



Security Removable Media Manager
(secRMM)

Intune Access Control Setup Guide

Version 9.11.27.0

(April 2024)

Protect your valuable data



secRMM Intune Access Control Setup Guide

© 2011 Squadra Technologies, LLC. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Squadra Technologies, LLC.

If you have any questions regarding your potential use of this material, contact:

Squadra Technologies, LLC
7575 West Washington Ave
Suite 127-252
Las Vegas, NV 89128 USA
www.squadratechnologies.com
email: info@squadratechnologies.com

Refer to our Web site for regional and international office information.

TRADEMARKS

Squadra Technologies, secRMM are trademarks and registered trademarks of Squadra Technologies, LLC. Other trademarks and registered trademarks used in this guide are property of their respective owners.

Disclaimer

The information in this document is provided in connection with Squadra Technologies products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Squadra Technologies products. EXCEPT AS SET FORTH IN Squadra Technologies's TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, Squadra Technologies ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL Squadra Technologies BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF Squadra Technologies HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Squadra Technologies makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Squadra Technologies does not make any commitment to update the information contained in this document.

Squadra Technologies Administrator Guide
Created - March 2011

Contents

- INTRODUCTION4
- PREREQUISITES.....4
- SETUP OVERVIEW.....5
- SETUP DETAILS5
 - Setup an Azure “application”5
 - Login to your Azure tenant 5
 - Create Azure Application 5
 - Delegated permission (userid/password) 7
 - DeviceManagementManagedDevices.Read.All permission11
 - User.Read.All permission.....15
 - Application.Read.All permission18
 - Application permission (client secret)22
 - DeviceManagementManagedDevices.Read.All permission24
 - User.Read.All permission.....27
 - Application.Read.All permission30
 - Updating the Manifest.....35
 - CONFIGURE SECRMM TO GET MOBILE DEVICE STATE38
 - Delegated permission (userid/password)39
 - Application permission (client secret)39
 - TEST THE CONFIGURATION40
- EVENT DATA.....41
- CONTACTING SQUADRA TECHNOLOGIES SUPPORT43
- ABOUT SQUADRA TECHNOLOGIES, LLC.43

Introduction

Squadra Technologies *security Removable Media Manager* (**secRMM**) software is Windows security software that runs on your company's workstations and servers. secRMM manages and monitors removable media. In this context, Removable media is defined as external hard disks, USB (flash) drives, smart phones, tablets, SD-Cards, CD-ROM and DVD. Such devices typically use the computers Universal Serial Bus (USB) ports to connect to the computer. Removable media devices are popular because they are very convenient when you want to copy files around or backup data. secRMM allows you to track all write activity to the removable media devices in your computer environment as well as giving you the ability to control (or authorize) who can write to the removable media devices.

This document is focused on removable media that is contained within mobile devices (either the devices flash storage or an SD-card). Mobile devices are so popular now that there are many software products which help organizations manage how mobile devices are used within the work place. These software products are called/categorized as "Mobile Device Management" (MDM) products. Microsoft has a MDM product named Intune that runs in the Microsoft cloud. Microsofts cloud is named Azure. All of the MDM products focus on security.

Unfortunately, when it comes to connecting the mobile device over a USB cable, the MDM products either allow or disallow a USB connection (i.e. either on or off). This is a sub-optimal solution for two reasons:

1. The device must be enrolled in the MDM to enforce this rule (i.e. either USB allowed or disallowed). This is roughly analogous to saying that police officers can catch all criminals but only if the criminals first go to the police station to get finger-printed. Otherwise it is not possible to catch them.
2. A rule that only enforces allowed or disallowed is on the one hand (allowed) too relaxed and on the other hand (disallowed) too restrictive. The right solution is to have policy such as secRMM to control read, write and who can have this access, from where they can copy data from, etc.

secRMM can be configured to use the mobile device definitions in Microsoft Intune to decide if a mobile device can be used over the USB connection. A mobile device can be used over a USB connection to transfer files to and from the mobile device to the Windows Desktop computer it is connected to (over the USB cable). You can configure secRMM to check if the mobile device is simply enrolled in Intune or that the device's state (within the MDM) must be "compliant" before it can be used over the USB connection. Whether or not a mobile device is compliant is defined by the organization configuring the MDM and the devices within the MDM. An example would be that a device is compliant if the organizations apps were installed on the device.

If the functionality in the paragraph above is a desirable feature for your environment, this document will help you setup this secRMM feature.

Prerequisites

You will need to have a licensed Intune instance in Azure. By default, this also means you will have an "Azure Active Directory" (AAD) instance. Both Intune and AAD are defined within your Azure tenant. A tenant is a Microsoft term that can be thought of as a container that holds services, programs, device

secRMM Intune Access Control Setup Guide

definitions, data and virtual computers in the cloud that your company can access. Each tenant within Azure has a unique id (Microsoft calls this the “tenant id” and “directory id”).

Setup overview

Here are the high-level steps we will take to setup the secRMM connection to your Azure tenant (i.e. AAD and Intune).

1. Setup an Azure application
2. Configure secRMM to get mobile device state from Intune via the Azure application

Setup details

Setup an Azure “application”

Of course, Microsoft does not allow external programs access to your Azure tenant by default. If you want to allow a program access to the services (i.e. Intune) within your Azure tenant, you must define an “application” within your Azure tenant (via your AAD). The external program must go through these Azure applications to access the services and data within Azure. These Azure applications are really nothing more than a collection of security settings that tell Azure what parts of Azure the external program can access. This document will walk you through the process of setting up the application so you really do not need to have a deep understanding of the whys and hows. Once you follow the steps, the end result will be that secRMM can access the mobile device data in your AAD and Intune so that secRMM can make the decision about mounting your mobile devices over USB connections based on your Azure tenant data.

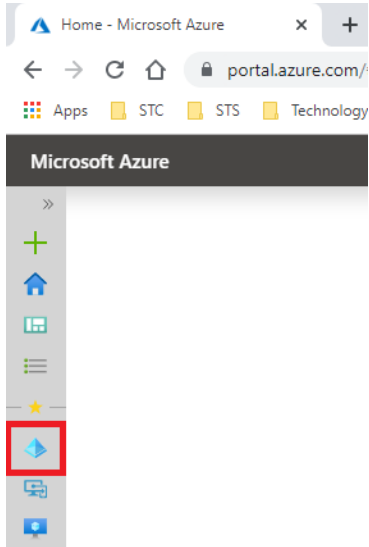
Login to your Azure tenant

Using a web browser, go to URL <https://portal.azure.com>. You will need to supply your Azure userid and password. The userid you use must be defined as the Azure Global Administrator account. Azure Global Administrators are the only userids that can define Azure applications.

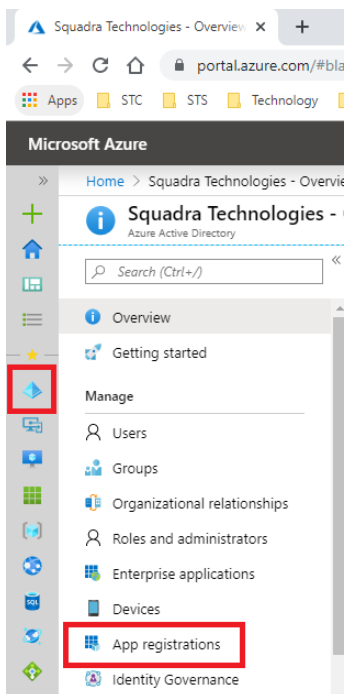
Create Azure Application

Once you are logged in, you will be at your Azure tenant Dashboard.
On the left hand side of the web page, find and select “**Azure Active Directory**”.

secRMM Intune Access Control Setup Guide

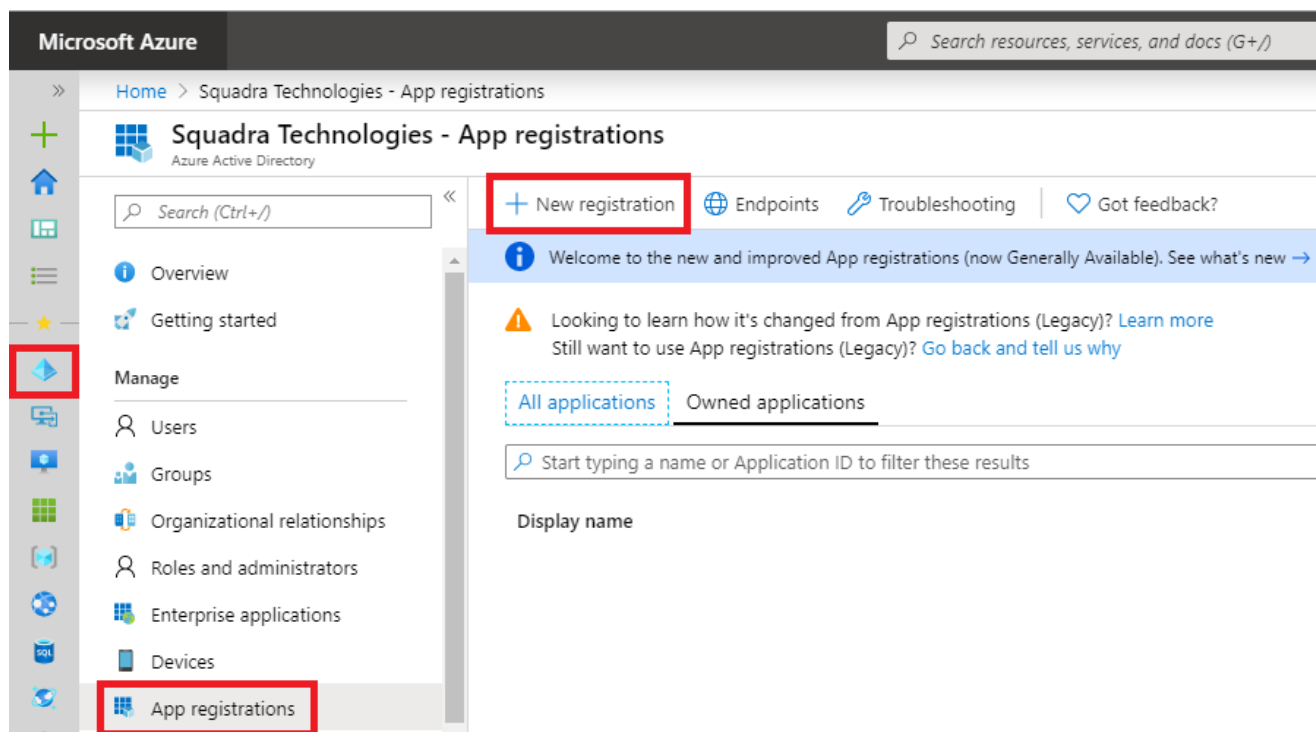


A new column will appear just to the right of the Dashboard column. In the new column, select "**App registrations**".



A new page will appear just to the right of the "App registrations" column. In the new page, at the top, select "**New application registration**".

secRMM Intune Access Control Setup Guide



The next two sections show 2 different Azure “application” setups:



1. Delegated permission (userid/password)
2. Application permission (client secret)

You only need to configure (follow) one of the Azure “application” setups.




If you do not have a preference, then you should choose the “Application permission (client secret)” setup. Also, if your environment requires multifactor authentication for users, then you **MUST** use the “Application permission (client secret)” setup since the “Delegated permission (userid/password)” cannot support multifactor authentication.


Delegated permission (userid/password)


secRMM Intune Access Control Setup Guide


 **secRMMIntuneApp_Delegated** 

<<


 Delete  Endpoints  Preview features


 Overview


 Quickstart


 Integration assistant


Manage


 Branding


 Authentication


 Certificates & secrets


 Token configuration


 API permissions

 Expose an API


 App roles | Preview


 Owners

 Roles and administrators | Preview

 Manifest

Support + Troubleshooting

 Troubleshooting

 New support request


Essentials


Display name : **secRMMIntuneApp_Delegated**

Application (client) ID : c5c492e1-6981-4eb2-98d0-21e6a3c8e910


Directory (tenant) ID : 805a3915-a0ac-4d2a-9ec8-4bb702169c30

Object ID : fbd45900-2b15-4321-83f9-57bee1167b0a

 Welcome to the new and improved App registrations. Looking to learn how it's changed?

 Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory. Applications will need to be upgraded to Microsoft Entra ID.

Call APIs



Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

View API permissions

secRMM Intune Access Control Setup Guide

secRMMIntuneApp_Delegated | API permissions

Search (Ctrl+/) << Refresh Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

✓ Grant admin consent for Squadra Technologies

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Squadra Technologies > secRMMIntuneApp_Delegated

secRMMIntuneApp_Delegated | API permissions

Search (Ctrl+/) << Refresh Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles | Preview

Owners

Roles and administrators | Previ...

Manifest

Configured permissions

Applications are authorized to call APIs when they are granted permissions include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

✓ Grant admin consent for Squadra Technologies

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

Request API permissions

Select an API

Microsoft APIs

APIs my organization uses

My APIs

Commonly used Microsoft APIs



Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and a single endpoint.



Azure DevOps

Integrate with Azure DevOps and Azure DevOps server



Azure Rights Management Services

Allow validated users to read and write protected content



Azure Security

Programmatic access to functionality available via portal



Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data



Dynamics 365 Business Central

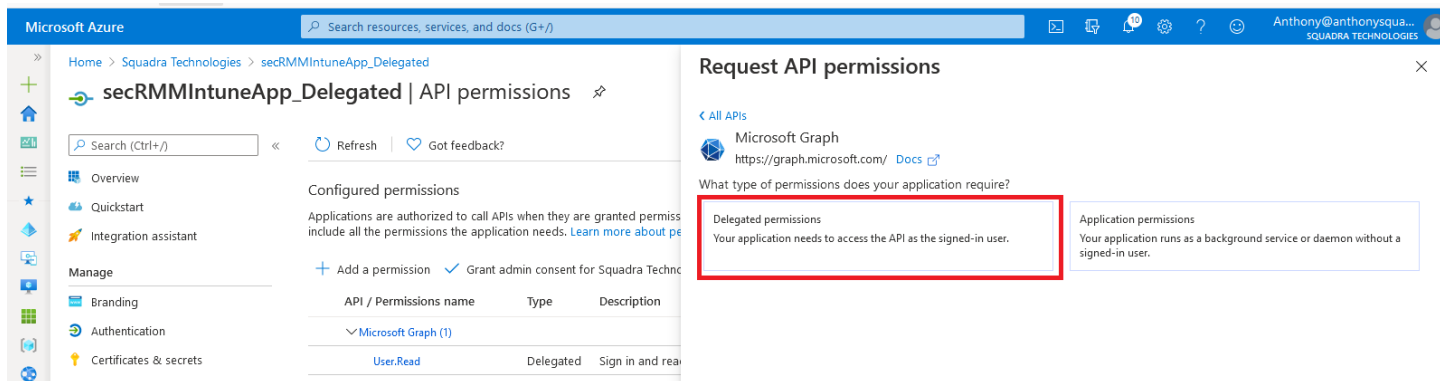
Programmatic access to data and functionality in Dynamics 365 Business Central



Intune

Programmatic access to functionality available via portal

secRMM Intune Access Control Setup Guide



DeviceManagementManagedDevices.Read.All permission

Select the "DeviceManagementManagedDevices.Read.All" permission and then click the "Add permissions" button as shown in the screenshot below.

Request API permissions

[← All APIs](#)



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand](#)

Permission

Admin consent required

✓ DeviceManagementManagedDevices (1)



DeviceManagementManagedDevices.PrivilegedOperations.All ⓘ
Perform user-impacting remote actions on Microsoft Intune devices

Yes



DeviceManagementManagedDevices.Read.All ⓘ
Read Microsoft Intune devices

Yes



DeviceManagementManagedDevices.ReadWrite.All ⓘ
Read and write Microsoft Intune devices

Yes

Add permissions

Discard

You will now be back on the "Configured permissions" page. Click the "Add permission" button again as shown in the screenshot below.

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs



Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure DevOps

Integrate with Azure DevOps and Azure DevOps server



Azure Rights Management Services

Allow validated users to read and write protected content



Azure Service Management

Programmatic access to much of the functionality available through the Azure portal



Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data



Dynamics 365 Business Central

Programmatic access to data and functionality in Dynamics 365 Business Central



Intune

Programmatic access to Intune data

Request API permissions

< All APIs



Microsoft Graph

<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

secRMM Intune Access Control Setup Guide

User.Read.All permission

Select the "User.Read.All" permission and then click the "Add permissions" button as shown in the screenshot below.

Request API permissions

[← All APIs](#)

Microsoft Graph
<https://graph.microsoft.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permission
Your application runs as a signed-in user.

Select permissions

Permission

> IdentityRiskyUser

▼ User (1)

☒ **User.Read.All** ⓘ
Read all users' full profiles

Add permissions Discard

D03052021

You will now be back on the “Configured permissions” page. Click the “Add permission” button again as shown in the screenshot below.

Request API permissions

Select an API

Microsoft APIs

APIs my organization uses

My APIs

Commonly used Microsoft APIs



Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure DevOps

Integrate with Azure DevOps and Azure DevOps server



Azure Rights Management Services

Allow validated users to read and write protected content



Azure Service Management

Programmatic access to much of the functionality available through the Azure portal



Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data



Dynamics 365 Business Central

Programmatic access to data and functionality in Dynamics 365 Business Central



Intune

Programmatic access to Intune data

[Application.Read.All permission](#)

Select the "Application.Read.All" permission and then click the "Add permissions" button as shown in the screenshot below.

Request API permissions

[← All APIs](#)



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as an app, not as a signed-in user.

Select permissions



Application.Read.All



The "Admin consent required" column shows the default value for an organization. However, user or app permissions may vary. This column may not reflect the value in your organization, or in organization. [more](#)

Permission



Application (1)



Application.Read.All ⓘ

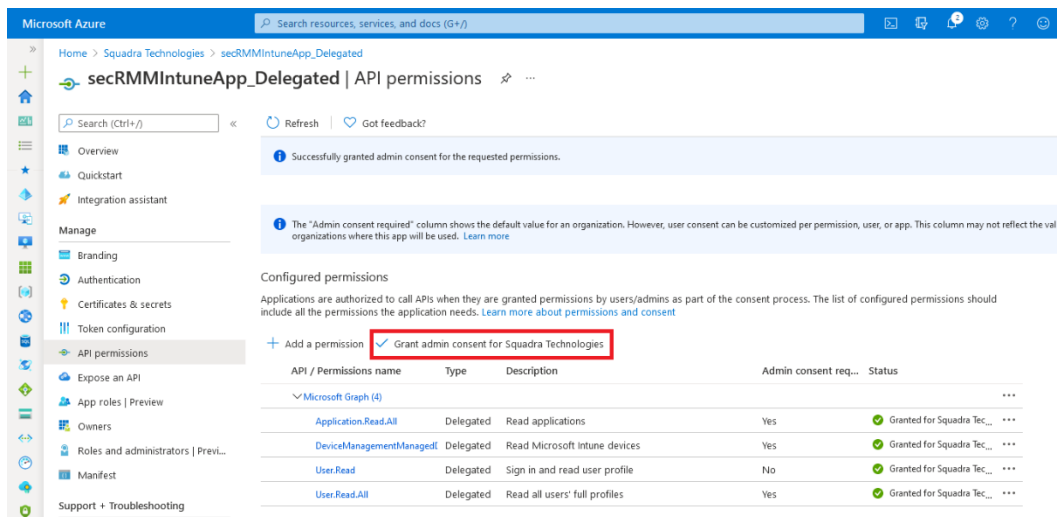
Read applications

Add permissions

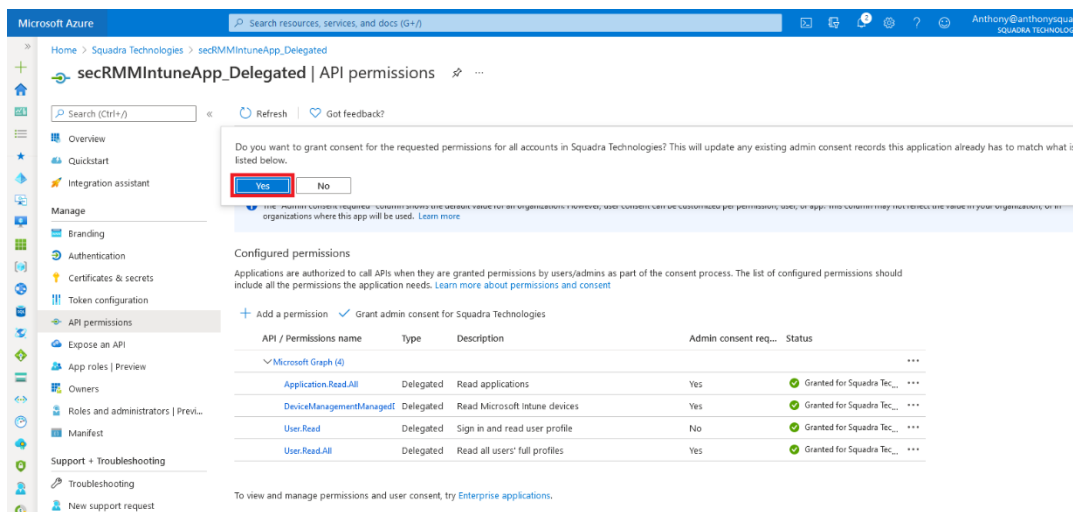
Discard

You will now be back on the "Configured permissions" page. Click the "Grant admin consent" button as shown in the screenshot below.

secRMM Intune Access Control Setup Guide



Click the "Yes" button as shown in the screenshot below.



The permissions will now turn to green icons showing success as shown in the screenshot below.

secRMM Intune Access Control Setup Guide

Microsoft Azure

Home > Squadra Technologies > secRMMIntuneApp_Delegated

secRMMIntuneApp_Delegated | API permissions

Search resources, services, and docs (G+/?)

Grant consent
Grant consent successful

Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)



+ Add a permission ✓ Grant admin consent for Squadra Technologies

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (4)				
Application.Read.All	Delegated	Read applications	Yes	✓ Granted for Squadra Tec... ***
DeviceManagementManaged	Delegated	Read Microsoft Intune devices	Yes	✓ Granted for Squadra Tec... ***
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Squadra Tec... ***
User.Read.All	Delegated	Read all users' full profiles	Yes	✓ Granted for Squadra Tec... ***

Now please go to the section below titled "Updating the Manifest" to complete the setup of the Azure Application.

Page 22

secRMM Intune Access Control Setup Guide

 **secRMMIntuneApp_Application** 

<<

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles | Preview

Owners




Roles and administrators | Previ...

Manifest

Support + Troubleshooting

Troubleshooting

New support request

 Delete  Endpoints  Preview features


^ Essentials


Display name : [secRMMIntuneApp_Application](#)

Application (client) ID : 23767375-7c40-4968-bc0e-9c4fd87c58b7


Directory (tenant) ID : 805a3915-a0ac-4d2a-9ec8-4bb702169c30

Object ID : 4b97f85e-88de-4f61-adde-952ee47d8352

 Welcome to the new and improved App registrations. Looking to learn how it's char

 Starting June 30th, 2020 we will no longer add any new features to Azure Active Direc no longer provide feature updates. Applications will need to be upgraded to Microsc

Call APIs



Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API permissions](#)

secRMM Intune Access Control Setup Guide

secRMMIntuneApp_Application | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage Branding Authentication Certificates & secrets Token configuration

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins to include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Squadra Technologies

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

Microsoft Azure Search resources, services, and docs (G+)

Home > Squadra Technologies > secRMMIntuneApp_Application

secRMMIntuneApp_Application | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage Branding Authentication Certificates & secrets Token configuration API permissions

Expose an API App roles | Preview Owners Roles and administrators | Preview Manifest

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more with a single endpoint.

Azure DevOps Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services Allow validated users to read and write protected content

Azure Service Bus Programmatic access to functionality available via portal

Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Dynamics 365 Business Central Programmatic access to data and functionality in Dynamics 365 Business Central

Intune Programmatic access to functionality available via portal

Microsoft Azure Search resources, services, and docs (G+)

Home > Squadra Technologies > secRMMIntuneApp_Application

secRMMIntuneApp_Application | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage Branding Authentication Certificates & secrets Token configuration API permissions

Expose an API App roles | Preview Owners Roles and administrators | Preview Manifest

Request API permissions

< All APIs

Microsoft Graph <https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions Your application needs to access the API as the signed-in user.

Application permissions Your application runs as a background service or daemon without a signed-in user.

DeviceManagementManagedDevices.Read.All permission

Select the "DeviceManagementManagedDevices.Read.All" permission and then click the "Add permissions" button as shown in the screenshot below.

secRMM Intune Access Control Setup Guide

Request API permissions



< All APIs



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand](#)



devicemanagementmanageddevices

Permission

Admin consent required

✓ DeviceManagementManagedDevices (1)



DeviceManagementManagedDevices.PrivilegedOperations.All ⓘ
Perform user-impacting remote actions on Microsoft Intune devices

Yes



DeviceManagementManagedDevices.Read.All ⓘ
Read Microsoft Intune devices

Yes



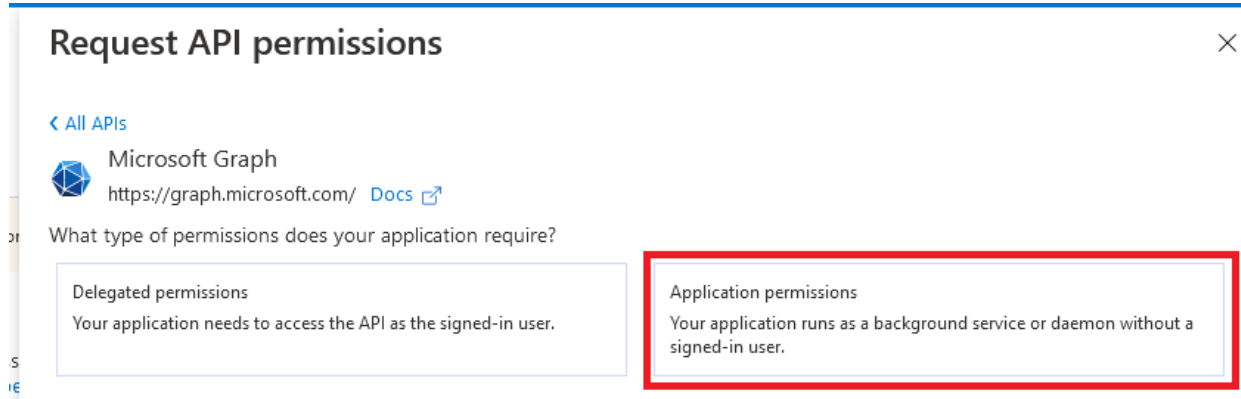
DeviceManagementManagedDevices.ReadWrite.All ⓘ
Read and write Microsoft Intune devices

Yes

Add permissions

Discard

You will now be back on the "Configured permissions" page. Click the "Add permission" button again as shown in the screenshot below.



User.Read.All permission

Select the "User.Read.All" permission and then click the "Add permissions" button as shown in the screenshot below.

Request API permissions

[← All APIs](#)



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service and needs to access the API on behalf of signed-in user.

Select permissions

Permission

Admin cons



IdentityRiskyUser



User (1)



User.Read.All ⓘ

Read all users' full profiles

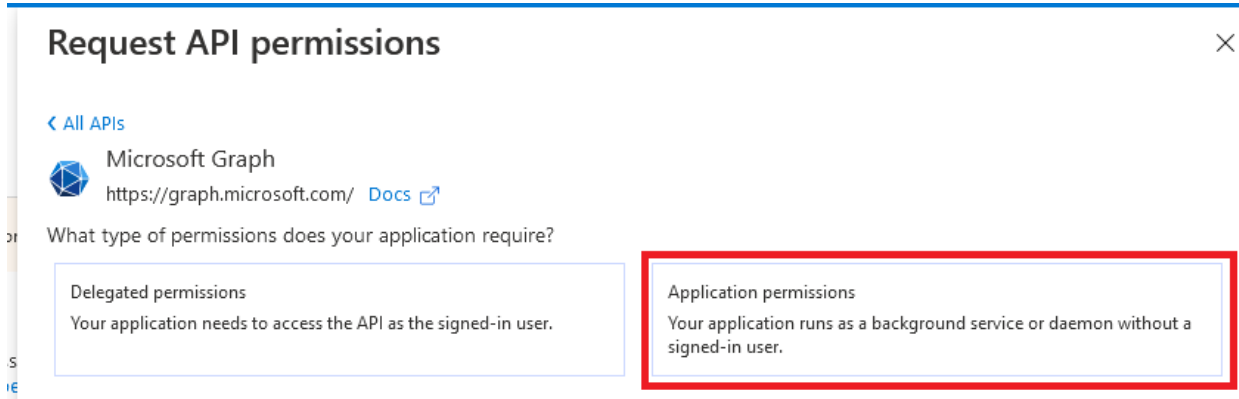
Yes

Add permissions

Discard

D03052021

[illegible]



Application.Read.All permission

Select the "Application.Read.All" permission and then click the "Add permissions" button as shown in the screenshot below.

Request API permissions



[← All APIs](#)



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

<input type="text" value="Application.Read.All"/>	
Permission	Admin consent required
Application (1)	
<input checked="" type="checkbox"/>	<div>Application.Read.All ⓘ Read all applications</div> Yes

Add permissions

Discard

You will now be back on the "Configured permissions" page. Click the "Grant admin consent" button as shown in the screenshot below.

secRMM Intune Access Control Setup Guide

secRMMIntuneApp_Application | API permissions

Search (Ctrl+F) Refresh Got feedback?

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ☒ Grant admin consent for Squadra Technologies

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (4)				
Application.Read.All	Application	Read all applications	Yes	Not granted for Squadra Tec...
DeviceManagementManaged...	Application	Read Microsoft Intune devices	Yes	Granted for Squadra Tec...
User.Read	Delegated	Sign in and read user profile	No	Granted for Squadra Tec...
User.Read.All	Application	Read all users' full profiles	Yes	Granted for Squadra Tec...

To view and manage permissions and user consent for this application, see [Manage permissions](#).

Click the "Yes" button as shown in the screenshot below.

secRMMIntuneApp_Application | API permissions

Search (Ctrl+F) Refresh Got feedback?

Do you want to grant consent for the requested permissions for all accounts in Squadra Technologies? This will update any existing admin consent records this application already has to match what is listed below.

[Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ☒ Grant admin consent for Squadra Technologies

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (4)				
Application.Read.All	Application	Read all applications	Yes	Not granted for Squadra Tec...
DeviceManagementManaged...	Application	Read Microsoft Intune devices	Yes	Granted for Squadra Tec...
User.Read	Delegated	Sign in and read user profile	No	Granted for Squadra Tec...
User.Read.All	Application	Read all users' full profiles	Yes	Granted for Squadra Tec...

The permissions will now turn to green icons showing success as shown in the screenshot below.

Home > Squadra Technologies > secRMMIntuneApp_Application

secRMMIntuneApp_Application | API permissions

Search (Ctrl+F) Refresh Got feedback?

Grant consent successful

Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ☒ Grant admin consent for Squadra Technologies

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (4)				
Application.Read.All	Application	Read all applications	Yes	Granted for Squadra Tec...
DeviceManagementManaged...	Application	Read Microsoft Intune devices	Yes	Granted for Squadra Tec...
User.Read	Delegated	Sign in and read user profile	No	Granted for Squadra Tec...
User.Read.All	Application	Read all users' full profiles	Yes	Granted for Squadra Tec...

Now click the "Certificates & Secrets" as shown in the screenshot below.

secRMM Intune Access Control Setup Guide

Microsoft Azure

Search resources, services, and docs (G+)

Home > Squadra Technologies >

secRMMIntuneApp_Application

Search (Ctrl+)

Delete Endpoints Preview features

Essentials

Display name : secRMMIntuneApp_Application

Application (client) ID : 23767375-7c40-4968-bc0e-9c4fd87c58b7

Directory (tenant) ID : 805a3915-a0ac-4d2a-9ec8-4bb702169c30

Object ID : 4b97f85e-88de-4f61-adde-952ee47d8352

Starting June 30th, 2020 we will no longer add any new features to Az no longer provide feature updates. Applications will need to be upgr

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.


View API permissions

Certificates & secrets

- Overview
- Quickstart
- Integration assistant
- Branding
- Authentication
- Token configuration
- API permissions
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Previ...
- Manifest
- Troubleshooting

Scroll down a bit on the page and select "New client secret" as shown in the screenshot below.

secRMM Intune Access Control Setup Guide

 Got feedback?

Thumbprint	Start date	Expires	ID
------------	------------	---------	----

No certificates have been added for this application.

Client secrets

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


 New client secret

Description	Expires	Value	ID
-------------	---------	-------	----

No client secrets have been created for this application.

Fill in the "client secret" information as shown in the screenshot below. Note the the description is free form and you are free to choose when the client secret will expire (based on your environment).

| Certificates & secrets

 Got feedback?

Add a client secret

Description

secRMMIntuneAppClientSecret

Expires

- ☐ In 1 year
☐ In 2 years
☒ Never

Add

Cancel

secRMM Intune Access Control Setup Guide

The “client secret” will be generated. You will need to take the Value as shown in the screenshot below. The value will need to be copied into the secRMM property. This is shown later in this document in the section named “Configure secRMM to get mobile device state”. You must copy this value now because once you go off the page, the value will not be displayed again. If you forget to copy the value, just delete the old secret and create a new one.

Client secrets

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

[+ New client secret](#)

Description	Expires	Value	ID
secRMMIntuneAppClientS...	12/31/2299	<div>~srF.N6CRw2g-XHJL22-Fj..</div>	<div>8e192a33-eb34-46eb-84 ...</div>

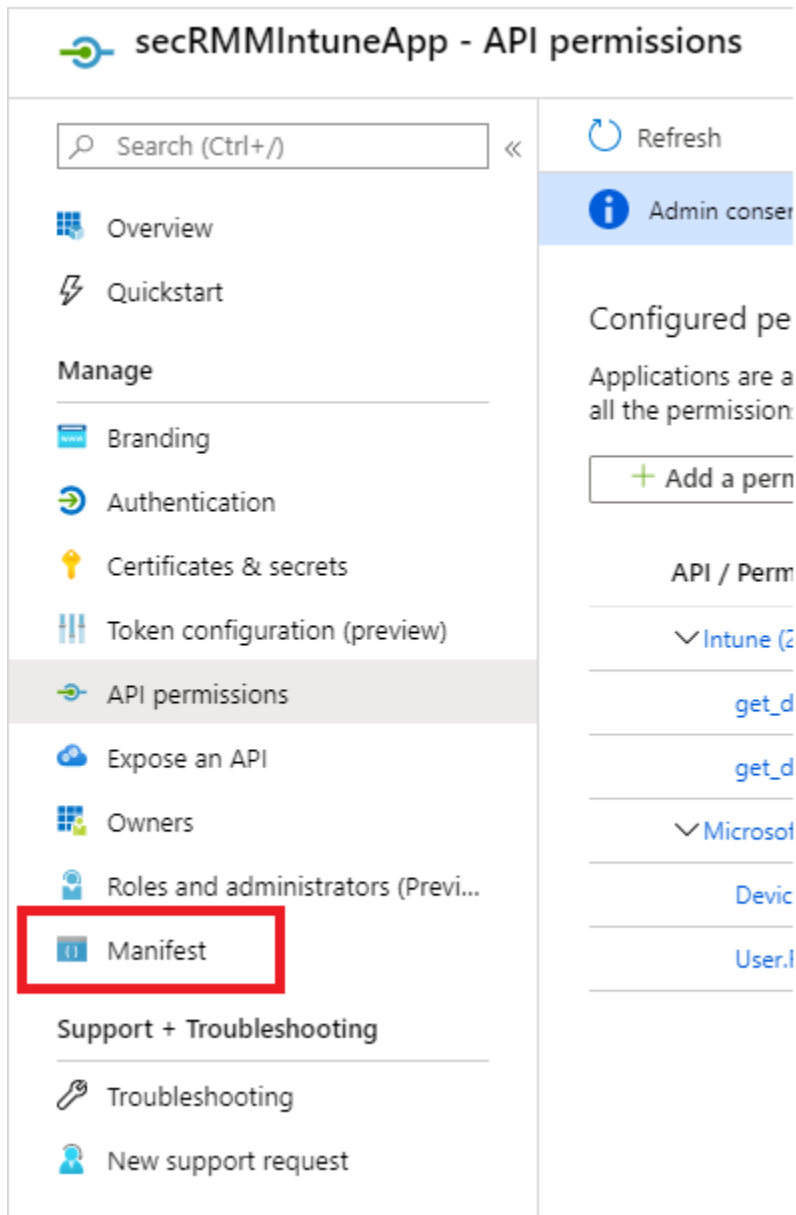
Now please go to the section below titled “Updating the Manifest” to complete the setup of the Azure Application.

Updating the Manifest

Whether you chose to use the “Delegated permission” (Azure userid and password) or “Application permission” (“application secret”), you need to update the Azure Application “Manifest” as described below.

Click the “Manifest” button on the left side of the page as shown in the screenshot below.

secRMM Intune Access Control Setup Guide



Change the word "null" on the line with "allowPublicClient" to "true" as shown in the screenshots below.

secRMM Intune Access Control Setup Guide

 Save  Discard  Upload  Download

The editor below allows you to update this application by directly modifying its JSON representation.

```
1 {  
2   "id": "38d3d160-824e-4d9a-9141-61e7e966fd6e",  
3   "acceptMappedClaims": null,  
4   "accessTokenAcceptedVersion": null,  
5   "addIns": [],  
6   "allowPublicClient": null,  
7   "appId": "5a8b3630-4a06-45c6-b229-b80d9ba8ec6f",  
8   "appRoles": [],
```

 Save  Discard  Upload  Download

The editor below allows you to update this application by directly modifying its JSON representation. details, see: [Understanding the Azure Active Directory application manifest](#).

```
1 {  
2   "id": "38d3d160-824e-4d9a-9141-61e7e966fd6e",  
3   "acceptMappedClaims": null,  
4   "accessTokenAcceptedVersion": null,  
5   "addIns": [],  
6   "allowPublicClient": true,  
7   "appId": "5a8b3630-4a06-45c6-b229-b80d9ba8ec6f",  
8   "appRoles": [],
```

Click the "Save" button as shown in the screenshot below.

 Save  Discard  Upload  Download

The editor below allows you to update this application by directly modifying its JSON representation. details, see: [Understanding the Azure Active Directory application manifest](#).

```
1 {  
2   "id": "38d3d160-824e-4d9a-9141-61e7e966fd6e",  
3   "acceptMappedClaims": null,  
4   "accessTokenAcceptedVersion": null,  
5   "addIns": [],  
6   "allowPublicClient": true,  
7   "appId": "5a8b3630-4a06-45c6-b229-b80d9ba8ec6f",
```

secRMM Intune Access Control Setup Guide

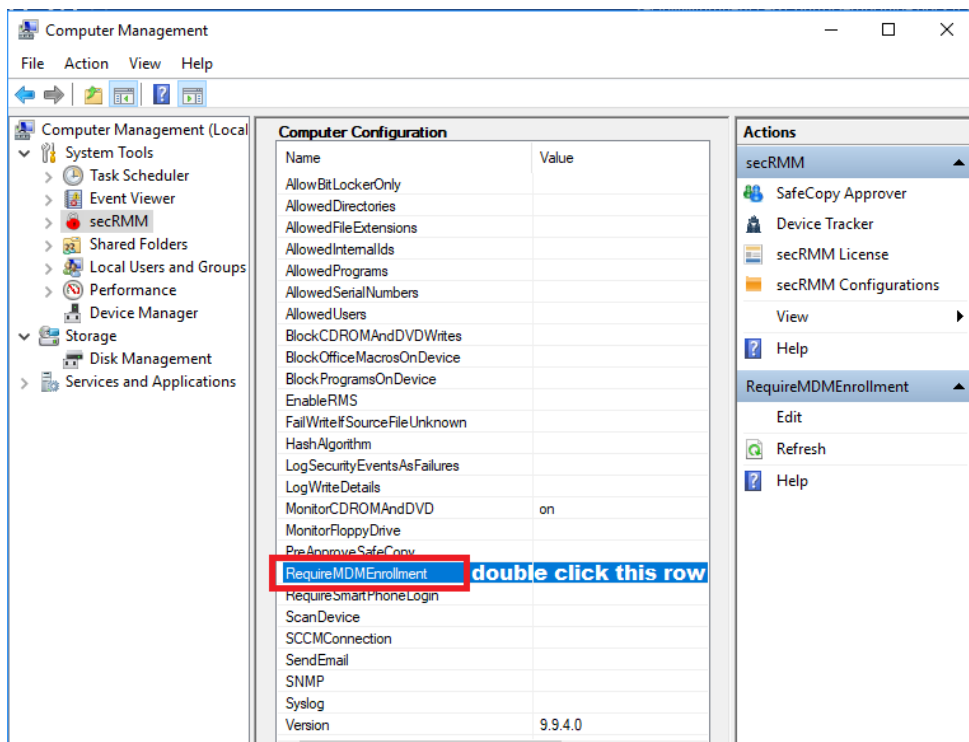
Note that if you do not change the "allowPublicClient" to "true" in the Manifest, when you do a "Test Connection" in the secRMM console, you will get the error:

Error: AADSTS700218: The request body must contain the following parameter: 'client_assertion' or 'client_secret'.

Configure secRMM to get mobile device state

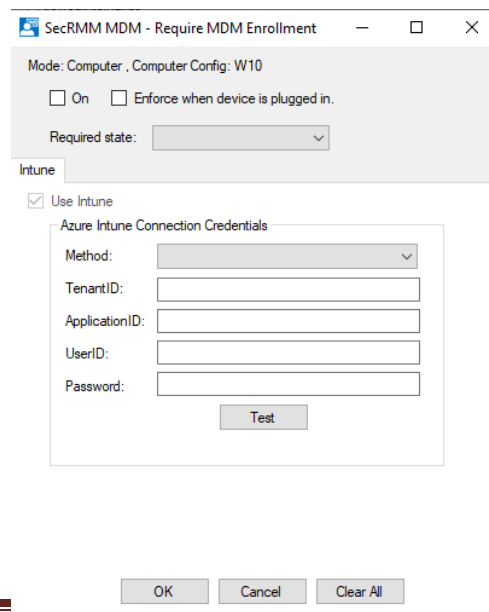
Now that we have setup where secRMM will get the mobile device state, we will give secRMM the information about how to get the mobile device state data. secRMM can be centrally managed with either System Center Configuration Manager (SCCM) or Azure Intune or Active Directory Group Policy Objects (AD GPO). You can also individually manage a single computer using the Windows "Computer Management" MMC interface (a good tool when you are testing...before you deploy a policy to your entire environment).

Regardless of which interface you use to configure secRMM, there is a secRMM property named "RequireMDMEnrollment". Double



click the "RequireMDMEnrollment" row to open the window that lets you configure the Intune connection. As you can see in the screenshot, there are several options available to you. We will break down each option below.

The first checkbox (labeled "On") is required to be checked. It is here to be consistent with all of the other secRMM on/off properties. The second checkbox (labeled "Enforce when device is plugged in.") will make secRMM communicate with Intune as soon as the end-user connects the mobile device using the USB cable. If you do not check this checkbox, secRMM will enforce the rule when an end-user tries to transfer a file to the mobile device. Next, is the drop-down listbox (labeled "Required state"). There are two options: Enrolled and Compliant. This tells secRMM what state is required to allow the mobile device to be used over a USB connection. The compliant state is the most strict since the mobile device must be both enrolled and compliant at the same time. It is not possible for the device to be compliant if it is not enrolled.



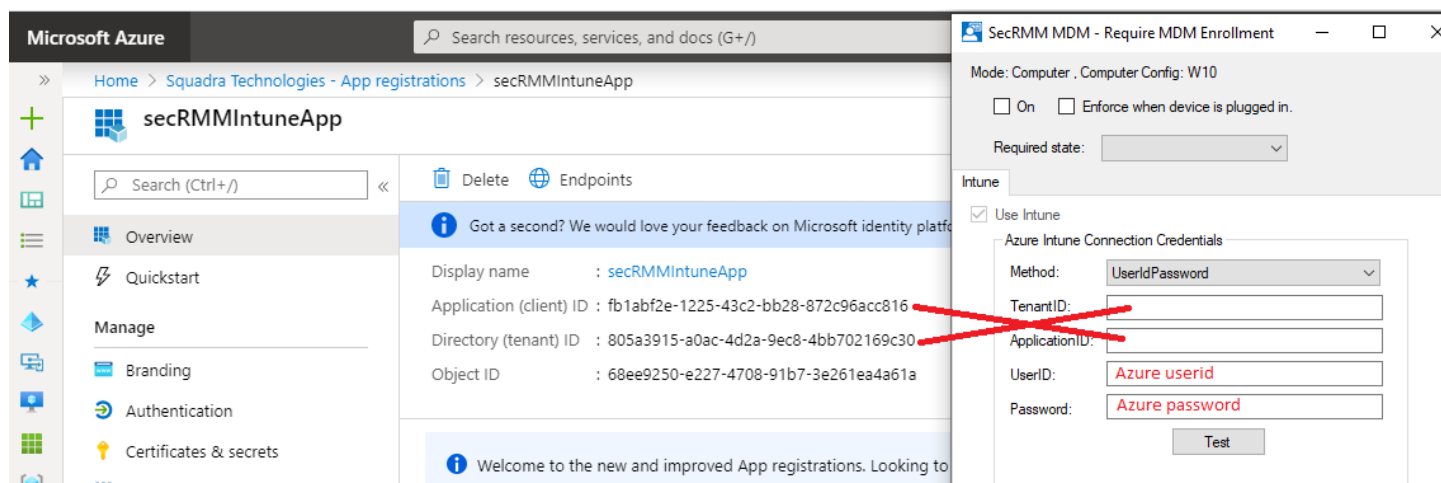
secRMM Intune Access Control Setup Guide

Next, you need to specify the "Azure Intune Connection Credentials" Method.

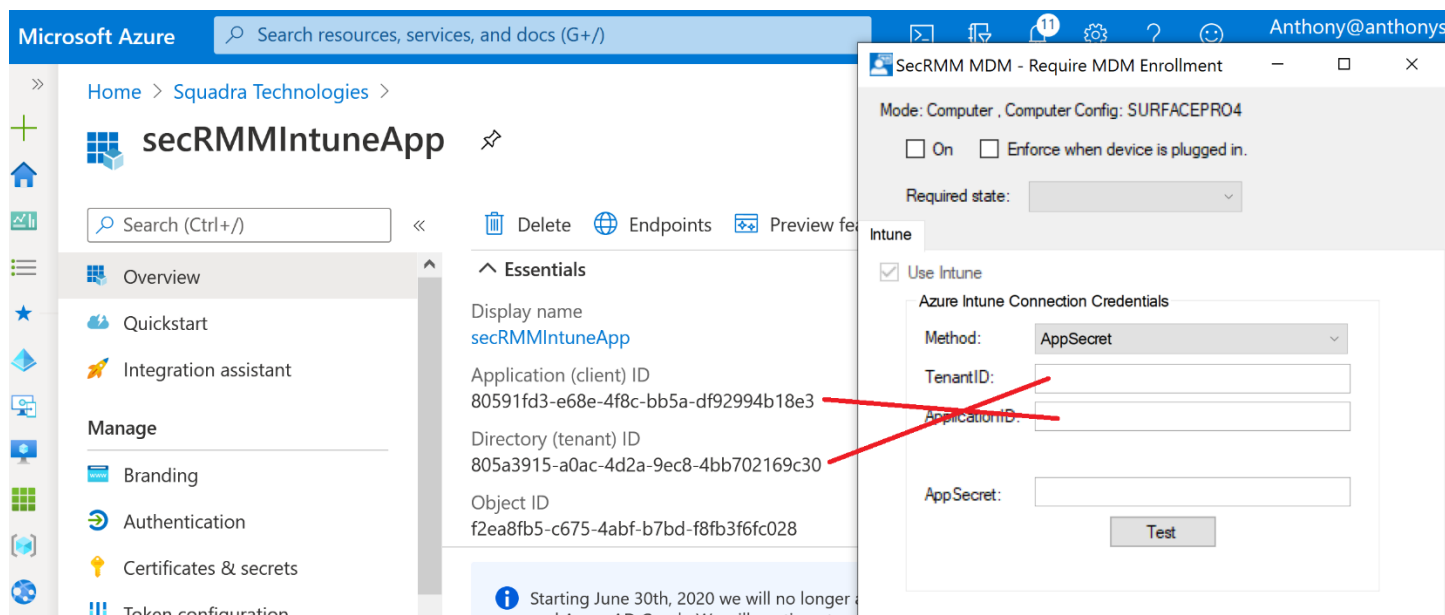
Select the "UserIdPassword" method if you configured the Azure application permission for "Delegation".
Select the "AppSecret" method if you configured the Azure application permission for "Application".

Both methods are shown in the screenshots below.

Delegated permission (userid/password)



Application permission (client secret)



secRMM Intune Access Control Setup Guide

Microsoft Azure | Search resources, services, and docs (G+)

Home > Squadra Technologies > secRMMIntuneApp

secRMMIntuneApp | Certificates & secrets

Search (Ctrl+/)

Got feedback?

upload certificate

Thumbprint Start date

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity password.

+ New client secret

Description	Expires	Value	ID
secRMMIntuneAppClientS...	12/31/2299	~srF.N6CRw2g-XHJL22-F...	8e192a33-eb34-46eb-84...

Intune

☐ On ☐ Enforce when device is plugged in.

Required state: [v]

☒ Use Intune

Azure Intune Connection Credentials

Method: AppSecret [v]

TenantID: []

ApplicationID: []

AppSecret: Azure client secret []

Test

OK Cancel Clear All

Test the configuration

Once you have all the required properties filled in, click the "Test" button to make sure the connection succeeds. A success message will look like the screenshot below. If the test is unsuccessful, you can look in "C:\Program Files\secRMM\AdminUtils\MDM\Intune\secRMMMDMIntune.log for trace where you can see the detailed errors.

secRMM Intune Access Control Setup Guide

The image displays two side-by-side screenshots of the "SecRMM MDM - Require MDM Enrollment" dialog box, followed by a "Microsoft Intune connection test" dialog box.

Left Screenshot (W10 Configuration):

- Mode: Computer , Computer Config: W10
- ☒ On ☐ Enforce when device is plugged in.
- Required state: **Enrolled**
- Intune section:
 - ☒ Use Intune
 - Azure Intune Connection Credentials:
 - Method: **UserIdPassword**
 - TenantID: 805a3915-a0ac-4d2a-9ec8-4bb702169c30
 - ApplicationID: fb1abf2e-1225-43c2-bb28-872c96acc816
 - UserID: anthony@anthonysquadratechnologies.onmicrosoft.com
 - Password: [Redacted]
 - Test** button

Right Screenshot (SURFACEPRO4 Configuration):

- Mode: Computer , Computer Config: SURFACEPRO4
- ☒ On ☐ Enforce when device is plugged in.
- Required state: **Enrolled**
- Intune section:
 - ☒ Use Intune
 - Azure Intune Connection Credentials:
 - Method: **AppSecret**
 - TenantID: 805a3915-a0ac-4d2a-9ec8-4bb702169c30
 - ApplicationID: 80591fd3-e68e-4f8c-bb5a-df92994b18e3
 - AppSecret: [Redacted]
 - Test** button

Microsoft Intune connection test Dialog:

- IntuneGraphApi.TestIntuneConnection: succeeded.
- Intune Authentication Token (first 10 bytes): eyJ0eXAiOi...
- OK** button

Once you have a successful connection, save the secRMM values by clicking the OK button on the "Require MDM Enrollment" dialog.

Event Data

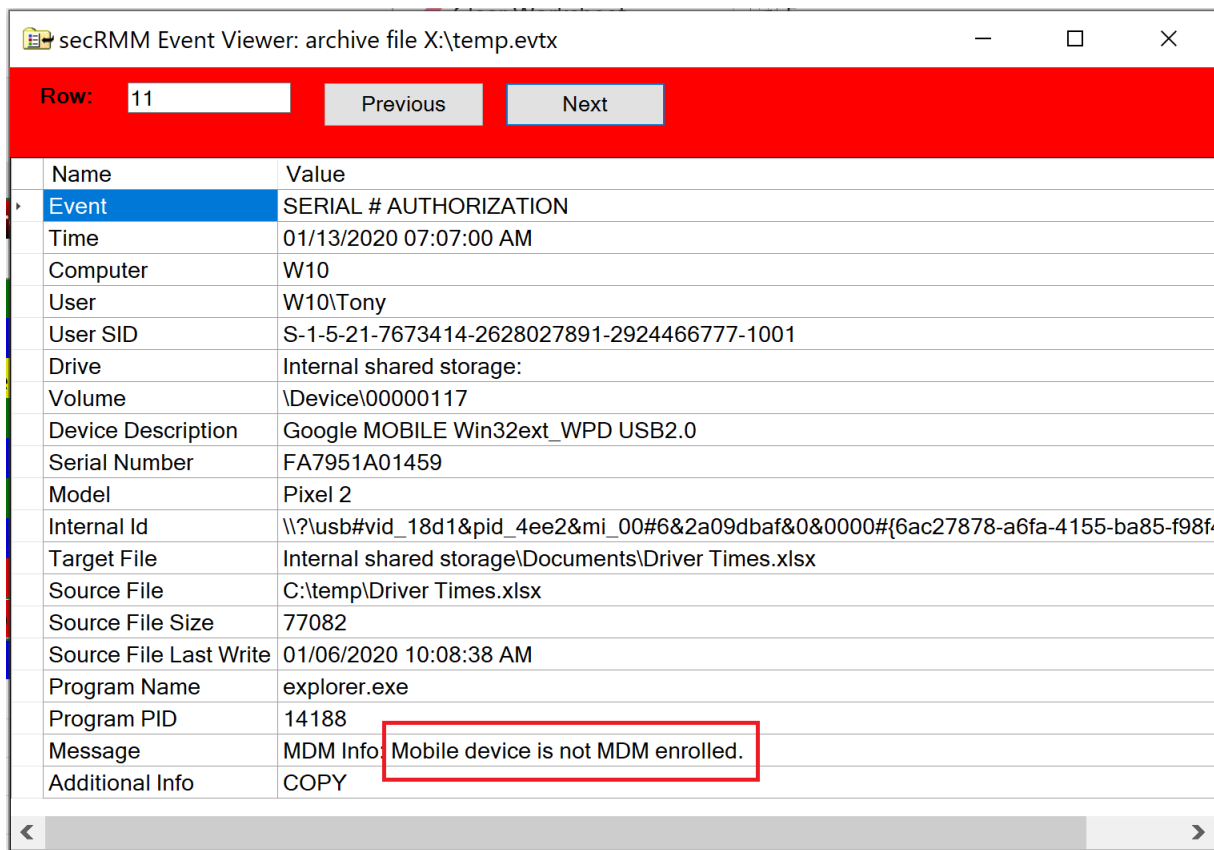
The secRMM event log will collect data from Azure Intune when mobile devices come ONLINE (over a USB connection) as shown in the screenshot below.

secRMM Intune Access Control Setup Guide

secRMM Event Viewer: localhost, event log secRMM		
Row: 3	Previous	Next
	Name	Value
▶	Event	ONLINE
	Time	01/16/2020 03:40:18 PM
	Computer	W10
	User	W10\Tony
	Drive	Internal Storage:
	Volume	\Device\000000f4
	Device Description	Apple Inc. MOBILE Win32ext_WPD USB2.0
	Serial Number	0b1cd80db69b95012d185ae2a284f0db50ac15a0
	Model	Apple iPhone
	Internal Id	\\?\usb\vid_05ac&pid_12a8&mi_00#6&1cbb703&0&0000#{6ac27878-a6fa-4155-ba85-f98f491d4f33}
	Additional Info	SerialNumber=F17STK9XH7K, BluetoothAddress=d0:c5f3:31:59:b0, EthernetAddress=d0:c5f3:31:59:b1, WiFiAddress=d0:c5f3:31:59:af,
		//===Intune Data===
		{"@odata.context":"https://graph.microsoft.com/v1.0/\$metadata#deviceManagement/managedDevices"
		"@odata.count":1
		"value":[{"id":"e22e4b92-bec0-4de8-8911-84d395e76a40"
		"userId":"7fa4323-1e8c-45af-a826-655b4a85fe7b"
		"deviceName":"Anthony LaMark\u2019s iPhone"
		"managedDeviceOwnerType":"personal"
		"enrolledDateTime":"2019-11-21T17:58:33Z"
		"lastSyncDateTime":"2020-01-16T17:20:31Z"
		"operatingSystem":"iOS"
		"complianceState":"compliant"

Below is a screenshot of an end-user trying to copy a file (but the file copy was unsuccessful) to the mobile device over a USB connection where the mobile device was not Intune enrolled.

secRMM Intune Access Control Setup Guide



secRMM Event Viewer: archive file X:\temp.evtx

Row: 11 Previous Next

Name	Value
Event	SERIAL # AUTHORIZATION
Time	01/13/2020 07:07:00 AM
Computer	W10
User	W10\Tony
User SID	S-1-5-21-7673414-2628027891-2924466777-1001
Drive	Internal shared storage:
Volume	\Device\00000117
Device Description	Google MOBILE Win32ext_WPD USB2.0
Serial Number	FA7951A01459
Model	Pixel 2
Internal Id	\\?\usb#vid_18d1&pid_4ee2&mi_00#6&2a09dbaf&0&0000#{6ac27878-a6fa-4155-ba85-f98f}
Target File	Internal shared storage\Documents\Driver Times.xlsx
Source File	C:\temp\Driver Times.xlsx
Source File Size	77082
Source File Last Write	01/06/2020 10:08:38 AM
Program Name	explorer.exe
Program PID	14188
Message	MDM Info: Mobile device is not MDM enrolled.
Additional Info	COPY

Contacting Squadra Technologies Support

Squadra Technologies Support is available to customers who have purchased a commercial version of secRMM and have a valid maintenance contract or who are in a trial mode of the product.

When you contact Support please include the following information:

1. The version of secRMM you have installed.
2. The Windows versions you have installed: XP, 2003 Server, 2008 Server R2, Vista, Windows 7, etc.
3. Whether the Windows Operating System is 32bit or 64bit.
4. The specific issue you are contacting support for.

About Squadra Technologies, LLC.

Squadra Technologies delivers innovative products that help organizations get more data protection within the computer infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Squadra Technologies is helping customers worldwide.

Contacting Squadra Technologies, LLC.

Phone 562.221.3079 (United States and Canada)

secRMM Intune Access Control Setup Guide

Email info@squadratechnologies.com

Mail Squadra Technologies, LLC.
 World Headquarters
 7575 West Washington Ave. Suite 127-252
 Las Vegas, NV 89128
 USA

Web site <http://www.squadratechnologies.com/>