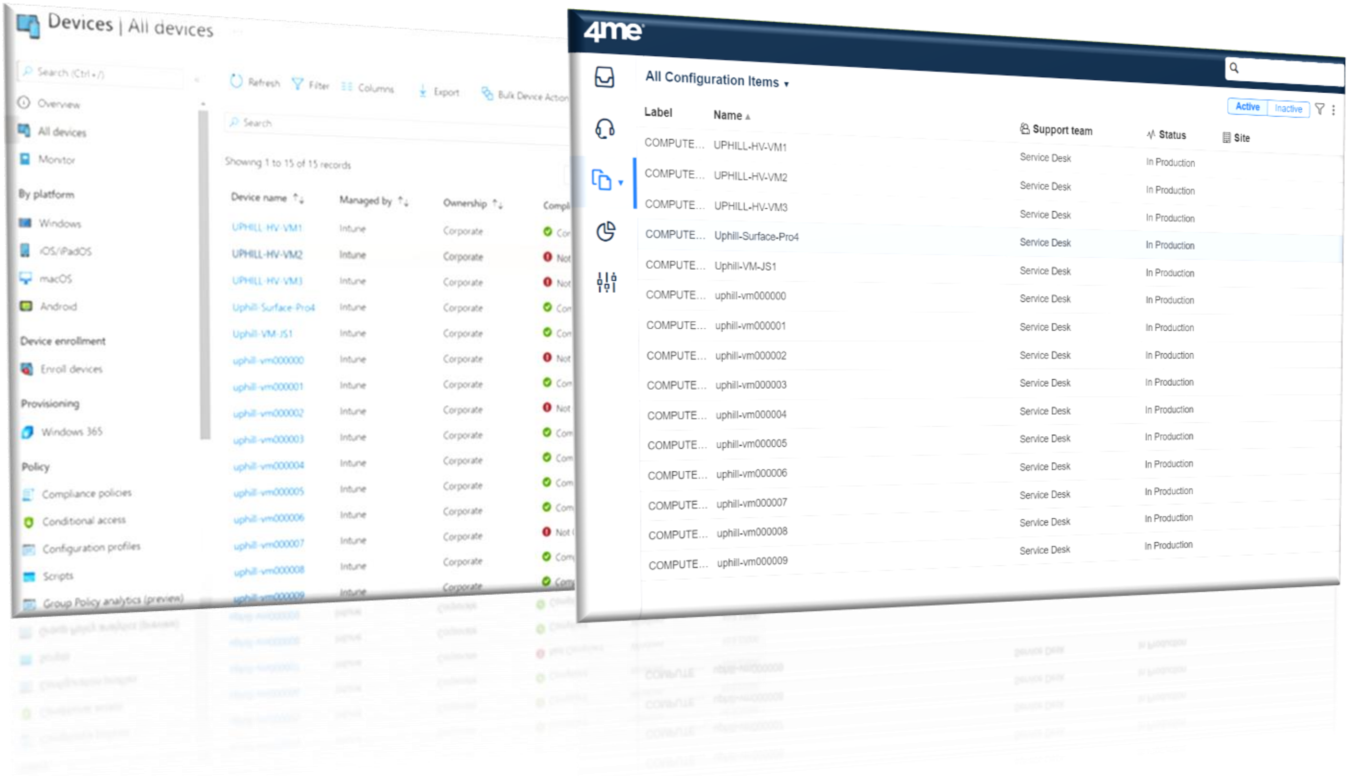
Microsoft Intune connector for 4me

Implementation Whitepaper

Version 1.1



Devices | All devices

Showing 1 to 15 of 15 records

Device name ↑↓	Managed by ↑↓	Ownership ↑↓	Compl
UPHILL-HV-VM1	Intune	Corporate	✓ Cor
UPHILL-HV-VM2	Intune	Corporate	❗ Not
UPHILL-HV-VM3	Intune	Corporate	❗ Not
Uphill-Surface-Pro4	Intune	Corporate	✓ Con
Uphill-VM-JS1	Intune	Corporate	✓ Con
uphill-vm000000	Intune	Corporate	❗ Not
uphill-vm000001	Intune	Corporate	✓ Com
uphill-vm000002	Intune	Corporate	❗ Not
uphill-vm000003	Intune	Corporate	✓ Com
uphill-vm000004	Intune	Corporate	✓ Com
uphill-vm000005	Intune	Corporate	✓ Com
uphill-vm000006	Intune	Corporate	✓ Com
uphill-vm000007	Intune	Corporate	❗ Not (
uphill-vm000008	Intune	Corporate	✓ Com
uphill-vm000009	Intune	Corporate	✓ Com

All Configuration Items ▾

Label	Name ▴	Support team	Status	Site
COMPUTE...	UPHILL-HV-VM1	Service Desk	In Production	
COMPUTE...	UPHILL-HV-VM2	Service Desk	In Production	
COMPUTE...	UPHILL-HV-VM3	Service Desk	In Production	
COMPUTE...	Uphill-Surface-Pro4	Service Desk	In Production	
COMPUTE...	Uphill-VM-JS1	Service Desk	In Production	
COMPUTE...	uphill-vm000000	Service Desk	In Production	
COMPUTE...	uphill-vm000001	Service Desk	In Production	
COMPUTE...	uphill-vm000002	Service Desk	In Production	
COMPUTE...	uphill-vm000003	Service Desk	In Production	
COMPUTE...	uphill-vm000004	Service Desk	In Production	
COMPUTE...	uphill-vm000005	Service Desk	In Production	
COMPUTE...	uphill-vm000006	Service Desk	In Production	
COMPUTE...	uphill-vm000007	Service Desk	In Production	
COMPUTE...	uphill-vm000008	Service Desk	In Production	
COMPUTE...	uphill-vm000009	Service Desk	In Production	

Table of Contents

Contents

1 SUMMARY

Integrating IT systems to get a complete overview of the companies IT assets as well as being able to troubleshoot faster is a key concern for modern companies.
Integrating Intune (What is Microsoft Intune | Microsoft Docs) with 4me (The Complete Service Management Platform - 4me) enables companies to get a quick overview of up to date data on assets and devices within the enterprise. This will enable companies to do the following directly in their Service Management Platform:

- ✓ Understand which assets the company owns
- ✓ Understand who is using the asset
- ✓ Understand if these assets are secure or exposes a threat to the company.
- ✓ Provide faster help if an end-user is having issues with one or more devices.

The purpose of this document is to provide an overview of how-to best plan and implement the 4me connector for Microsoft Intune.

Connector outcomes

By implementing the Microsoft Intune for 4me connector the following benefits can be leveraged:

- ✓ Enable customers to act on cloud data in 4me while using already defined workflow and automation.
- ✓ Easy onboarding with no need for knowledge or maintenance
- ✓ Build with scalability, security, and resilience in mind

Connector Value Propositions

The connector between Intune and 4me provides the following value propositions to the company:

- ✓ Faster time to resolution
- ✓ Fewer consoles to navigate
- ✓ Better overview of company assets

2 Introduction of the Microsoft Intune for 4me connector

Functionality

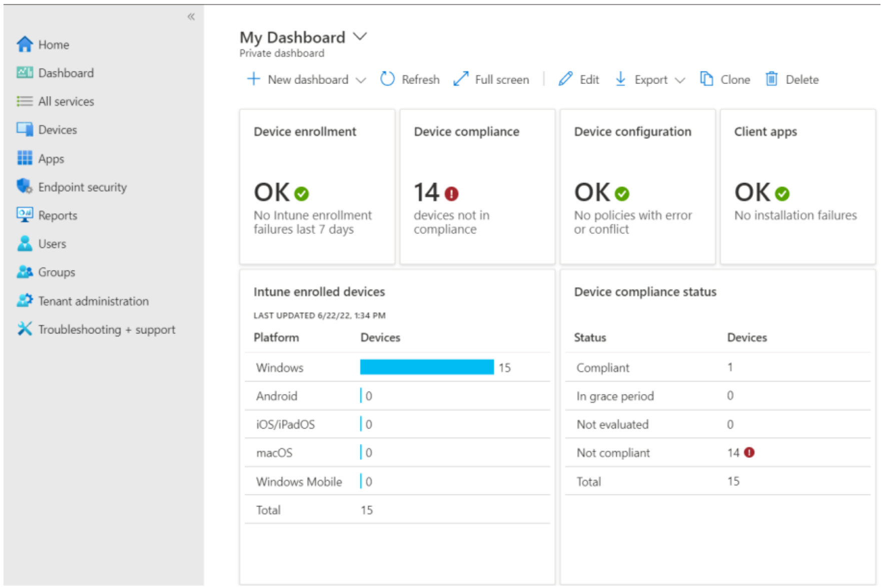
The connector is built to transfer valuable information from Intune to 4me to deliver visibility and collaboration for assets managed by Intune.

A series of core capabilities are designed to ensure that data that can be used for asset management or troubleshooting is made available to the teams and the tools they use the most with the following core areas in mind:

- ✓ Quick overview of device configuration for faster troubleshooting
- ✓ Fast insight if any devices are exposed to compliance risk.
- ✓ Deep link to more detailed information at the source if needed.

Intune overview

Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). You can manage your organizations devices using Intune including smart phones, tablets and laptops. Intune also allows you to define policies for your devices and alert you if any of these policies are out of company compliance. For example, you can raise a policy alert if a computer's hard drive is not encrypted or if Antivirus software is not running on a laptop that is managed by Intune. Intune integrates with Azure Active Directory (Azure AD) to control who has access and what they can access. It also integrates with Azure Information Protection for data protection. These features can enable the organization to implement and monitor for compliance policies that are not meeting company governance guidance.



Device enrollment: OK — No Intune enrollment failures last 7 days

Device compliance: 14 — devices not in compliance

Device configuration: OK — No policies with error or conflict

Client apps: OK — No installation failures

Intune enrolled devices

LAST UPDATED 6/22/22, 1:34 PM

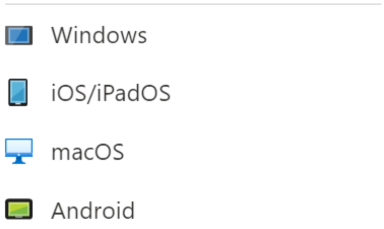
Platform	Devices
Windows	15
Android	0
iOS/iPadOS	0
macOS	0
Windows Mobile	0
Total	15

Device compliance status

Status	Devices
Compliant	1
In grace period	0
Not evaluated	0
Not compliant	14
Total	15

Devices are joined to Intune and hereafter they can be managed and inventoried using the Intune service.

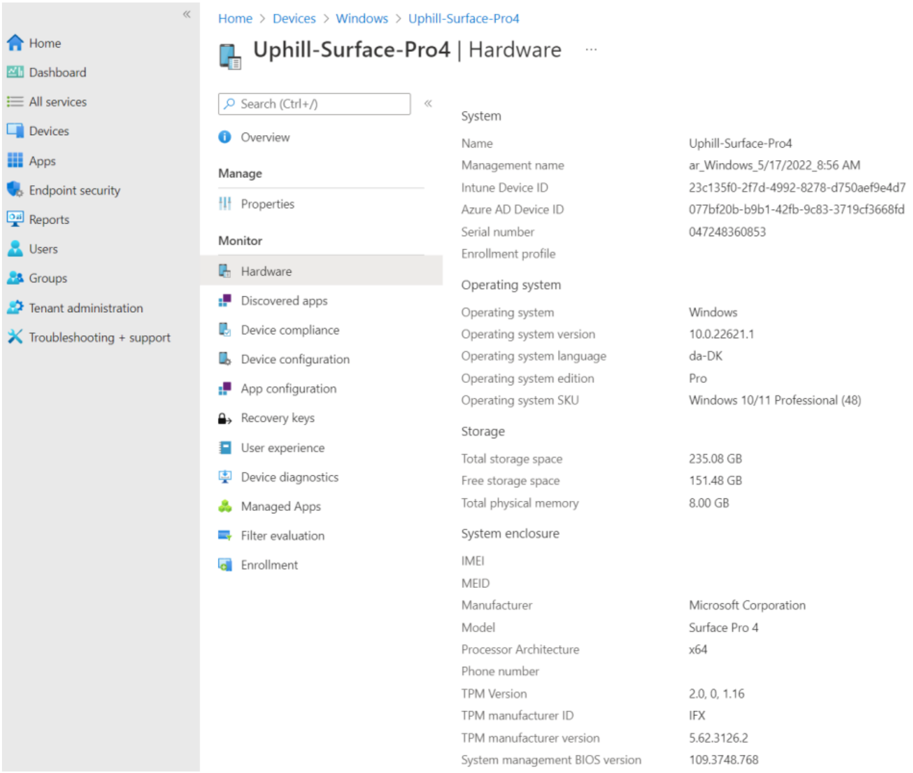
The picture below illustrates the type of devices that can be managed by Intune.



- Windows
- iOS/iPadOS
- macOS
- Android

Intune will collect hardware devices and software and make this data visible in the Intune portal.

The picture is an example of hardware information that can be seen in Intune for a Windows laptop.



Uphill-Surface-Pro4 | Hardware

System	
Name	Uphill-Surface-Pro4
Management name	ar_Windows_5/17/2022_8:56 AM
Intune Device ID	23c135f0-2f7d-4992-8278-d750aef9e4d7
Azure AD Device ID	077bf20b-b9b1-42fb-9c83-3719cf3668fd
Serial number	047248360853
Enrollment profile	
Operating system	
Operating system	Windows
Operating system version	10.0.22621.1
Operating system language	da-DK
Operating system edition	Pro
Operating system SKU	Windows 10/11 Professional (48)
Storage	
Total storage space	235.08 GB
Free storage space	151.48 GB
Total physical memory	8.00 GB
System enclosure	
IMEI	
MEID	
Manufacturer	Microsoft Corporation
Model	Surface Pro 4
Processor Architecture	x64
Phone number	
TPM Version	2.0, 0, 1.16
TPM manufacturer ID	IFX
TPM manufacturer version	5.62.3126.2
System management BIOS version	109.3748.768

Intune Compliance Policy Overview

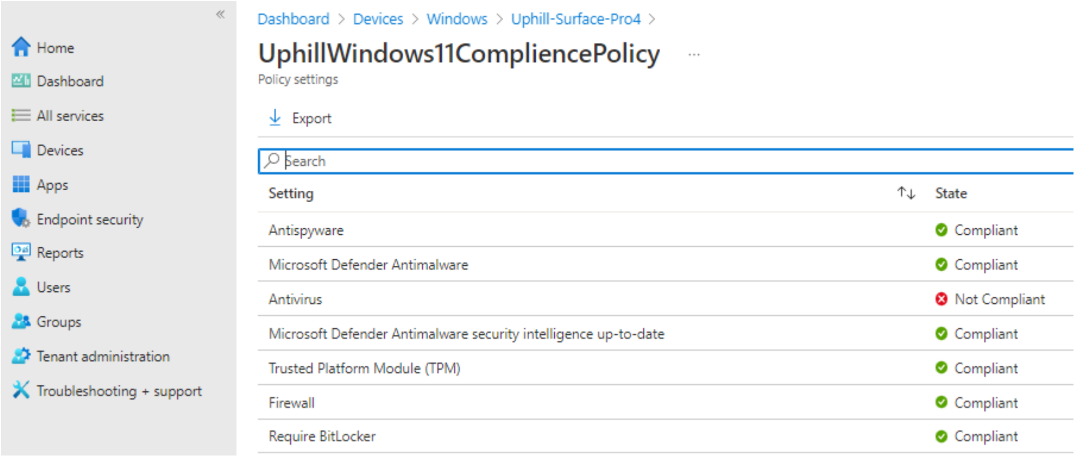
Intune provides the option to help protect organizational data by requiring users and devices to meet defined requirements. In Intune, this feature is called compliance policies.
This enables Intune administrators to define the rules and settings that users and devices must meet to be compliant in accordance with Company compliance policy.
This gives the following advantages

- ✓ Include actions that apply to devices that are noncompliant.
- ✓ Actions for noncompliance can alert users to the conditions of noncompliance and safeguard data on noncompliant devices.
- ✓ Can be combined with Conditional Access, which can then block users and devices that do not meet the rules.

Intune device compliance policies are defined in the following way:

- ✓ Define the rules and settings that users and managed devices must meet to be compliant. Examples of rules include requiring devices run a minimum OS version, not being jail-broken or rooted, and being at or under a threat level as specified by threat management software you've integrated with Intune.
- ✓ Support actions that apply to devices that do not meet your compliance rules. Examples of actions include being remotely locked or sending a device user an email about the device status so they can fix it.
- ✓ Deploy to users in user groups or devices in device groups. When a compliance policy is deployed to a user, all the user's devices are checked for compliance. Using device groups in this scenario helps with compliance reporting.

The picture below shows a device that is out of compliance, in this example the firewall is not running on the device:



Dashboard > Devices > Windows > Uphill-Surface-Pro4 >

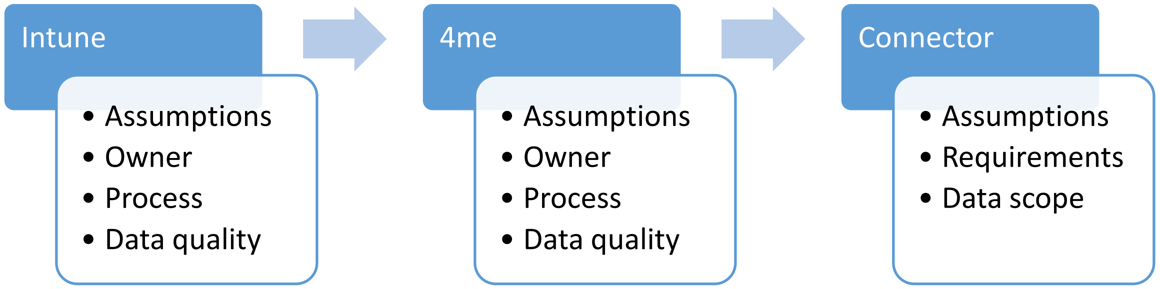
UphillWindows11Complience Policy ...

Policy settings

Setting	State
Antispyware	✓ Compliant
Microsoft Defender Antimalware	✓ Compliant
Antivirus	✗ Not Compliant
Microsoft Defender Antimalware security intelligence up-to-date	✓ Compliant
Trusted Platform Module (TPM)	✓ Compliant
Firewall	✓ Compliant
Require BitLocker	✓ Compliant

3 BEFORE YOU GET STARTED

3.1 Overall process flow



Intune

- Assumptions
- Owner
- Process
- Data quality

4me

- Assumptions
- Owner
- Process
- Data quality

Connector

- Assumptions
- Requirements
- Data scope

3.2 Intune

3.2.1 Assumptions

To get the most out of the integration between Intune and 4me, it’s advised that only devices that should be under management in 4me should be imported into the system. So before doing any integration it’s recommended to review the devices in Intune and decide which of these that should be imported into 4me.

3.2.2 Intune Owner

Is there an owner of Intune that looks after the system and maintains it?
Good practice to maintain good hygiene in Intune is to have an owner that looks after the system and is responsible for making sure that policies and devices joining or leaving Intune is following the processes defined by the company. This persona would also be responsible for communicating and establishing the needed procedures for why, how and when devices, software and policies are distributed to devices that are joined to Intune. The owner of the system would be responsible for carrying out the defined process of Intune.

3.2.3 Intune defined process

Is there a defined process for the lifecycle of devices, software, and policies in Intune?
Having such a process optimizes the value that Intune brings to the business but also optimizes the devices and their data that gets imported into 4me using the Microsoft Intune connector for 4me. It’s recommended that a process defines when a device gets added to Intune and when it leaves Intune. Furthermore, it should also define when a user is associated with a device and how any compliance policies are associated with a device and how this is enforced. This is to ensure that when data is imported into 4me that the data is correct and follows the intended data quality by following the described process of Intune.

3.2.4 Intune Data Quality

There are some high-level recommendations to follow before you are ready to connect the Microsoft Intune connector for 4me. Ensuring the data imported into 4me is accurate and holds high quality data is key for the success of the connector. This mainly falls back on the process and the owner being correctly established. However, before connecting the two systems, it's advised to perform a quick health check to understand if both systems are ready for this. Once verified the actual work of integrating the two systems can begin.

3.2.5 Bring Intune devices to a healthy state

If there are many devices not being used or orphan devices with no owner, it's recommended that these are cleaned up and removed from Intune, so they are not imported into 4 me. Having devices that are not under management in 4me might not bring the quality and follow the defined processes they were intended for. If auto pilot or other technology is used there can be exceptions to this rule, and this can be in accordance with the defined process.

3.2.6 Bring Intune policy to a healthy state

Policies used are implemented in accordance with governance requirements to frame the right picture of alerts being sent from Intune into 4me as requests, once the connector is configured. If these are not up-to-date or out of sync, there will be many unnecessary requests sent to 4me. Therefor it's advised before implementing the connector that the status and configuration of compliance policies matches and reflects the given situation in the environment, so this is raised accordingly in the 4me platform.

3.3 4me

3.3.1 Assumptions

To get the most out of the Microsoft Intune connector for 4me it's advised to consider the following areas as control points before configuring the connector for 4me. This is to ensure that the 4me platform does not get overloaded with CIs that were not intended and ensuring that service requests are created in the platform that does not have a described impact.

3.3.2 CI & Asset owner in 4me

It's advised that an owner of configuration and asset management is identified and looks after the system and maintains it. This owner should outline (via the process) the requirements for CIs & Assets being imported and if they hold the needed data to maintain and bring it under management.

3.3.3 There is a defined process for the lifecycle of devices in 4me

For CIs to be managed in accordance with the SCIM process definition it’s advised to have a defined process described and maintained in 4me. This process should be responsible for maintaining the CI through their life cycle and ensure that what CIs gets into 4me is in accordance with the process definition.

This process should define or have a scope of the following:

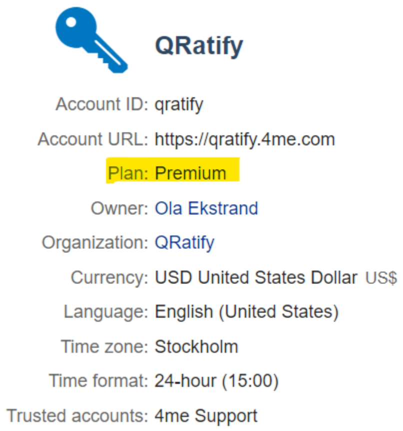
- ✓ Which devices should be in 4me?
- ✓ How do they get in there?
- ✓ How / when do the get deleted / removed
- ✓ Align with other process owners such as Financial Management, procurement, and similar functions

3.3.4 License type of 4me used in the Enterprise

In order to use the Microsoft Intune connector for 4me it’s a prerequisite that the Premium plan is used as the connector makes use of the asset management module that is part of this plan.

To find out which SKU you have, you can do the following.

1. Go to 4me console
2. Go to settings
3. Select Account overview
4. Verify that the plan used is Premium



QRatify

Account ID: qratify
Account URL: https://qratify.4me.com
Plan: Premium
Owner: Ola Ekstrand
Organization: QRatify
Currency: USD United States Dollar US$
Language: English (United States)
Time zone: Stockholm
Time format: 24-hour (15:00)
Trusted accounts: 4me Support

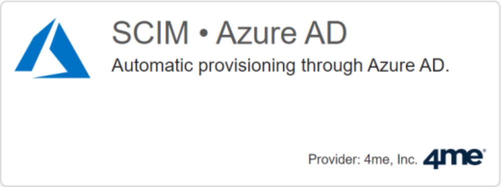
3.4 Azure Active Directory

For the connector to be able to define relationships between devices and their owners (connector will only do this where the requirements are met) the connector between Azure Active Directory and 4me must be configured before enabling the Microsoft Intune connector for 4me. If devices between Configuration Manager and Intune is configured, it's a requirement to also configure Azure AD sync between Azure and on-prem Active Directory. It is also a requirement that the Azure AD connector is configured to at least include the scope of users (owners) that Intune is importing devices and alerts for, to do the mapping correctly.

3.4.1 Setup the Azure Active Directory Connector

To be able to map users with the primary user of a device, the AAD connector (SIAM) needs to be configured first and the scope of users that matches the users having devices in Intune should be showing under people in 4me.

Make sure the following App is showing under installed apps and is configured accordingly



SCIM • Azure AD

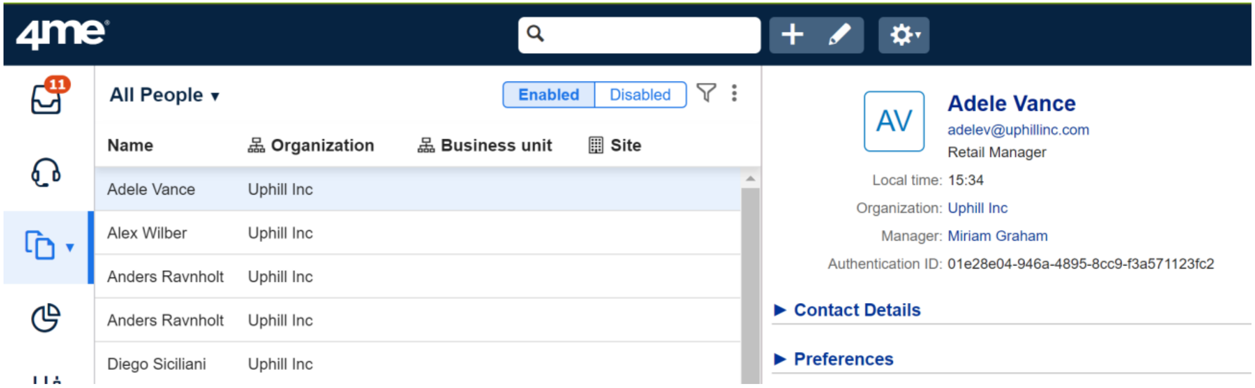
Automatic provisioning through Azure AD.

Provider: 4me, Inc.

To install the 4me connector please follow this guidance

Tutorial: Configure 4me for automatic user provisioning with Azure Active Directory - Microsoft Entra | Microsoft Docs

Users in 4me should now be listed under people like in the picture below.



Name	Organization	Business unit	Site
Adele Vance	Uphill Inc		
Alex Wilber	Uphill Inc		
Anders Ravnholt	Uphill Inc		
Anders Ravnholt	Uphill Inc		
Diego Siciliani	Uphill Inc		

AV Adele Vance
adelev@uphillinc.com
Retail Manager

Local time: 15:34
Organization: Uphill Inc
Manager: Miriam Graham
Authentication ID: 01e28e04-946a-4895-8cc9-f3a571123fc2

Ensure that the e-mail address listed under the person matches the UPN for the primary person listed for a device in Intune (primary user).

4 Microsoft Intune connector for 4me details

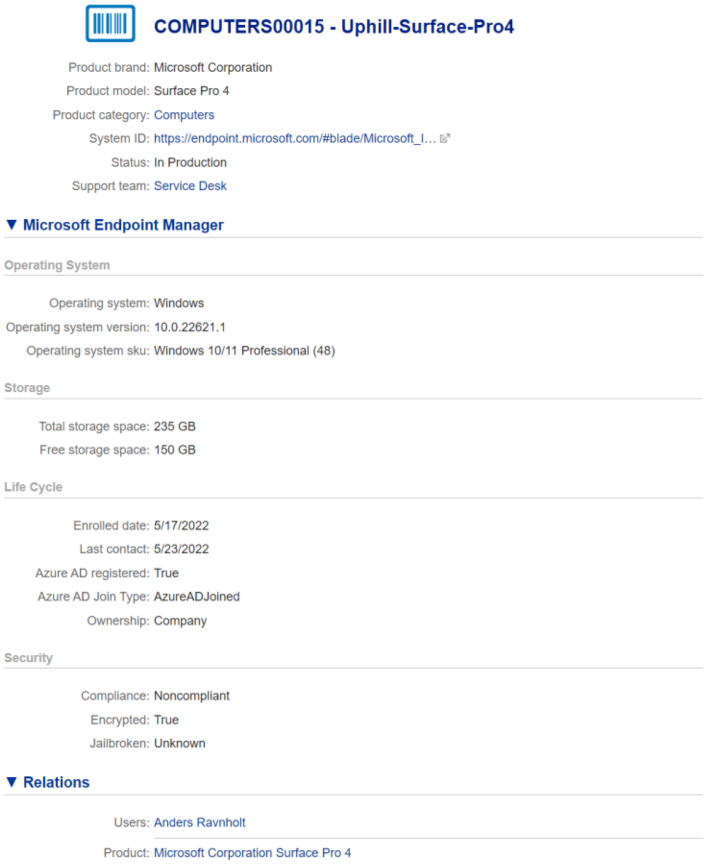
This section will outline the data that is synchronized from Intune to 4me as part of the connector. This is split into two parts, the Configuration Items and the Intune Policy Incidents as well as the relationships maintained by the connector.

4.1 CI Data that is synced to 4me.

The following information will be brought over from Intune as attributes for a CI under Configuration Items:

CI Type	Data	Example
Operating System	Operating System	Windows
	Operating System version	10.0.22621.1
	Operating System SKU	Windows 10 Professional
Storage	Total Storage Space	235 GB
	Free Storage Space	150 GB
Life Cycle	Enrolled date	11/17/2022
	Last Contact	11/23/2022
	Azure AD registered	True
	Azure AD Join Type	AzureADJoined
	Ownership	Company
Security	Compliance	Noncompliant
	Encrypted	True
	Jailbroken	Unknown

This information will look like the following in the 4me portal under CIs



COMPUTERS00015 - Uphill-Surface-Pro4

Product brand: Microsoft Corporation
Product model: Surface Pro 4
Product category: Computers
System ID: https://endpoint.microsoft.com/#blade/Microsoft_I…
Status: In Production
Support team: Service Desk

▼ **Microsoft Endpoint Manager**

Operating System

Operating system: Windows
Operating system version: 10.0.22621.1
Operating system sku: Windows 10/11 Professional (48)

Storage

Total storage space: 235 GB
Free storage space: 150 GB

Life Cycle

Enrolled date: 5/17/2022
Last contact: 5/23/2022
Azure AD registered: True
Azure AD Join Type: AzureADJoined
Ownership: Company

Security

Compliance: Noncompliant
Encrypted: True
Jailbroken: Unknown

▼ **Relations**

Users: Anders Ravnholt
Product: Microsoft Corporation Surface Pro 4

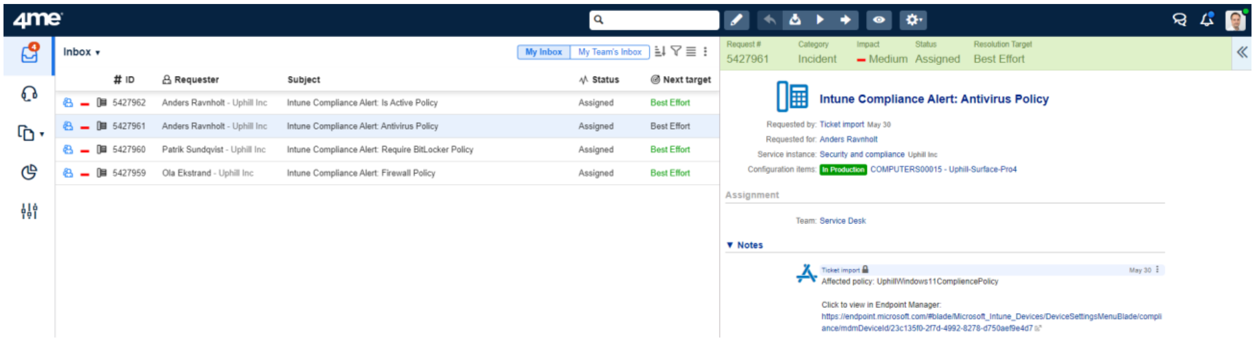
4.2 CI relationship data in 4me

The following relationship are made if the requirements are met when configuring the Intune connector.

- CI to Person relationship
- Product to CI relationship
- Intune Service Request relationship to Person and CI

4.3 Compliance Data that is synced to 4me

The Intune connector can forward Intune Compliancy Policy alerts directly to 4me as Incidents with associated device and person.
This will enable you to quickly respond to configuration drifts in terms of policy violations and compliancy risks that needs to be addressed accordingly.



# ID	Requester	Subject	Status	Next target
5427962	Anders Ravnholt - Uphill Inc	Intune Compliance Alert: Is Active Policy	Assigned	Best Effort
5427961	Anders Ravnholt - Uphill Inc	Intune Compliance Alert: Antivirus Policy	Assigned	Best Effort
5427960	Patrik Sundqvist - Uphill Inc	Intune Compliance Alert: Require BitLocker Policy	Assigned	Best Effort
5427959	Ola Ekstrand - Uphill Inc	Intune Compliance Alert: Firewall Policy	Assigned	Best Effort

Request #	Category	Impact	Status	Resolution Target
5427961	Incident	▬ Medium	Assigned	Best Effort

Intune Compliance Alert: Antivirus Policy

Requested by: Ticket import May 30
Requested for: Anders Ravnholt
Service instance: Security and compliance Uphill Inc
Configuration items: In Production COMPUTERS00015 - Uphill-Surface-Pro4

Assignment

Team: Service Desk

▼ Notes

Ticket import May 30
Affected policy: UphillWindows11CompliencePolicy

Click to view in Endpoint Manager:
https://endpoint.microsoft.com/#blade/Microsoft_Intune_Devices/DeviceSettingsMenuBlade/compliance/mdmDeviceId/23c135f0-2f7d-4992-8278-d750aef9e4d7

4.4 Configuration Manager Data that is synced to 4me

Configuration Manager devices can be imported into 4me if data between Configuration Manager and Intune is configured correctly. This is referred to as co-management
There are two paths to reach co-management:
Existing Configuration Manager clients: You have Windows 10 or later devices that are already Configuration Manager clients. You set up hybrid Azure AD, and enroll them into Intune
New internet-based devices: You have new Windows 10 or later devices that join Azure AD and automatically enroll to Intune. You install the Configuration Manager client to reach a co-management state.

This is a described process and can be configured by following this link:
Enable co-management - Configuration Manager | Microsoft Docs

If devices are replicated (co-managed) in Intune from Configuration Manager, the connector will import these devices into 4me.

5 CONNECTOR IMPLEMENTATION

Implementing the Microsoft Intune connector for 4me is simple and straight forward. The process itself takes a few minutes to complete and requires minimal effort to implement. There are a few requirements that must be in place, to install the app and most of these deals with access rights in Intune and 4me.

5.1 Intune prerequisites

To get devices into 4me you would need to have the required licenses for Intune for the users and or devices.
Please see the following link for more details on Licenses available for Microsoft Intune | Microsoft Docs
Following this as part of the installation there will be a request for providing Azure Active Directory credentials that has enough rights to consent to giving the following rights to a Service Principal in Azure Active Directory.

- Sign in and read user profile
- Read Microsoft Intune devices
- Read Microsoft Intune policy

5.2 4me Prerequisites

5.2.1 Artifacts

The following artifacts will be implemented into 4me as part of the connector configuration.

- CI UI Extension (Intune data attributes)
- Automation rules

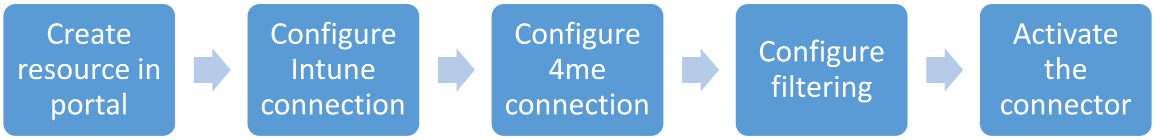
5.2.2 Security requirements

To install the app in your 4me environment you would have to have one or more of the following roles:

- Account owner
- Account designer
- Account administrator

5.3 Installing the Intune for 4me connector overview

The end-to-end process for installing the connector is illustrated below.
The installation should take no more than 9 minutes to complete.

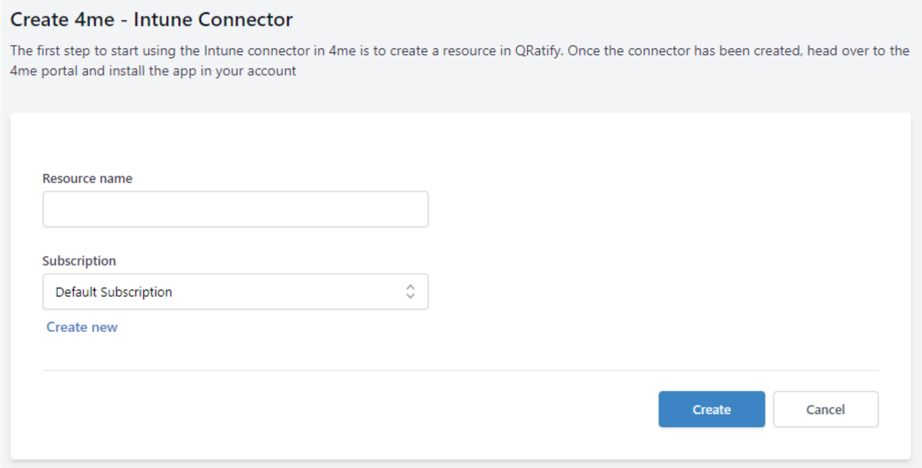


Create resource in portal → Configure Intune connection → Configure 4me connection → Configure filtering → Activate the connector

5.3.1 Create resource (Connector) in portal

To create the connector in the QRatify portal follow these steps:

1. Create a "4me – Intune Connector" resource
   a. Use the link that has been provided to you to go to the QRatify portal
   b. Click Sign In
   c. Complete the sign-in with the user that you want to make administrator in the QRatify Platform
   d. Click Products
   e. Click Create on the product offering called "4me - Intune Connector"
   f. Give the Resource a name and place it in a Subscription



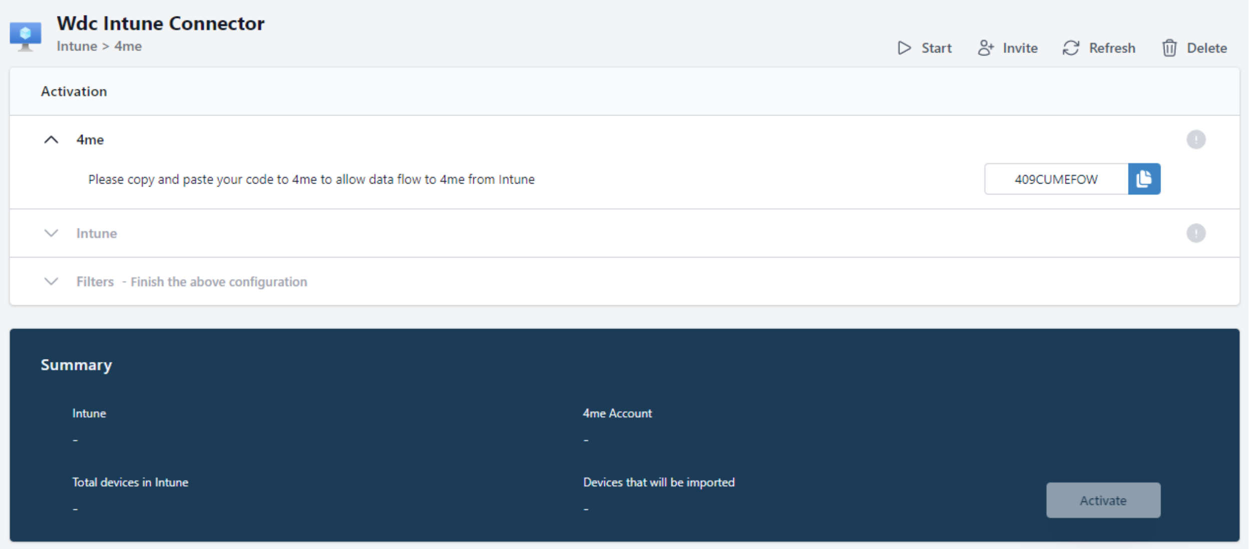
Create 4me - Intune Connector

The first step to start using the Intune connector in 4me is to create a resource in QRatify. Once the connector has been created, head over to the 4me portal and install the app in your account

Resource name

Subscription: Default Subscription

2. Connect the resource to 4me



Wdc Intune Connector

Intune > 4me

Please copy and paste your code to 4me to allow data flow to 4me from Intune

409CUMEFOW

Summary

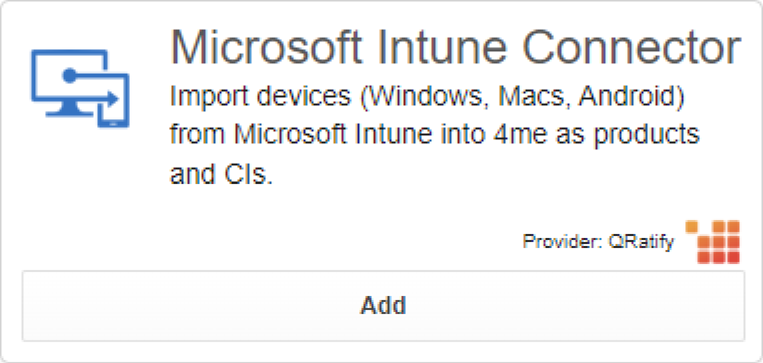
Intune: -

4me Account: -

Total devices in Intune: -

Devices that will be imported: -

   a. Copy to code
   b. Go to the App Store in 4me
   c. Click Add on the Microsoft Intune Connector

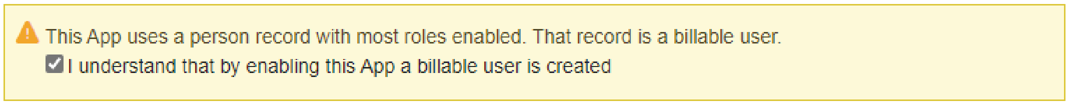


Microsoft Intune Connector

Import devices (Windows, Macs, Android) from Microsoft Intune into 4me as products and CIs.

Provider: QRatify

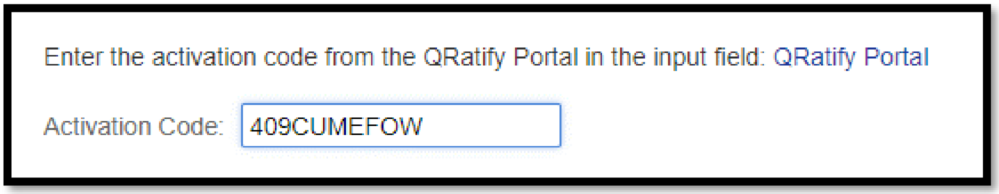
   d. Confirm the fact that the App uses a person record which is a billable user.



⚠ This App uses a person record with most roles enabled. That record is a billable user.

☑ I understand that by enabling this App a billable user is created

   e. At step 2, enter the code from the QRatify Portal



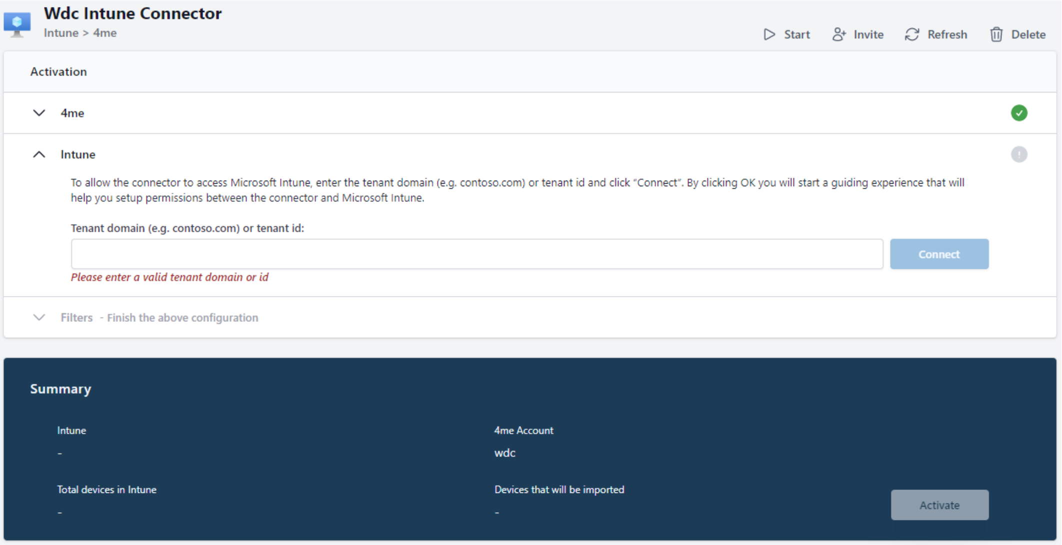
Enter the activation code from the QRatify Portal in the input field: QRatify Portal

Activation Code: 409CUMEFOW

   f. Click Save
   g. Go back to the resource previously created in the QRatify Portal

3. Connect to Microsoft Intune
   a. If the 4me connection doesn't show a checkmark, wait a bit an click Refresh.

b. In the Tenant domain textbox, enter the name of the Intune domain you want to connect to.



Wdc Intune Connector

Intune > 4me

Activation

4me

Intune

To allow the connector to access Microsoft Intune, enter the tenant domain (e.g. contoso.com) or tenant id and click "Connect". By clicking OK you will start a guiding experience that will help you setup permissions between the connector and Microsoft Intune.

Tenant domain (e.g. contoso.com) or tenant id:

Please enter a valid tenant domain or id

Filters - Finish the above configuration

Summary

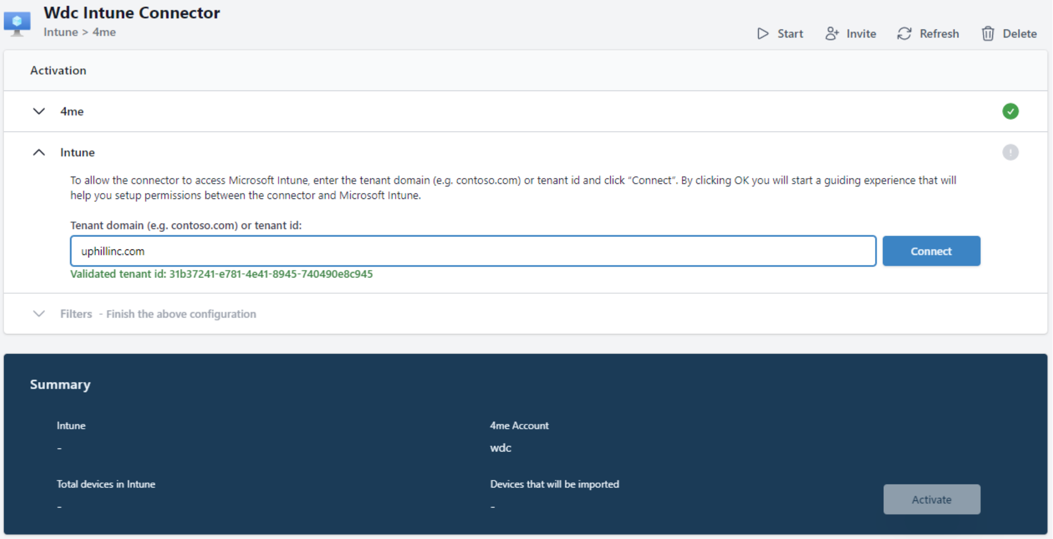
Intune: -

4me Account: wdc

Total devices in Intune: -

Devices that will be imported: -

c. Once the domain has been validated, click Connect



Wdc Intune Connector

Intune > 4me

Activation

4me

Intune

To allow the connector to access Microsoft Intune, enter the tenant domain (e.g. contoso.com) or tenant id and click "Connect". By clicking OK you will start a guiding experience that will help you setup permissions between the connector and Microsoft Intune.

Tenant domain (e.g. contoso.com) or tenant id: uphillinc.com

Validated tenant id: 31b37241-e781-4e41-8945-740490e8c945

Filters - Finish the above configuration

Summary

Intune: -

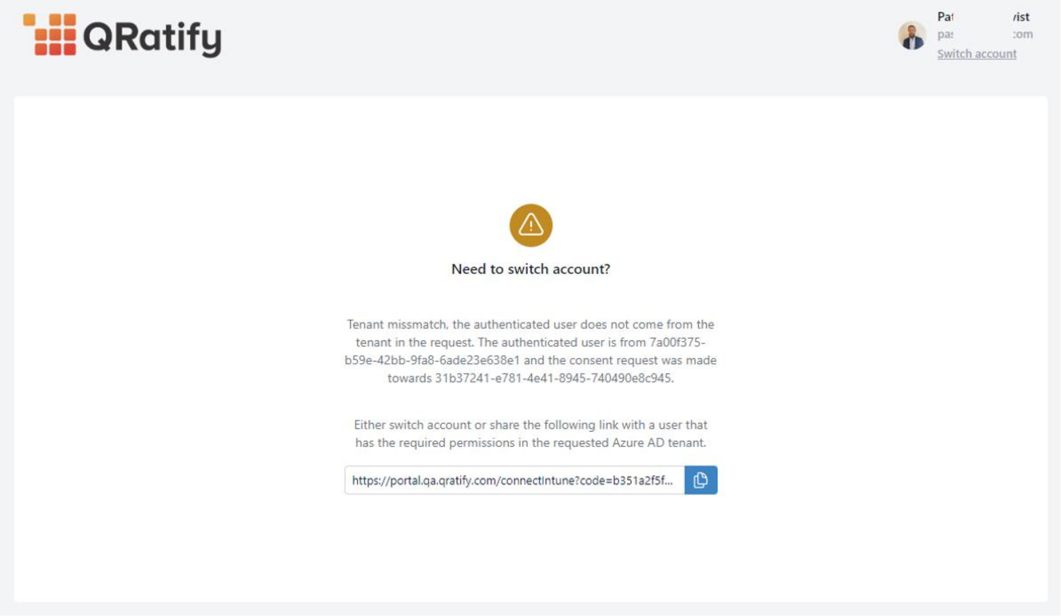
4me Account: wdc

Total devices in Intune: -

Devices that will be imported: -

d. A new tab in the browser opens where you can review, consent and give access to the Intune domain

e. If the user you're currently logged in with doesn't have the required permission or is from the wrong tenant you'll be notified and have the option to switch account or send a link to a user that has the required permissions.



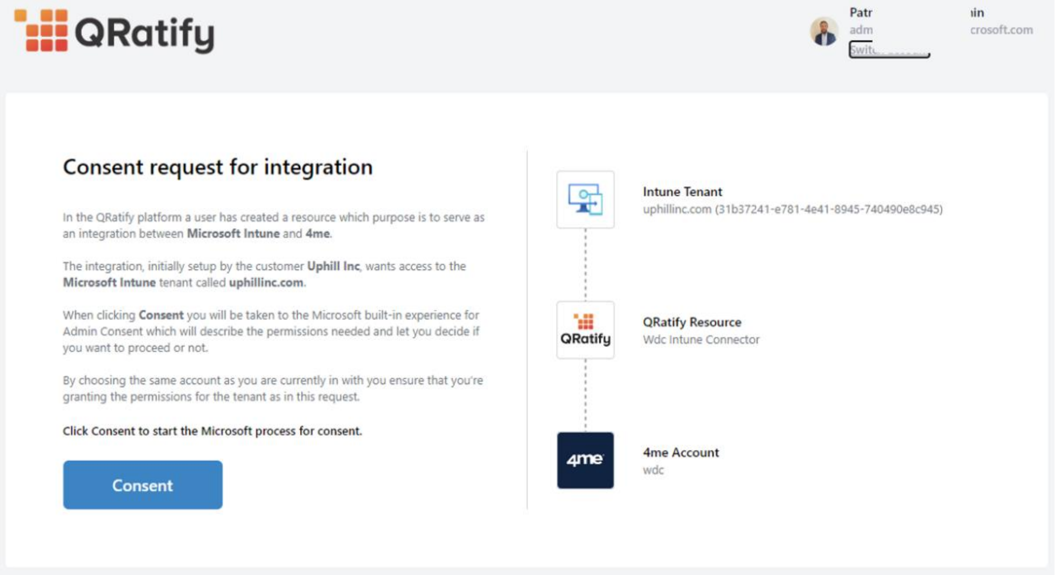
Need to switch account?

Tenant missmatch, the authenticated user does not come from the tenant in the request. The authenticated user is from 7a00f375-b59e-42bb-9fa8-6ade23e638e1 and the consent request was made towards 31b37241-e781-4e41-8945-740490e8c945.

Either switch account or share the following link with a user that has the required permissions in the requested Azure AD tenant.

https://portal.qa.qratify.com/connectintune?code=b351a2f5f...

f. When you have switch to an account the has the required permissions you can see information about the connection your about to make.



Consent request for integration

In the QRatify platform a user has created a resource which purpose is to serve as an integration between **Microsoft Intune** and **4me**.

The integration, initially setup by the customer **Uphill Inc**, wants access to the **Microsoft Intune** tenant called **uphillinc.com**.

When clicking **Consent** you will be taken to the Microsoft built-in experience for Admin Consent which will describe the permissions needed and let you decide if you want to proceed or not.

By choosing the same account as you are currently in with you ensure that you're granting the permissions for the tenant as in this request.

Click Consent to start the Microsoft process for consent.

Consent

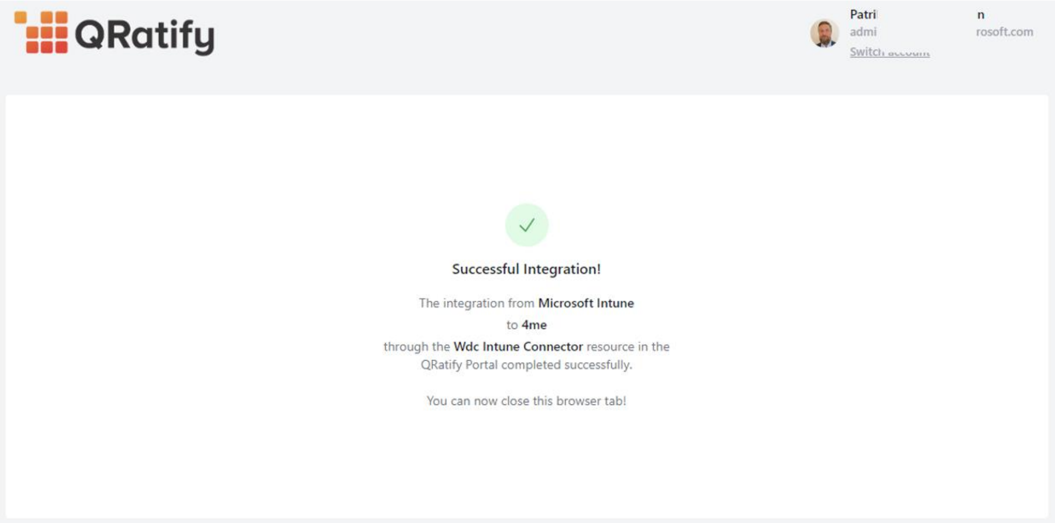
Intune Tenant
uphillinc.com (31b37241-e781-4e41-8945-740490e8c945)

QRatify Resource
Wdc Intune Connector

4me Account
wdc

g. Once pleased click Consent, this will start the actual Consent process to setup the connection.
Note: You might be prompted to select Account again in this process but that is currently by design.

h. Once you have reviewed the requested permissions, terms and completed the Consent process the page will inform you that the integration was successful.



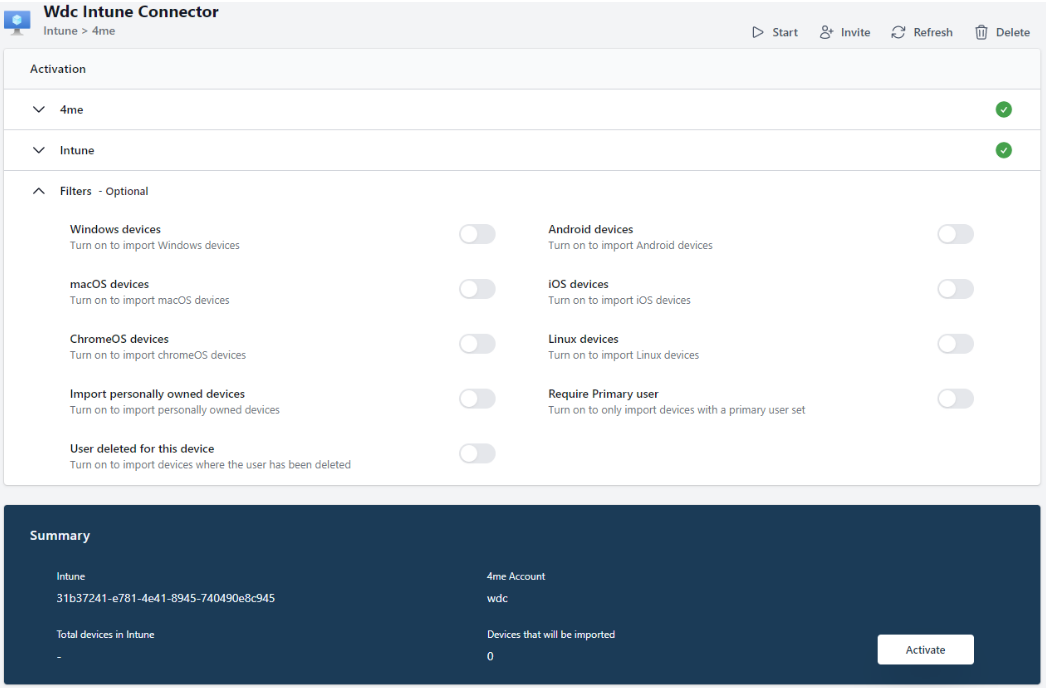
✓

Successful Integration!

The integration from **Microsoft Intune**
to **4me**
through the **Wdc Intune Connector** resource in the
QRatify Portal completed successfully.

You can now close this browser tab!

i. You can now return to the previous browser tab showing your connector resource connected to both 4me and Intune



Activation

4me ✓

Intune ✓

Filters - Optional

Windows devices Turn on to import Windows devices	○	Android devices Turn on to import Android devices	○
macOS devices Turn on to import macOS devices	○	iOS devices Turn on to import iOS devices	○
ChromeOS devices Turn on to import chromeOS devices	○	Linux devices Turn on to import Linux devices	○
Import personally owned devices Turn on to import personally owned devices	○	Require Primary user Turn on to only import devices with a primary user set	○
User deleted for this device Turn on to import devices where the user has been deleted	○		

Summary

Intune: 31b37241-e781-4e41-8945-740490e8c945

4me Account: wdc

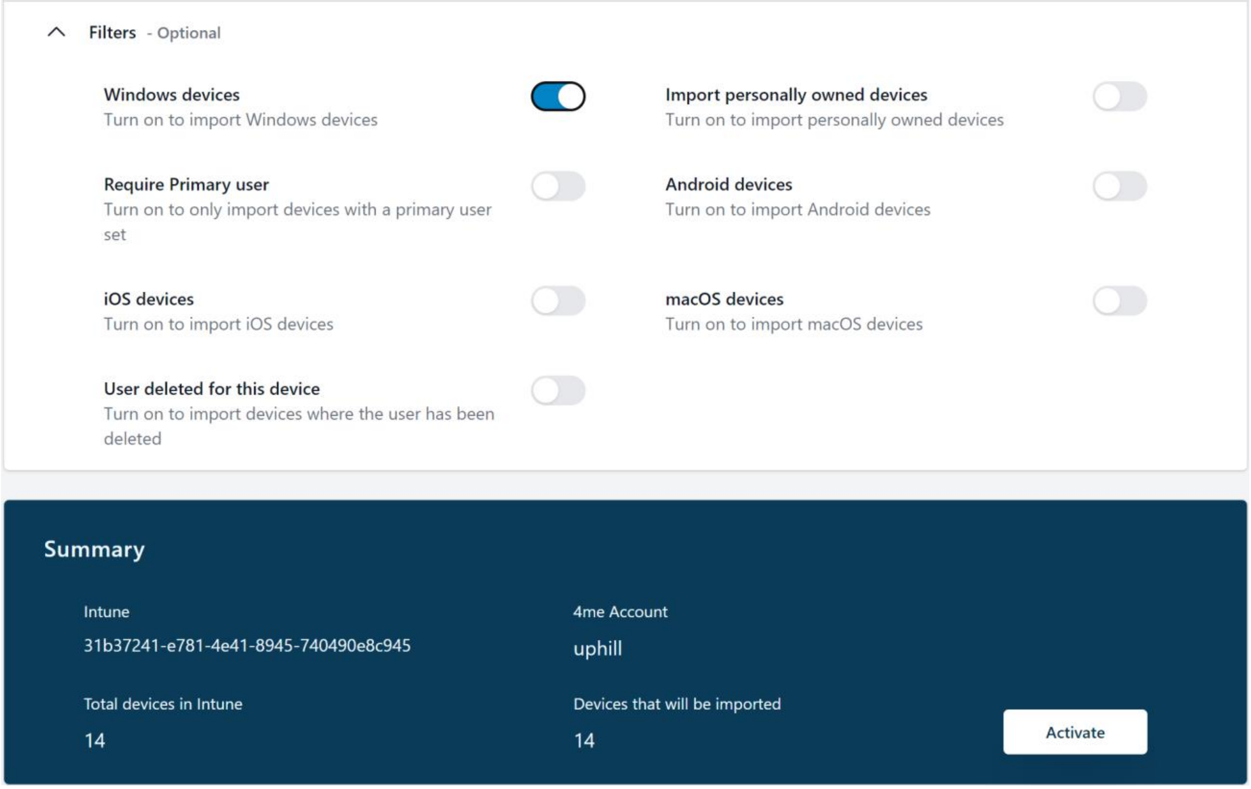
Total devices in Intune: -

Devices that will be imported: 0

5.4 Configuration Settings

As part of the implementation of the Microsoft Intune connector for 4me a series of configuration options are provided to enable the enterprise with an optimal selection of filters to ensure only devices that should be under management gets imported into 4me.

By default, no CIs gets imported but, device types can be filter in / out along with other settings. Below is an explanation of each setting that can filter CIs being imported into 4me.



Filters - Optional

● **Windows devices**
Turn on to import Windows devices

○ **Import personally owned devices**
Turn on to import personally owned devices

○ **Require Primary user**
Turn on to only import devices with a primary user set

○ **Android devices**
Turn on to import Android devices

○ **iOS devices**
Turn on to import iOS devices

○ **macOS devices**
Turn on to import macOS devices

○ **User deleted for this device**
Turn on to import devices where the user has been deleted

Summary

Intune
31b37241-e781-4e41-8945-740490e8c945

4me Account
uphill

Total devices in Intune
14

Devices that will be imported
14

Configuration options:	Description
User deleted for this device	If this filter is turned on (Off by default) devices which had the primary owner deleted will be imported into 4me. The name of the device will be “user deleted for this device” and there will be limited information about the device.
Require Primary User	This filter will, if enabled, only import users that has a primary user assigned to the device. If this is enabled, it will also filter out devices that “User deleted for this device.
Import personally owned devices	This will, if enabled, import personally owned devices which reflects the way (and ownership) that the devices were added to Intune. By default, it means that the company is not responsible for the device but can enforce policies and settings on e.g., a phone to ensure it’s “protected”. This setting will have impact on the computer devices imported by the connector and not phones and mobile devices.
Windows Devices	Will if enabled import Windows devices registered in Intune into 4me.
Android Devices	Will if enabled import Android devices registered in Intune into 4me.
iOS Devices	Will if enabled import iOS devices registered in Intune into 4me.
macOS Devices	Will if enabled import macOS devices registered in Intune into 4me.

Summary Section

In the summary section there will be an overview of how many devices there is in total and toggling the different options will adjust the number of devices that will be imported with the given configuration.

Once the right combination is found click activate to enable the connector.

6 4ME POST IMPLEMENTATION ACTIONS

Once the connector has been implemented correctly the following actions can be performed to validate that the correct information is now being imported from Intune into 4me.

6.1 Products from Intune created in 4me

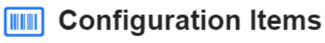
When the Configuration Items are imported to 4me the connector tries to find existing Configuration Items in 4me using the serial number of the device. If a match is found the existing CI is updated with metadata from Microsoft Intune. If an existing CI isn't found the connector creates a new CI as well as a simple product, representing the type of device. These products should be seen as a temporary product association until you have associated the CI with the product of your choice. You should also make sure that you associate your CIs with the correct Service and Service Instance.

Note: It's very important that you associate your CIs with correct Services and Service Instances before enabling the Alerts functionality in the Intune Connector.

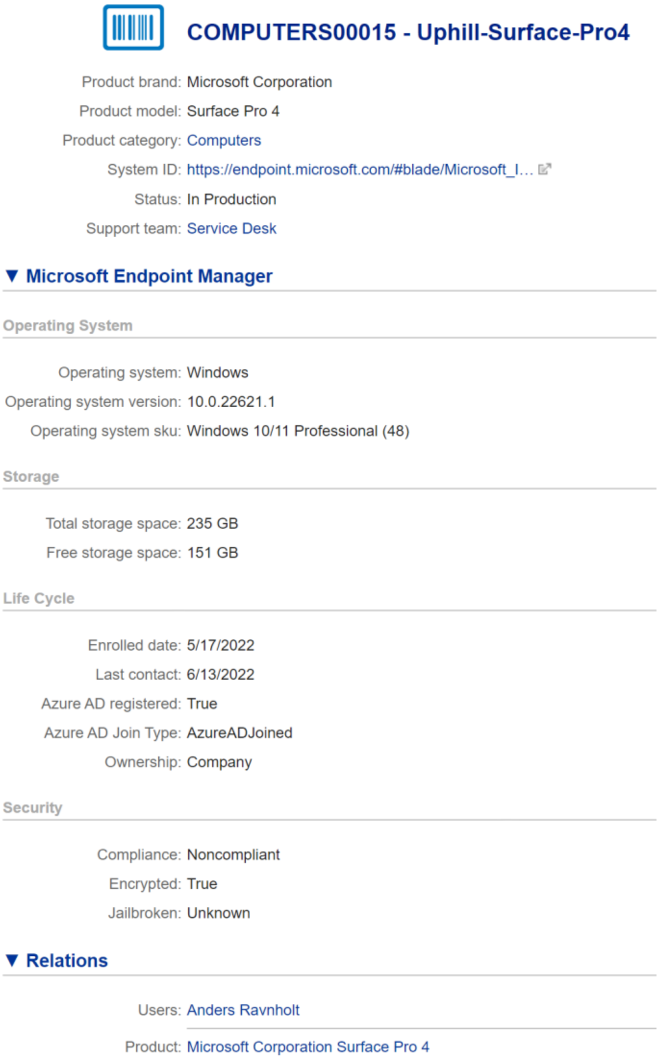
6.2 Configuration Items from Intune created in 4me

To verify that CIs are correctly imported from Intune into 4me the following steps can be taken.

Note: It can take a few minutes before the connector has updated the CI information in your 4me account.

1. In the main console Select "Records"
2. Select "Configuration Items" in the Menu list 

3. Select a Configuration Item that was imported from Intune, there should be minimum 1 or more in the list.
4. Verify that the information is correct and that there is minimum 1 product and 1 user showing (requires that Azure AD connector is configured) under relations.



COMPUTERS00015 - Uphill-Surface-Pro4

Product brand: Microsoft Corporation
Product model: Surface Pro 4
Product category: Computers
System ID: https://endpoint.microsoft.com/#blade/Microsoft_I…
Status: In Production
Support team: Service Desk

▼ Microsoft Endpoint Manager

Operating System

Operating system: Windows
Operating system version: 10.0.22621.1
Operating system sku: Windows 10/11 Professional (48)

Storage

Total storage space: 235 GB
Free storage space: 151 GB

Life Cycle

Enrolled date: 5/17/2022
Last contact: 6/13/2022
Azure AD registered: True
Azure AD Join Type: AzureADJoined
Ownership: Company

Security

Compliance: Noncompliant
Encrypted: True
Jailbroken: Unknown

▼ Relations

Users: Anders Ravnholt
Product: Microsoft Corporation Surface Pro 4

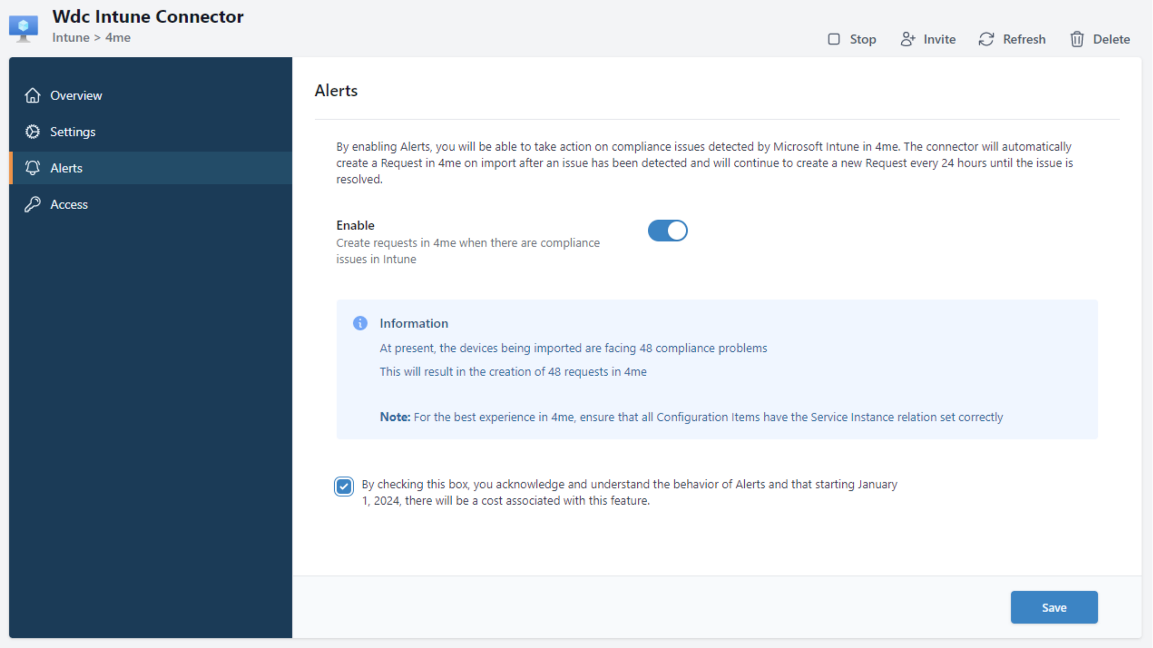
7 Compliance Alerts

The connector allows you to create Incidents based on Compliance Issues in Microsoft Intune. The following sections guides you through the processing of enabling Alerts for the connector which allows you to quickly raise awareness about possible security issues detected by Microsoft Intune.

7.1 Enable Alerts

To enable this for the imported devices, follow these steps:

1. Sign in to the QRatify Portal
2. Locate the connector resource you want to enable Alerts for
3. Toggle the Enable button
4. Make sure you read and understand that the Alerts feature comes with an additional Cost starting January 1st 2024



Alerts

By enabling Alerts, you will be able to take action on compliance issues detected by Microsoft Intune in 4me. The connector will automatically create a Request in 4me on import after an issue has been detected and will continue to create a new Request every 24 hours until the issue is resolved.

Enable
Create requests in 4me when there are compliance issues in Intune

Information
At present, the devices being imported are facing 48 compliance problems
This will result in the creation of 48 requests in 4me

Note: For the best experience in 4me, ensure that all Configuration Items have the Service Instance relation set correctly

☑ By checking this box, you acknowledge and understand the behavior of Alerts and that starting January 1, 2024, there will be a cost associated with this feature.

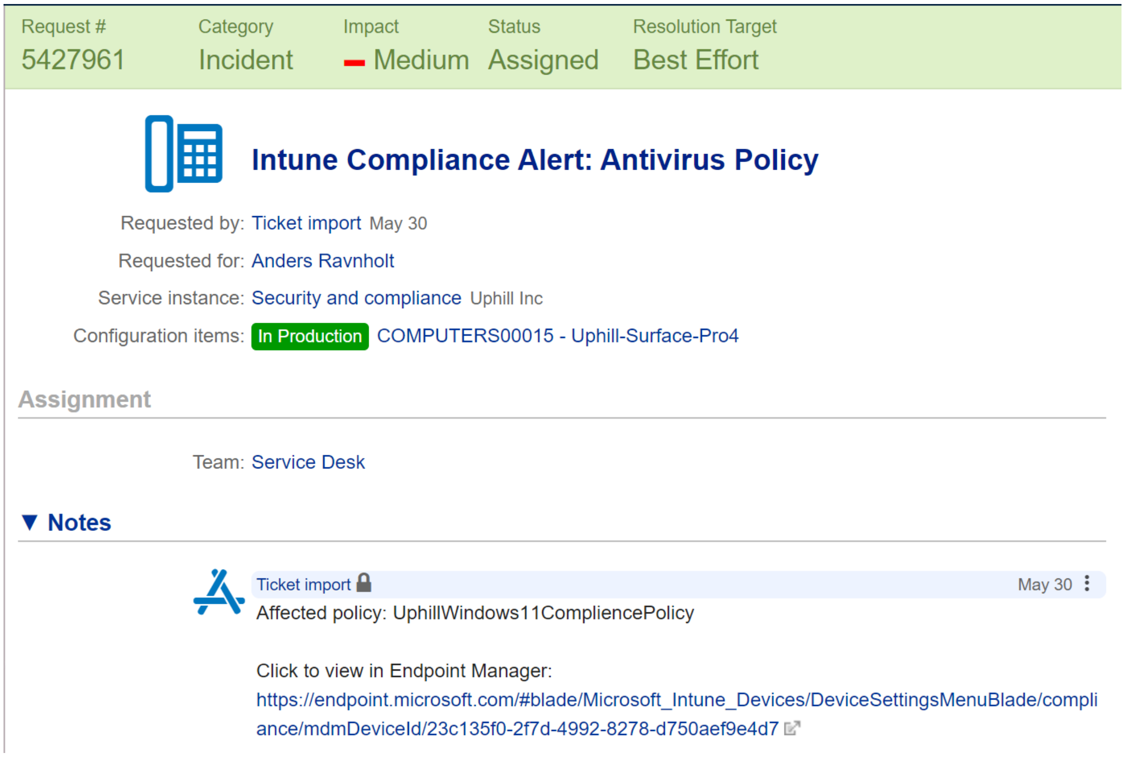
5. Click Save

Note: It's very important that you associate your CIs with correct Services and Service Instances before enabling the Alerts functionality in the Intune Connector. If this isn't done the connector will not be able to associate the Request with the affected configuration item.

7.2 Requests are created from Intune in 4me

To verify that Intune policy alerts are correctly imported from Intune into 4me the following steps can be taken:

1. In the main console Select "Records" ⧉ ▼
2. Select "Requests" in the Menu list
3. Select a request that was imported from Intune
   Note: It can take up to 60 minutes before the first Request is created (if you have any Compliance Issues in Intune)
4. Click on the request and verify that the request holds data like the one listed below.



Request #	Category	Impact	Status	Resolution Target
5427961	Incident	🟥 Medium	Assigned	Best Effort

Intune Compliance Alert: Antivirus Policy

Requested by: Ticket import May 30

Requested for: Anders Ravnholt

Service instance: Security and compliance Uphill Inc

Configuration items: In Production COMPUTERS00015 - Uphill-Surface-Pro4

Assignment

Team: Service Desk

▼ Notes

Ticket import 🔒 May 30 ⋮

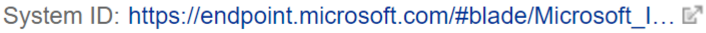
Affected policy: UphillWindows11CompliencePolicy

Click to view in Endpoint Manager:
https://endpoint.microsoft.com/#blade/Microsoft_Intune_Devices/DeviceSettingsMenuBlade/compliance/mdmDeviceId/23c135f0-2f7d-4992-8278-d750aef9e4d7

8 Using the Microsoft Intune connector for 4me

8.1 Using deep link within a CI.

To be able to quickly navigate between the 4me console and Intune, the connector will add a deep link to the CI under configuration item, to use this capability please take the following steps:
Note: You must have a user account that has minimum access of read to Intune Configuration Items to be able to access the data in Intune.

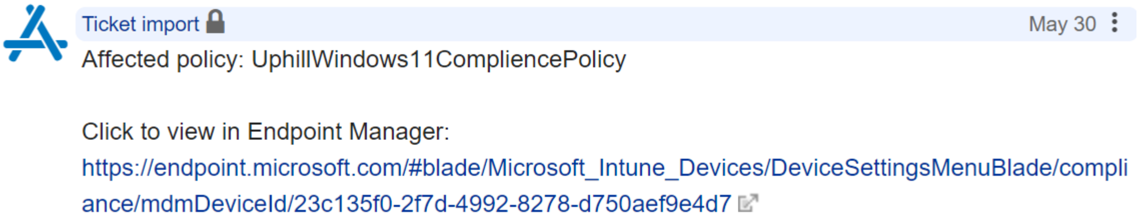
1. In the main console Select "Main Records" ▾
2. Select "Configuration Items" in the Menu list
   Configuration Items
3. Select a CI that was imported from Intune
4. Click on System ID to follow the deep link into Intune:
   
   System ID: https://endpoint.microsoft.com/#blade/Microsoft_I…
5. Login with you Azure AD credentials
6. Browse detailed information in Intune about the CI selected in 4me
   a. Hardware
   b. Discovered apps
   c. Device Compliance
   d. Device Configuration
   e. App Configuration
   f. Recovery keys

8.2 Using deep link within a Request

To be able to quickly navigate between the 4me console and Intune, the connector will add a deep link to the request so more information can be quickly obtained in Intune, to use this capability please take the following steps:

Note: You must have a user account that has minimum access of read in Intune policy compliance to be able to access the data in Intune, furthermore, there must be one or more Policy requests raised by Intune in order to follow this guidance.

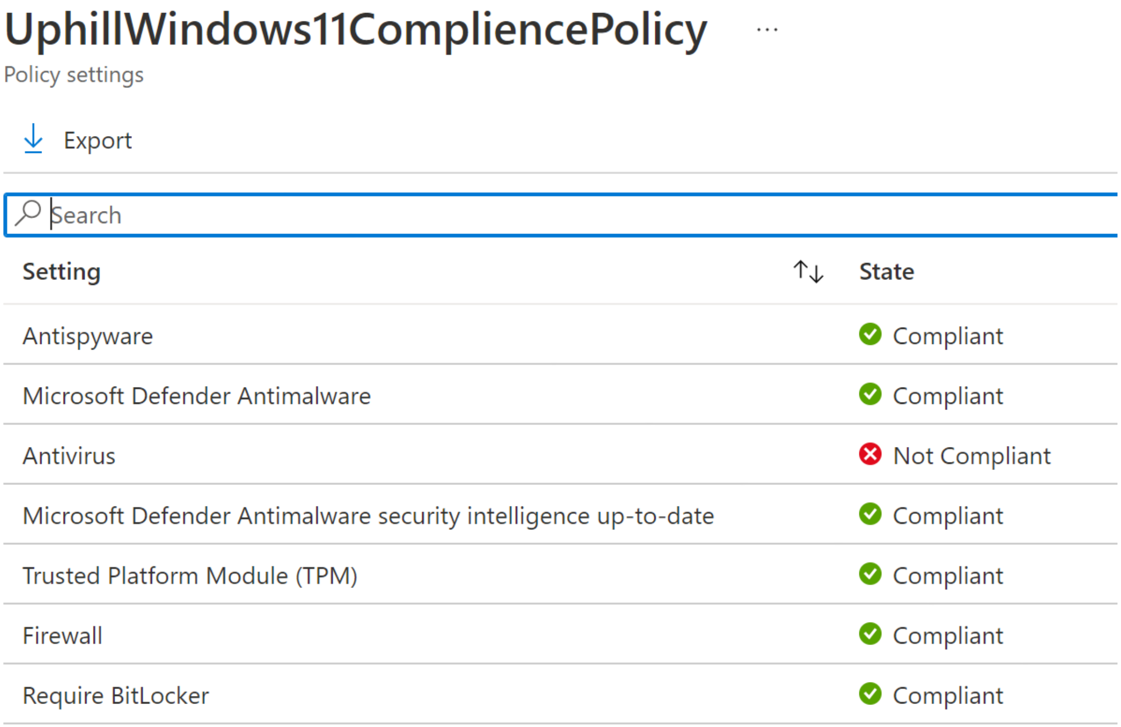
5. In the main console Select "Inbox"
6. Select a request that was created by Intune
7. Click on Notes to identify the policy that triggered the alert and see the deep link to Intune:



Affected policy: UphillWindows11CompliencePolicy

Click to view in Endpoint Manager:
https://endpoint.microsoft.com/#blade/Microsoft_Intune_Devices/DeviceSettingsMenuBlade/compliance/mdmDeviceId/23c135f0-2f7d-4992-8278-d750aef9e4d7

8. Login with you Azure AD credentials
9. Browse detailed information in Intune about the compliance issue raised by Intune



UphillWindows11CompliencePolicy

Policy settings

Setting	State
Antispyware	✓ Compliant
Microsoft Defender Antimalware	✓ Compliant
Antivirus	✗ Not Compliant
Microsoft Defender Antimalware security intelligence up-to-date	✓ Compliant
Trusted Platform Module (TPM)	✓ Compliant
Firewall	✓ Compliant
Require BitLocker	✓ Compliant

9 COMMON SUPPORT QUESTIONS

The following table contains a list of the most common support questions.

Question	Answer
Can I connect multiple Intune tenants into the same 4me Instance?	At this point we do not support connecting multiple Intune instances to one 4me account. If you have this need, please raise a request to QRatify so we can investigate the ask.
Can you support devices from Configuration Manager if I already have Intune?	Yes, this is possible, you would have to integrate Configuration Manager and Intune first, but after that is done then the connector will import these devices into 4me via the Intune service.
Do you store username and password to access data in Intune	There are no usernames or passwords stored in our system, to access data in Intune the service is asking for a consent that enables a service principal to access Intune with the rights needed to export Intune data.
How can I delete CIs that are imported into 4me using the connector?	At this moment it is not possible to delete CIs in QA or production environments, it is however possible to put a device into a non-active state, so it does not show in the Configuration Items view. You can setup retention policies within 4me for CIs to ensure non-active devices are archived and later trashed.