Certificate authorities, External Identities, Cross-tenant synchronization, Entra Connect, Domain names, Custom branding, and Mobility. Under Mobility, there are sub-sections: Monitoring & health, ID Protection, ID Governance, and Verified ID. The main content area is titled 'Mobility (MDM and WIP)' and shows a list of applications. The 'Microsoft Intune' application is highlighted with a red box and a red number '3' indicating it is the selected item. Other applications listed include Copilot, Home, Mobility (MDM and WIP), Add application, Refresh, Manage view, and Got feedback?.

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

X

* 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 [Learn more](#)

Register

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

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 ... X

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

Client credentials
[certificate_1 secret](#)

Redirect URLs
[Add a Redirect URI](#)

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

Supported account types
My organization only

Managed application in local directory
Concert-Intune-acmeone

Note: 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.

The screenshot shows the Microsoft Intune 'App registrations' page for the application 'Concert-Intune-acmeone'. The 'Certificates & secrets' tab is selected. A table lists one 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

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:

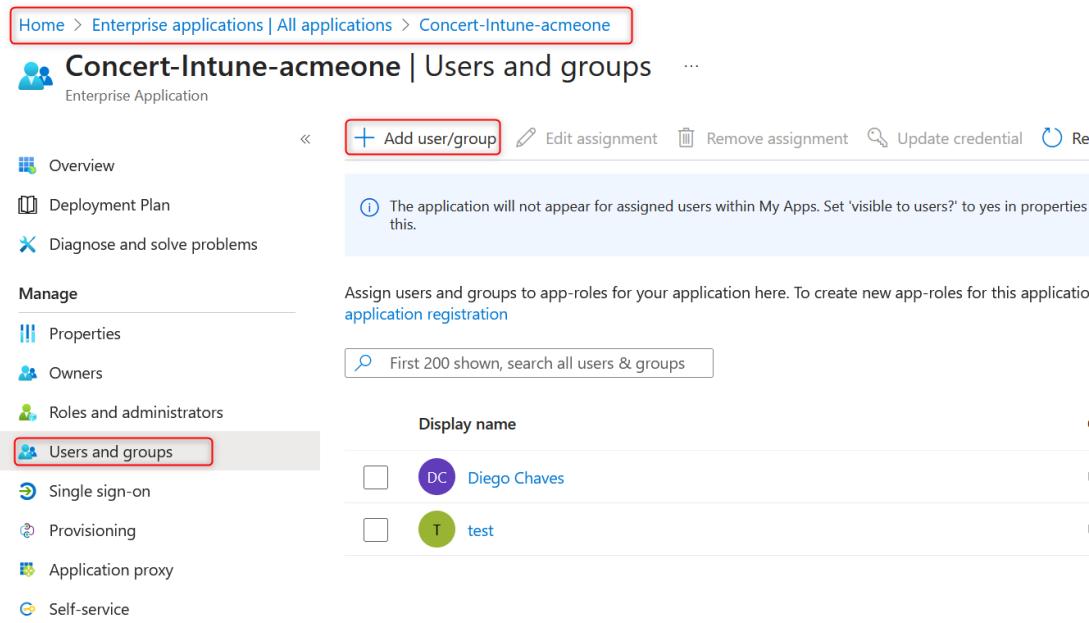
Enterprise applications > All applications > Select your Intune app > Users and groups

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

Overview Deployment Plan Diagnose and solve problems

Add user/group Edit assignment Remove assignment Update credential Re

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 registration

First 200 shown, search all users & groups

Display name

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

Manage

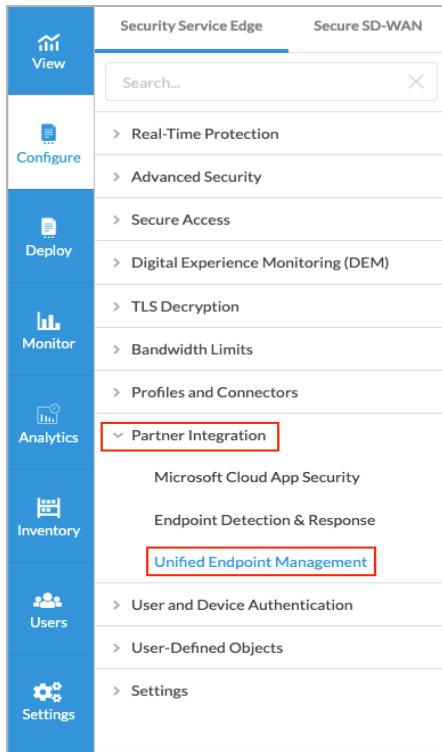
- Properties
- Owners
- Roles and administrators
- Users and groups**
- Single sign-on
- Provisioning
- Application proxy
- Self-service

Configuration in Concerto

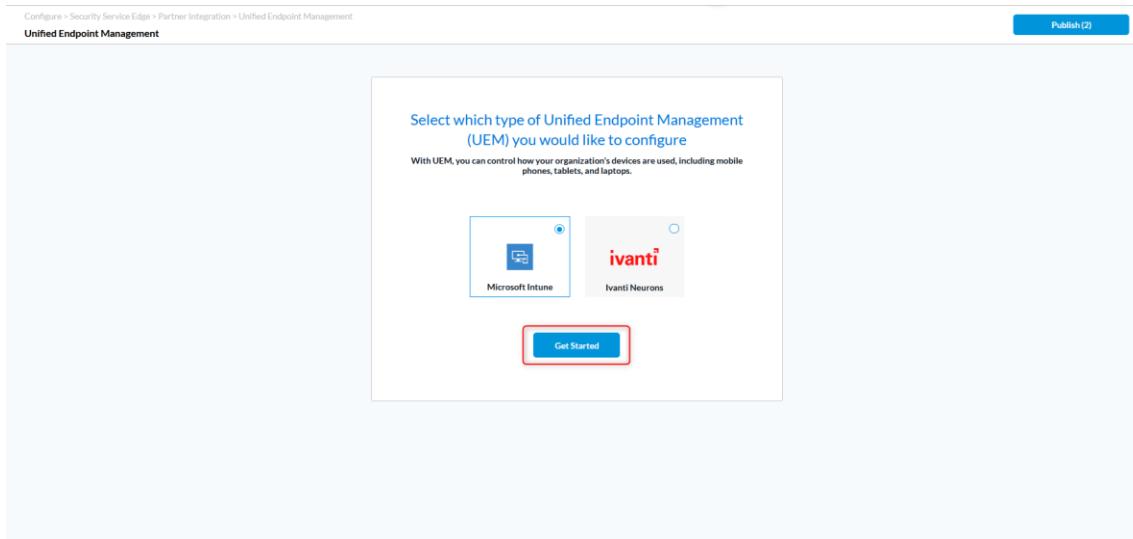
Integration with Accessing Unified Endpoint Management

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

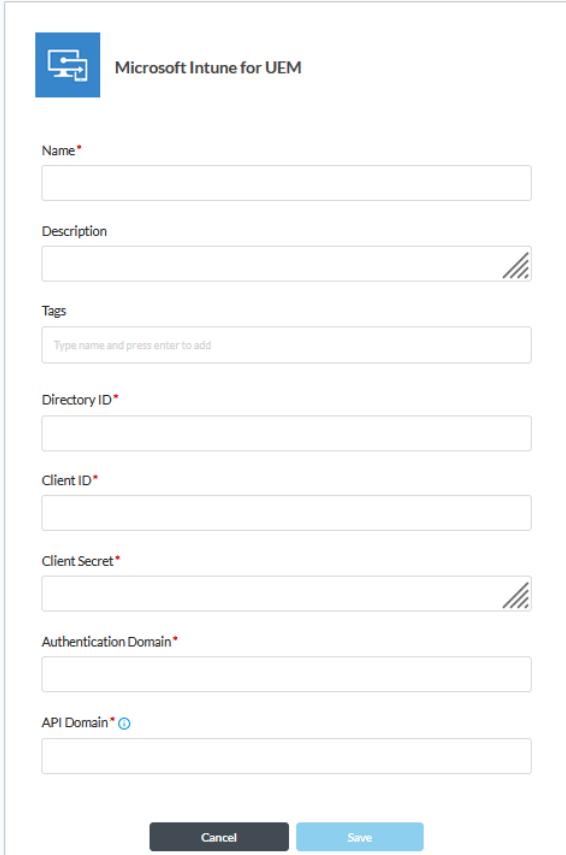
Configure > Security Service Edge (SSE) > Partner Integration > Unified Endpoint Management



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

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.

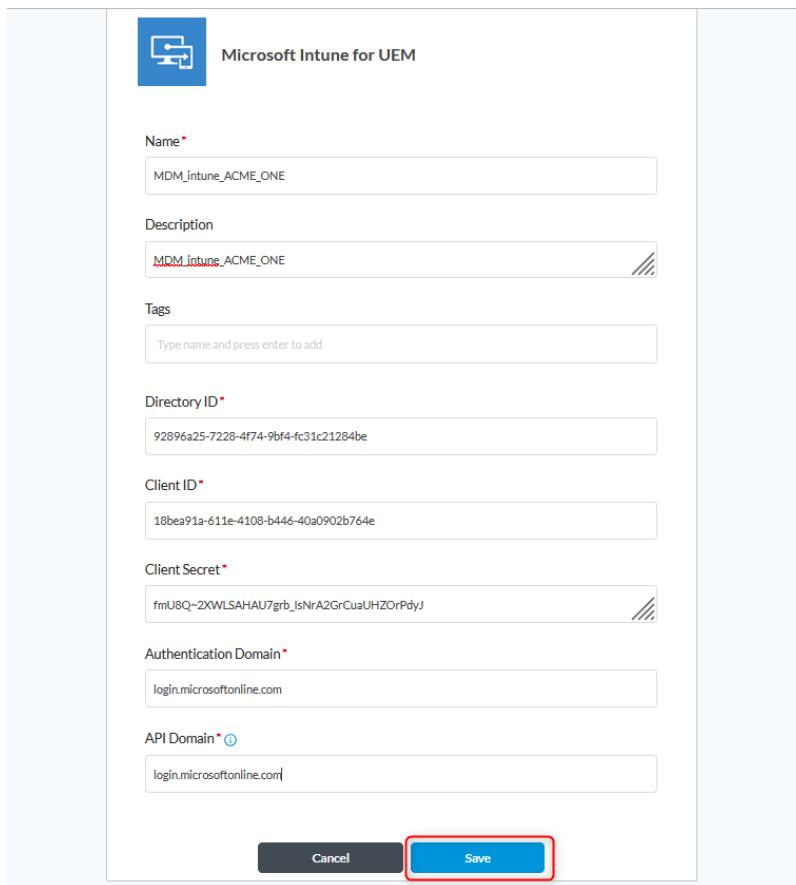
Client Secret (Required)	Enter the client secret provided by the graph (Intune) server, in string format.
Authentication Domain (Required)	Enter the domain name to use for authentication. login.microsoftonline.com
API Domain (Required)	Enter the domain name to use for APIs. graph.microsoft.com

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*
MDM_intune_ACME_ONE

Description
MDM_intune_ACME_ONE

Tags
Type name and press enter to add

Directory ID*
92896a25-7228-4f74-9bf4-fc31c21284be

Client ID*
18bea91a-611e-4108-b446-40a0902b764e

Client Secret*
fmU8Q>2XWLSAHU7grb_JsNrA2GrCuaUHZOrPdyJ

Authentication Domain*
login.microsoftonline.com

API Domain*
login.microsoftonline.com

Cancel Save

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
Example: test devices (one with Firewall disabled > non-compliant)	Open in Edge or Chrome: Paste <code>ms-device-enrollment?:model=aadj</code> Or Go to Settings > Accounts > Access work or school then Connect	Enter email + password. Select Join > click Done .	Reboot PC. Select Other user → sign in with same enrollment credentials.	Check that the Intune MDM certificate is present in the Computer certificate store.

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.

Microsoft Intune admin center

Home > Devices | Windows > Windows

Windows | Compliance

Create policy

Windows devices

Policy name: Windows_Setting, Platform or OS: Windows 10 and later, Policy type: Windows 10/11 compliance p..., Last modified: 09/10/2025

Policy name	Platform or OS	Policy type	Last modified
Windows_Setting	Windows 10 and later	Windows 10/11 compliance p...	09/10/2025,

Compliance

Scripts and remediations

Group Policy analytics

eSIM cellular profiles (preview)

Manage updates

Windows updates

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.

Home > Devices | Windows > Windows | Compliance >

Windows_Setting

Compliance policy - Windows 10 and later

Properties

Basics

Name: Windows_Setting, Description: --, Platform: Windows 10 and later, Profile type: Windows 10/11 compliance policy

Compliance settings

System Security

Firewall: Required

Actions for noncompliance

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

Scope tags

Default

Assignments

Included groups

Group	Filter	Filter mode
All Users	None	None

Excluded groups

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.

The screenshot shows the 'Properties' tab of a compliance policy named 'Windows_Setting'. The 'Basics' section includes fields for Name (Windows_Setting), Description (empty), Platform (Windows 10 and later), and Profile type (Windows 10/11 compliance policy). The 'Compliance settings' section contains a 'System Security' rule for 'Firewall' set to 'Required'. The 'Actions for noncompliance' section shows an action for 'Mark device noncompliant' with 'Schedule' set to 'Immediately' and 'Additional recipients (via email)' set to 'None selected'. The 'Scope tags' section shows a 'Default' tag. The 'Assignments' section shows the policy is assigned to 'All Users'. The 'Included groups' section shows 'All Users' is selected. The 'Excluded groups' section is empty.

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

Get access to resources like email, apps, and the network. Your work or school might control some things on this device when connected.

Add a work or school account Connect

Connected by test@acmeonelab.onmicrosoft.com
Connected to ACME-ONE's Entra ID

Related settings

- Export your management log files Export
- Create a test-taking account
- Add or remove a provisioning package

Related support

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.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
162fc8e5-9b5d-443d-8462-5d0540df688f	Microsoft Intune MDM Device CA	8/23/2023	Client Authentication	<None>
80fa1de5-1551-4939-98a3-eb914b8e77ac	MS-Organization-P2P-Access [20...	8/26/2022	Server Authentication	<None>
80fa1de5-1551-4939-98a3-eb914b8e77ac	MS-Organization-Access	8/23/2032	Client Authentication	<None>
localhost	Versa Networks Localhost CA	7/23/2032	Server Authentication	<None>
	Windows Azure CRP Certificate Generator	8/19/2023	<All>	TenantEncryption

3. confirm Windows device has synchronized on Intune

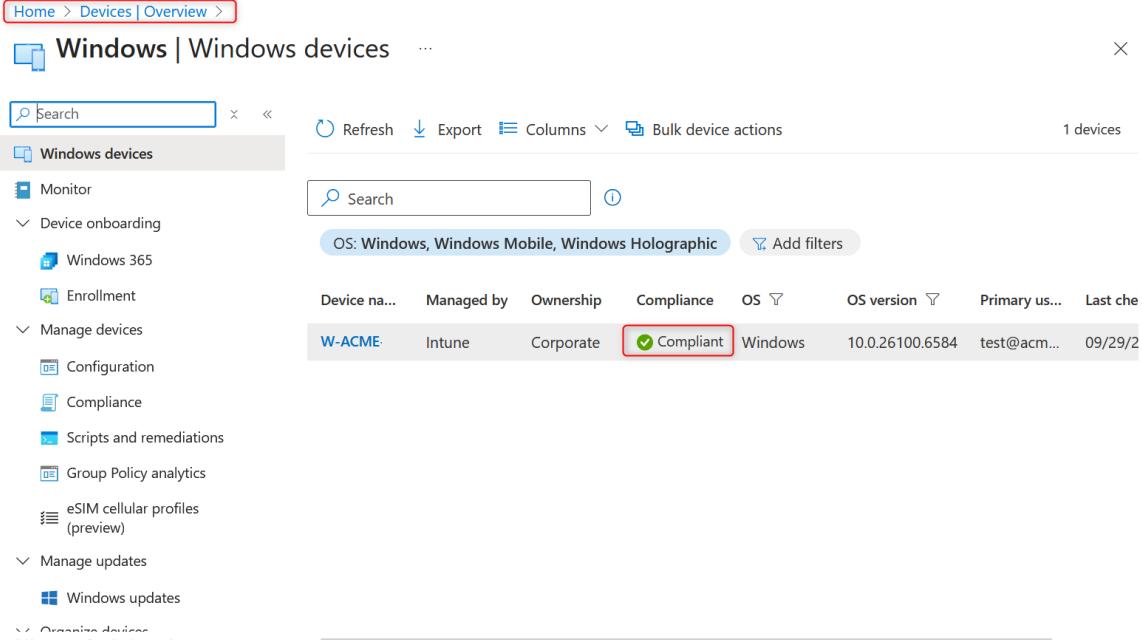
To confirm that your enrolled Windows device has synchronized with Intune and is reporting its compliance posture, check the device list inside the **Microsoft Intune admin center**.

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's 'Devices | Overview' section for Windows devices. The left sidebar lists categories like 'Monitor', 'Device onboarding', 'Enrollment', 'Manage devices', and 'Manage updates'. The main area displays a table with columns: Device name, Managed by, Ownership, Compliance, OS, OS version, Primary user, and Last checked. A device named 'W-ACME' is listed, and the 'Compliance' column for this device is highlighted with a red box, showing the status as 'Compliant'. The table also shows the OS as Windows, OS version as 10.0.26100.6584, Primary user as test@acm..., and Last checked as 09/29/22.

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.

ACME-ONE | CONFIGURATION | America/Bogota | English | 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
Secure_Access_Windows_Profile_LDAP_Users_Certificate	Windows Windows 10 Windows 10 Mobile Windows 11	AD Server_Acme_One Users Diego Chaves diego-lab@diegolab-versa.net VIP1.vip1@acme-one.com	Endpoint Information Profile (EIP) User Defined EIP_Profile_Windows_Registry 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 SaseGWDiegos-lab	Enabled 11/21/2025, 11:53:34 AM Administrator
Secure_Access_Windows_Profile	Windows Windows 10 Windows 10 Mobile Windows 11	ENTRA-ID-SAML Users vip2@diegolabvers.a.onmicrosoft.com vip3@diegolabvers.a.onmicrosoft.com vip4@diegolabvers.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 SaseGWDiegos-lab	Enabled 11/21/2025, 11:53:34 AM Administrator
Secure_Access_Windows_MDM	Windows Windows 10 Windows 10 Mobile Windows 11	AD Server_Acme_One Users Diego Chaves diego-lab@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 SaseGWDiegos-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 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

Match Criteria

Action

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	Apple	Android	Linux
<input type="checkbox"/> All Windows Operating Systems <input type="checkbox"/> User Defined <input type="checkbox"/> Oper-1 <input type="checkbox"/> testGoWindows <input type="checkbox"/> test-yn-ok <input type="checkbox"/> test-yn-pa <input type="checkbox"/> Predefined <input type="checkbox"/> Windows 10 <input type="checkbox"/> Windows 10 Mobile <input type="checkbox"/> Windows 11 <input type="checkbox"/> Windows 7 <input type="checkbox"/> Windows 8 <input type="checkbox"/> Windows 8.1 <input type="checkbox"/> Windows Server 2012	<input type="checkbox"/> All Apple Operating Systems <input type="checkbox"/> User Defined <input type="checkbox"/> testGo <input type="checkbox"/> Predefined <input type="checkbox"/> Mac OS X Server <input type="checkbox"/> Mac OS <input type="checkbox"/> All Apple Mobile <input type="checkbox"/> User Defined <input type="checkbox"/> testGoPad <input type="checkbox"/> Predefined <input type="checkbox"/> iOS <input type="checkbox"/> iPadOS	<input type="checkbox"/> All Android Operating Systems <input type="checkbox"/> User Defined <input type="checkbox"/> testGoAndroid <input type="checkbox"/> testGoAndroid01 <input type="checkbox"/> Predefined <input type="checkbox"/> Android	<input type="checkbox"/> All Linux Operating Systems <input type="checkbox"/> User Defined <input type="checkbox"/> testGoLinux <input type="checkbox"/> testGoNew <input type="checkbox"/> Predefined <input type="checkbox"/> Fedora <input type="checkbox"/> Linux <input type="checkbox"/> Red Hat Enterprise Linux <input type="checkbox"/> 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



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 (2)

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



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.

73.106.17/app/ACME-ONE/config/sase/secure-access-client/rule#

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.

```
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><autopreregister>autopreregister</autopreregister><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-b446-40a0902b764&scope=https://graph.microsoft.com/.default&client_secret=fmU80~2XWLSAHU7grb_IsNrA2GrCuaUHZOrPdyJ&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
```

- 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.

```
2025-09-29 20:28:52.511 DEBUG [0x101] mdm_access_token_cb:1252 resp_len = 3483
2025-09-29 20:28:52.511 DEBUG [0x101] mdm_access_token_cb:1254 response = HTTP/1.1 200 OK
Cache-Control: no-store, no-cache
Pragma: no-cache
Content-Type: application/json; charset=utf-8
Expires: -1
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff
P3P: CP="DSP CUR OTPi IND OTRi ONL FIN"
x-ms-request-id: dcb366bc-0397-481d-b798-529df751e500
x-ms-ests-server: 2.1.21950.4 - WUS3 ProdSlices
x-ms-srs: 1.0
Content-Security-Policy-Report-Only: object-src 'none'; base-uri 'self'; script-src 'self' 'nonce-jleJelQuYWHwpZNq7S0RCg' 'unsafe-inline' 'unsafe-eval' https://*.msauth.net https://*.msftauth.net https://*.msauthimages.net https://*.msidentity.net https://*.microsftonline-p.com https://*.microsftazureread-sso.com https://*.azuredge.net https://*.outlook.com https://*.office.com https://*.office365.com https://*.microsoft.com https://*.bing.com 'report-sample'; report-uri https://csp.microsoft.com/report/ESTS-UX-A1
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop-endpoint"
Reporting-Endpoints: coop-endpoint="https://idux.azurewebsites.net/api/coopReport"
X-XSS-Protection: 0
Set-Cookie: fpc=AKHDfbh5qJxPihs4HQDxgAFBgf0HAQAAAATjb0AOAAAAA; expires=Wed, 29-Oct-2025 20:28:52 GMT; path=/; secure; HttpOnly; SameSite=None
Set-Cookie: x-ms-gateway-slice=estsfd; path=/; secure; httponly
Set-Cookie: stsservicecookie=estsfd; path=/; secure; httponly
Date: Mon, 29 Sep 2025 20:28:52 GMT
Content-Length: 2028

{"token_type": "Bearer", "expires_in": 3599, "ext_expires_in": 3599, "access_token": "eyJ0eXAiOiJKV1QiLCJub25jZSI6IkJORuctTxMeHhdmZTRzNuUkJYY1hDlm9x0WEwVJGx1BqeG1WLWhMYKEiLCJhbGciOiJSUzI1NiIsIng1dCI6IkTMjNiN0RvN1RjYVUxUm9MSHdwSXEyNFZZZyIsImtpZCI6IkTMjNiN0RvN1RjYVUxUm9MSHdwSXEyNFZZZyJ9.eyJhdWQiOiJodHRwczovL2dyYXB0LmipY3Jvc29mdC5jb20tLCJpc3M0iijodhRwczovL3N0cy53aW5kb3dzLm8ldC85Mjg5NmFvNS03MiT4lTRmNz0t0WJmNC1mYzMyzTxMiaWE0TioxNzU5MTc3NDMvLCJuYmYiOjE3NTkxNzc0MzTsTmV4cCT6MTc10TE4MTMzMiwiYVlwTioi"}
```

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*)

```

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":"BY3PEPF000799EF"}}
OData-Version: 4.0
Date: Mon, 29 Sep 2025 20:28:51 GMT
7BD
{"@odata.context": "https://graph.microsoft.com/v1.0/$metadata#deviceManagement/managedDevices/$entity", "id": "5d7d35de-53c9-4358-ae39-6d9d8866254", "userId": "47990e2c-d1e9-40a4-a132-4b2ec4785417", "deviceName": "W-ACME-ONE-MDM", "managedDeviceOwnerType": "company", "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": "10.0.26100.6584", "easActivated": false, "easDeviceId": null, "activationLockBypassCode": null, "emailAddress": "test@acmeone.lab.onmicrosoft.com", "azureADDeviceId": "70d25038-8193-4b52-8b52-7a394482108b", "deviceRegistrationState": "registered", "deviceCategoryDisplayName": "", "isSupervised": false, "exchangeLastSuccessfulSyncDateTime": "2000-01-01T00:00:00Z", "exchangeAccessState": "none", "exchangeAccessStateReason": "none", "remoteAssistanceSessionUrl": "", "remoteAssistanceSessionErrorDetails": "", "isEncrypted": true, "userPrincipalName": "test@acmeone.lab.onmicrosoft.com", "model": "Standard PC (Q35 + ICH9, 2009)", "manufacturer": "QEMU", "imei": null, "complianceGracePeriodExpirationDateTime": "1999-12-31T23:59:59.9999999Z", "serialNumber": null, "phoneNumber": null, "androidSecurityPatchLevel": null, "userDisplayName": "test", "configurationManagerClientEnabledFeatures": null, "wiFiMacAddress": null, "deviceHealthAttentionState": null, "subscriberCarrier": "", "meid": null, "totalStorageSpaceInBytes": 160171032576, "freeStorageSpaceInBytes": 110230503424, "managedDeviceName": "test_Windows_9/10/2025_9:12 PM", "partnerReportedThreatState": "Unknown", "requireUserEnrollmentApproval": null, "managementCertificateExpirationDate": "2026-05-05T00:00:00Z", "iccId": "", "udid": "", "notes": null, "ethernetMacAddress": "B2C41A9E3D0", "physicalMemoryInBytes": 0, "enrollmentProfileName": "", "deviceActionResults": []}
sIVzZXiUmvhZC5BbGwiLCJEZXpY2VNY5h2ZVtZw50Q29uZmlndJhdGtvb155ZWFkLkfbsCJdLCJzdWI0i22mY1YmVmNs02YjM3LTrkZjItYTY5My0yNzFimGExNmYm5hZCJ0Zw5hbnRfcmVnaW9uX3Njb38Lljo10E1lCJ0aWQ10i15Mjg5NmeWfJNz03mj14LTrmNz0t0WJmC1mYzMyxzIxMjg0yMnU1lCJ1dGk10iJ2R2F6M0pjREhVaTNtRktkOTF1bEFBIwldmwyIjoiMS4bIwld2lkycIG6wyIwOTk3YTFkMC0wZDFkLTrhY2ItYj0wOC1kNWhhNzMxMjF1lOTA1xSwief1zX2Z0ZCI6InBXN0x2wEMwTJqV1VUaExkUGYxcFF0aEhtWFg3eUJVT1B2aVg2M29rbzhCZfH0M1pYTjBnleTfRyZIxeiisInhtc19pZHJlbCI6IjcgMza1lCJ4bXNfc0i0iIwLj0yTGPZQkpPzXm4a0pNTJMaVRndG9UbjRKSTFU1dyan6egWUHdkVrBeZ0SVLcVjNux3VYt1y131zgtN2VrMnytZf9NzVVKUkRTSUnaQVFJ1FHaEtLCJ4bXNfdGKkdC16MTC1Nz1M0Tlx0X0.QyrdjKTAC55PSB1duk98eSn5FPM63nE8y1by7XdoMjyQ1iwy9CRBlhUnP5y7hLq0bqQusb9uuk9kwRt803pMaikDnkdidC8cT0UbZCVsuxdKzb0PLua50wYrmpnEfW62C9GV1Y2CX871kXUzSxyupGkDX1efHllUxDo9yTmBqg3eh21Ncb6ZdwSBPsB3bZZSpEYQ0qmjP24C8816x0pqueun6y9qnnXxKp-jn0ELJFxpHqz6WTUpyl6Ht8XgwUbu16MrRkvW6b7ttK7Trov1wzIoh7HAKknR32HJx0mYiVrxZ70YmdhLxe6YKgb06qRd2IPxmy82jdNEAIA"} end_flow = 0
2025-09-29 20:28:52.970 DEBUG [0x101] mdm_parse_cloud_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 saccess session history all br
- show saccess session history all br | grep <<user>>
- show saccess session history id <<no>>

MACOS Enrollment

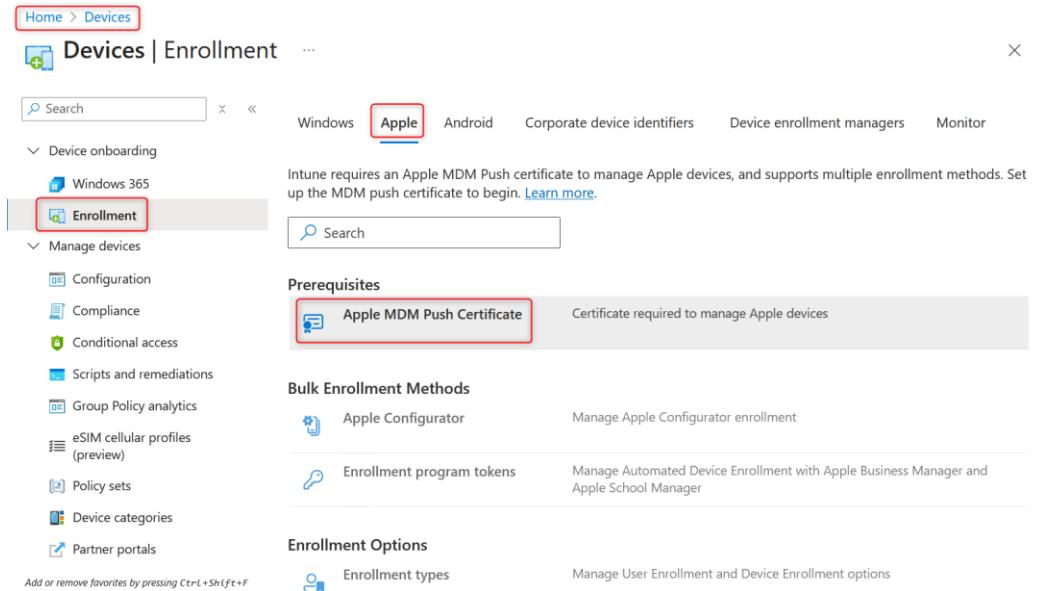
This walkthrough shows how to enroll a macOS device in Microsoft Intune and how its compliance state appears in VOS. It validates that the Intune integration behaves consistently across operating systems.

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



The screenshot shows the Microsoft Intune Admin Center interface. The top navigation bar includes 'Home > Devices', a search bar, and tabs for Windows, Apple (which is selected and highlighted with a red box), Android, Corporate device identifiers, Device enrollment managers, and Monitor. The left sidebar has sections for Device onboarding, Windows 365, Enrollment (which is highlighted with a red box), Manage devices, Configuration, Compliance, Conditional access, Scripts and remediations, Group Policy analytics, eSIM cellular profiles (preview), Policy sets, Device categories, and Partner portals. The main content area has a 'Prerequisites' section with a box around 'Apple MDM Push Certificate' and a note: 'Intune requires an Apple MDM Push certificate to manage Apple devices, and supports multiple enrollment methods. Set up the MDM push certificate to begin. [Learn more](#)'. Below this are 'Bulk Enrollment Methods' (Apple Configurator, Enrollment program tokens) and 'Enrollment Options' (Enrollment types). A note at the bottom says 'Add or remove favorites by pressing Ctrl+Shift+F'.

- 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

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

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

Steps:

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

Add or remove favorites by pressing **Ctrl+L**.

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	<input type="button" value="Revoke"/> <input type="button" value="Download"/> <input type="button" value="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.

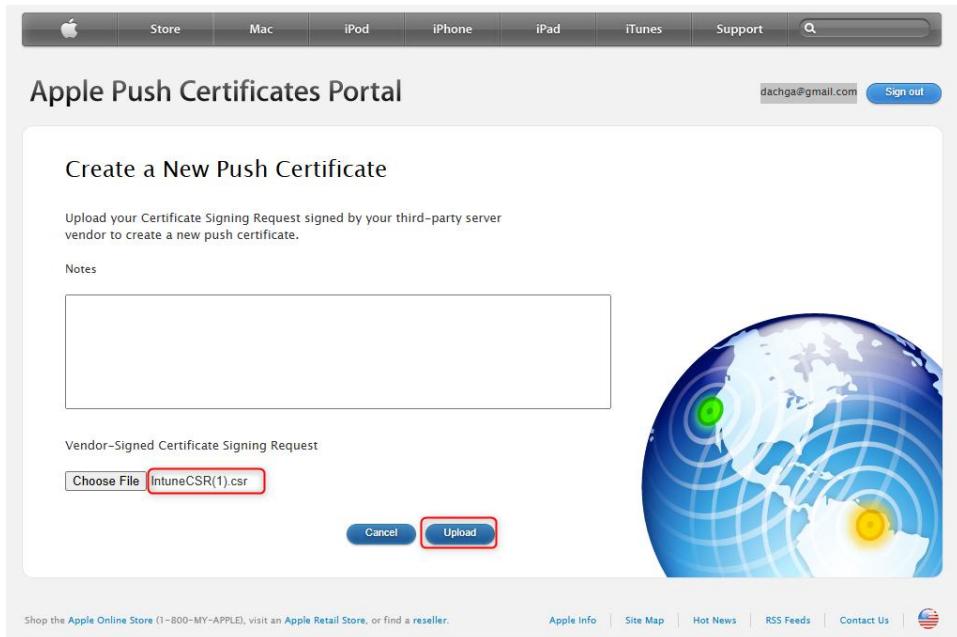
MDM push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificate Portal. Learn more about MDM push certificate migration.

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. Copyright © 2021 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

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

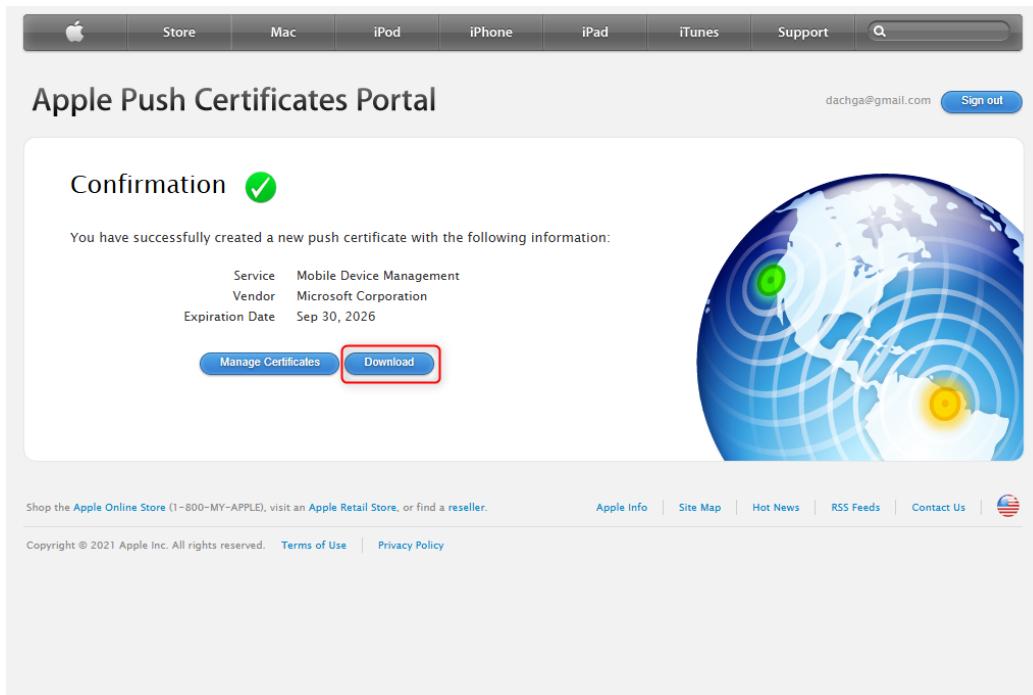
Choose File **IntuneCSR(1).csr**

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

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.

The screenshot shows the Microsoft Intune Admin Center interface. On the left, the navigation menu is visible with several sections like Device onboarding, Windows 365, Enrollment, Manage devices, Configuration, Compliance, and others. The 'Enrollment' section is highlighted with a red box and a red number '2'. The 'Apple' section is also highlighted with a red box and a red number '3'. Under the 'Apple' section, the 'Apple MDM Push Certificate' link is highlighted with a red box and a red number '4'. On the right, a 'Configure MDM Push Certificate' dialog box is open. Step 5 is shown with a checked 'I agree.' checkbox. Step 6 shows the 'Apple ID' field with 'dachga@gmail.com' entered. Step 7 shows the 'Apple MDM push certificate' field with the file path 'MDM_Microsoft Corporation_Certificate (2).pem' entered.

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).



Company Portal

Get access to work or school resources and keep them secure.

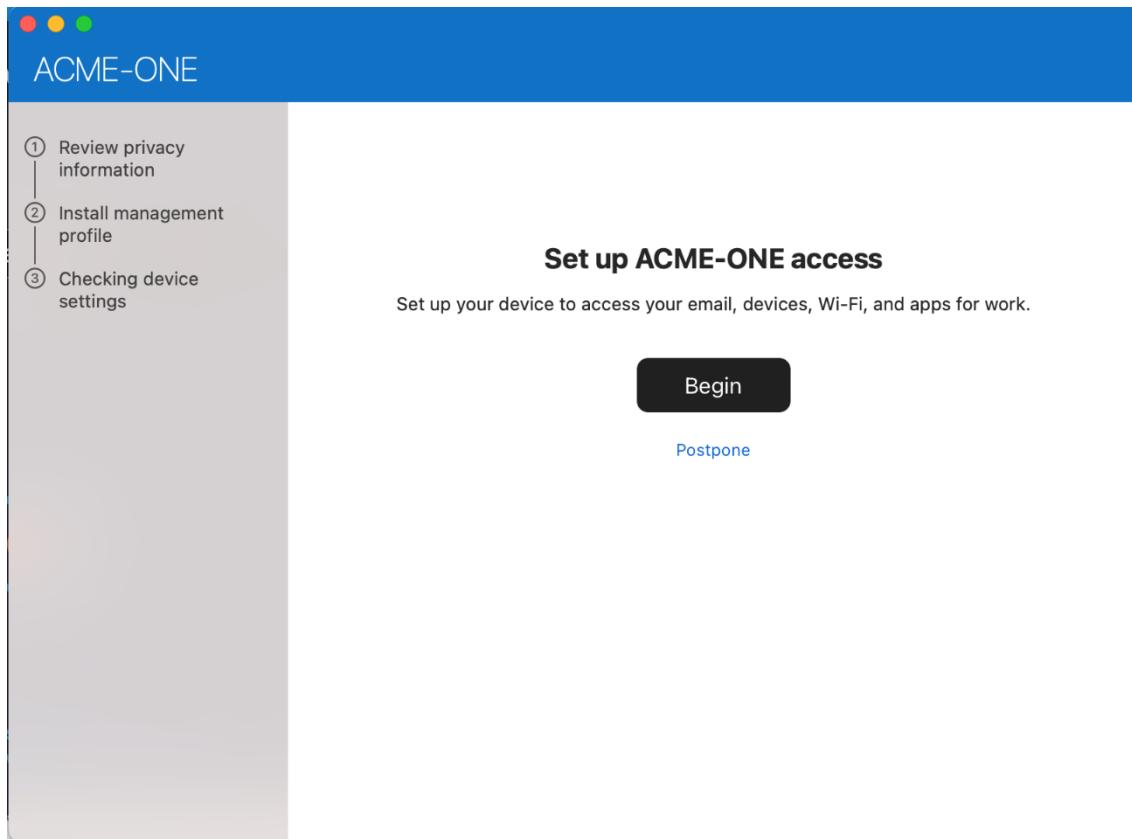
Sign in

[Microsoft privacy & cookies](#)

Consistent with Microsoft and Apple policy, we do not sell any data collected by our service to any third parties for any reason.

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.

ACME-ONE

① Review privacy information
② Install management profile
③ Checking device settings

What can ACME-ONE see?

Your organization can't:

- View browsing history on this device
- Open your emails, contacts, or calendar
- Access your passwords
- Review your documents

Your organization can:

- View the model, serial number, and operating system
- See the names of apps you've installed
- Identify your device by name
- Reset lost or stolen device to factory settings

[Learn more](#)

[Back](#) [Continue](#)

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

ACME-ONE

① Review privacy information
② **Install management profile**
③ Checking device settings

Install management profile

- Download profile**
- Select **Install** and follow the on-screen instructions to complete the installation.
- Come back to **Company Portal**.

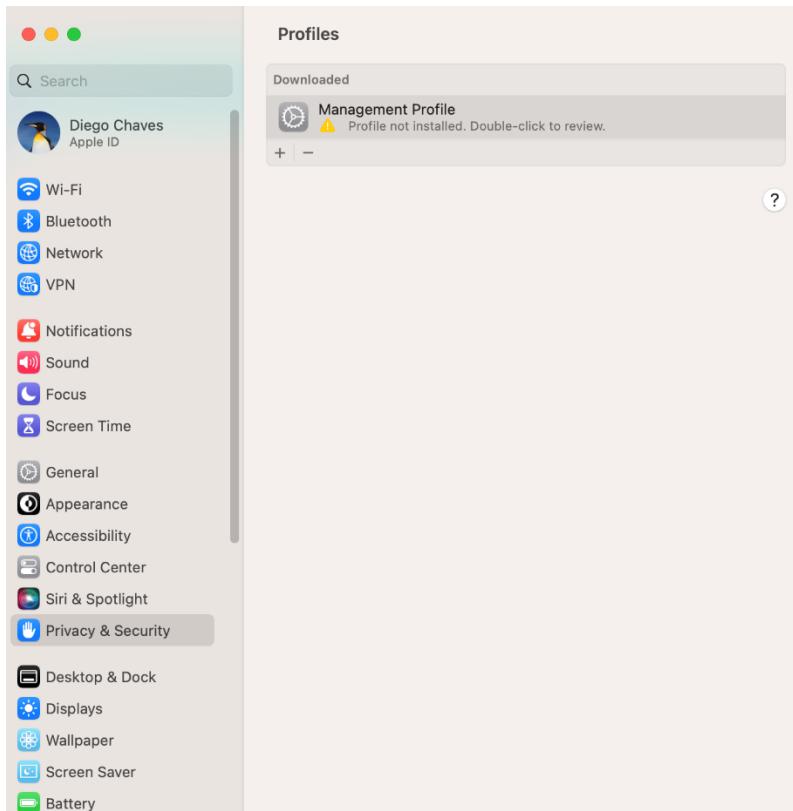
[Learn more](#)

[Back](#)

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.

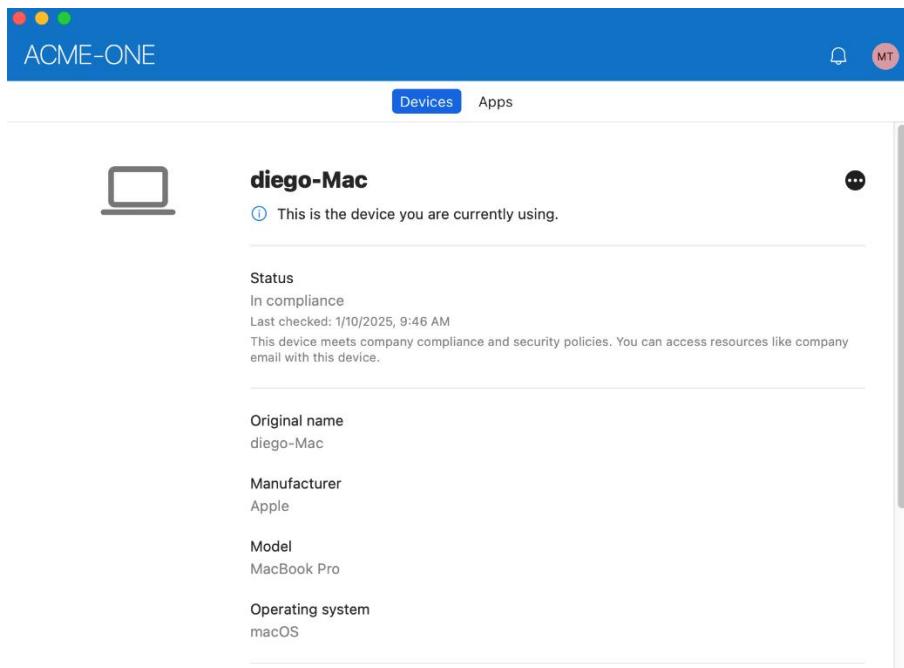
Once the profile installation is complete, **return to the Company Portal** to continue the enrollment process.

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.

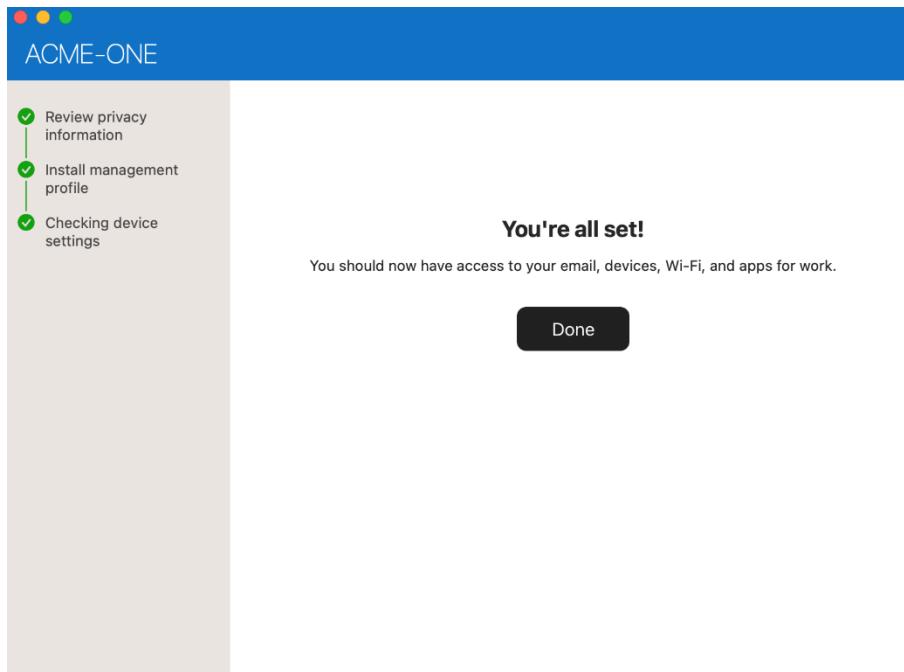
Note

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..



The screenshot shows the Microsoft Endpoint Manager portal. At the top, there are three colored dots (red, yellow, green) and the text 'ACME-ONE'. On the right, there are icons for a bell and 'MT'. Below the header, there are tabs for 'Devices' (which is selected) and 'Apps'. The main content area shows a device card for 'diego-Mac'. The card includes a small icon of a Mac, the device name 'diego-Mac', and a note: 'This is the device you are currently using.' Below this, there is a 'Status' section with the following details: 'In compliance', 'Last checked: 1/10/2025, 9:46 AM', and a note: 'This device meets company compliance and security policies. You can access resources like company email with this device.' Further down, there are sections for 'Original name' (diego-Mac), 'Manufacturer' (Apple), 'Model' (MacBook Pro), and 'Operating system' (macOS).

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



The screenshot shows the Microsoft Endpoint Manager portal after setup completion. At the top, there are three colored dots (red, yellow, green) and the text 'ACME-ONE'. On the left, there is a sidebar with three checked items: 'Review privacy information', 'Install management profile', and 'Checking device settings'. The main content area has a heading 'You're all set!' and the text 'You should now have access to your email, devices, Wi-Fi, and apps for work.' Below this is a 'Done' button.

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

Device name	Managed by	Ownership	Compliance	OS	OS version	Primary use...	Last check-in
diego-Mac	Intune	Personal	Compliant	macOS	13.7.8 (22H730)	mac-test@...	10/01/2025, 10:...

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.

ACME-ONE | CONFIGURATION | America/Bogota | English | 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
Secure_Access_Windows_Profile_LDAP_Users_Certificate	Windows Windows 10 Windows 10 Mobile Windows 11	AD Server_Acme_One Users Diego Chaves diego.labj@diegolab-versanet VIP1.vip1@acme-one.com	Endpoint Information Profile (EIP) User Defined EIP_Profile_Windows_Registry 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 SaseGWDiegos-lab	Enabled 11/21/2025, 11:53:34 AM Administrator
Secure_Access_Windows_Profile	Windows Windows 10 Windows 10 Mobile Windows 11	ENTRA-ID-SAML Users vip2@diegolabvers.a.onmicrosoft.com vip3@diegolabvers.a.onmicrosoft.com vip4@diegolabvers.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 SaseGWDiegos-lab	Enabled 11/21/2025, 11:53:34 AM Administrator
Secure_Access_Windows_MDM	Windows Windows 10 Windows 10 Mobile Windows 11	AD Server_Acme_One Users Diego Chaves diego.labj@diegolab-versanet	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	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 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

Match Criteria | Action

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	Apple	Android	Linux
<input type="checkbox"/> All Windows Operating Systems <input type="checkbox"/> User Defined <input type="checkbox"/> Oper-1 <input type="checkbox"/> testGovWindows <input type="checkbox"/> test-yn-ok <input type="checkbox"/> test-yn-pa <input type="checkbox"/> Predefined <input type="checkbox"/> Windows 10 <input type="checkbox"/> Windows 10 Mobile <input type="checkbox"/> Windows 11 <input type="checkbox"/> Windows 7 <input type="checkbox"/> Windows 8 <input type="checkbox"/> Windows 8.1 <input type="checkbox"/> Windows Server 2012	<input type="checkbox"/> All Apple Operating Systems <input type="checkbox"/> User Defined <input type="checkbox"/> testGo <input type="checkbox"/> Predefined <input type="checkbox"/> Mac OS X Server <input type="checkbox"/> OS X <input type="checkbox"/> Mac OS <input type="checkbox"/> All Apple Mobile <input type="checkbox"/> User Defined <input type="checkbox"/> testGoPad <input type="checkbox"/> Predefined <input type="checkbox"/> iOS <input type="checkbox"/> iPadOS	<input type="checkbox"/> All Android Operating Systems <input type="checkbox"/> User Defined <input type="checkbox"/> testGoAndroid <input type="checkbox"/> testGoAndroid01 <input type="checkbox"/> Predefined <input type="checkbox"/> Android	<input type="checkbox"/> All Linux Operating Systems <input type="checkbox"/> User Defined <input type="checkbox"/> testGoLinux <input type="checkbox"/> testGoNew <input type="checkbox"/> Predefined <input type="checkbox"/> Fedora <input type="checkbox"/> Linux <input type="checkbox"/> Red Hat Enterprise Linux <input type="checkbox"/> 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

Match Criteria

Action

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 

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

Match Criteria

Action

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.

Device Compliance Status

← Back

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.

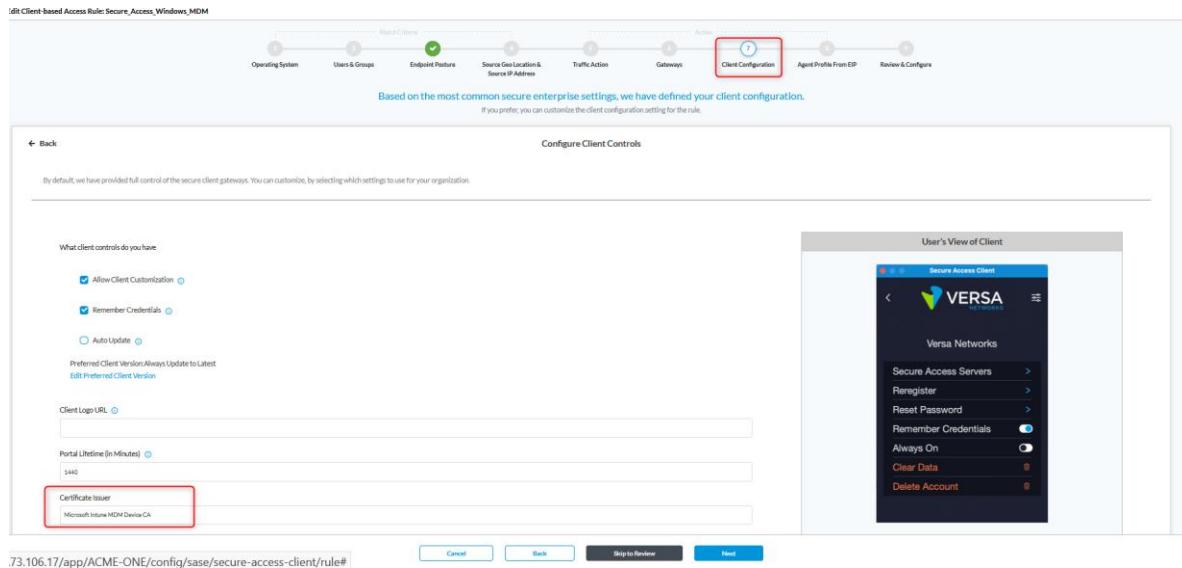
Client Configuration

- 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.



Client-based Access Rule: Secure_Access_Windows_MDM

Based on the most common secure enterprise settings, we have defined your client configuration.

Configure Client Controls

What client controls do you like?

- Allow Client Customization
- Remember Credentials
- Auto Update

Preferred Client Version: Always Update to Latest

Client Logo URL:

Portal Lifetime (in Minutes):

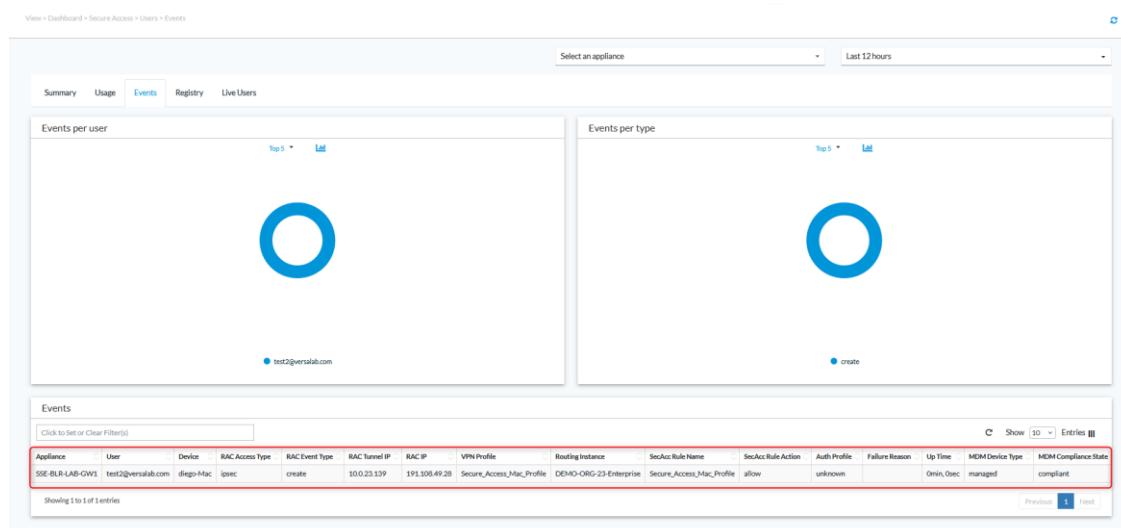
Certificate Issuer: Microsoft Intune MDM Device CA

73.106.17/app/ACME-ONE/config/sase/secure-access-client/rule#

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.



View > Dashboard > Secure Access > Users > Events

Summary Usage Events Registry Live Users

Events per user

Events per type

Events

Click to Set or Clear Filter(s)

Appliance	User	Device	RAC Access Type	RAC Event Type	RAC Tunneled IP	RAC IP	VPN Profile	Routing Instance	SecAcc Rule Name	SecAcc Rule Action	Auth Profile	Failure Reason	Up Time	MDM Device Type	MDM Compliance State
SSE-BLR-LAB-GW1	test2@versalab.com	diego-Mac	ipsec	create	10.0.23.139	191.100.49.20	Secure_Access_Mac_Profile	DEMO-ORG-23-Enterprise	Secure_Access_Mac_Profile	allow	unknown	0min,0sec	managed	compliant	

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](#).