



Security Removable Media Manager
(secRMM)

Intune Access Control Setup Guide

Version 9.9.28.0

(November 2020)

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

INTRODUCTION	4
PREREQUISITES	4
SETUP OVERVIEW	5
SETUP DETAILS	5
<i>Setup an Azure “application”</i>	5
Login to your Azure tenant	5
Create Azure Application.....	6
Delegated permission (userid/password)	11
Application permission (client secret).....	16
DeviceManagementManagedDevices.Read.All permission	16
User.Read.All permission.....	18
Updating the Manifest	24
CONFIGURE SECRMM TO GET MOBILE DEVICE STATE	27
Delegated permission (userid/password)	28
Application permission (client secret).....	28
Test the configuration	29
EVENT DATA	30
CONTACTING SQUADRA TECHNOLOGIES SUPPORT	32
ABOUT SQUADRA TECHNOLOGIES, LLC.	32

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) to 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

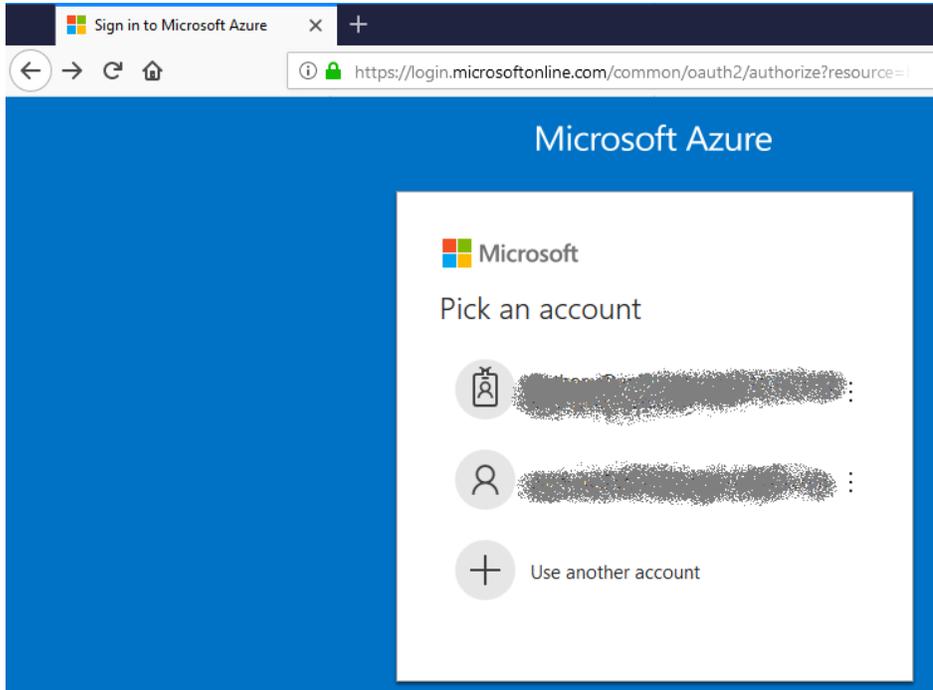
Setup an Azure "application"

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

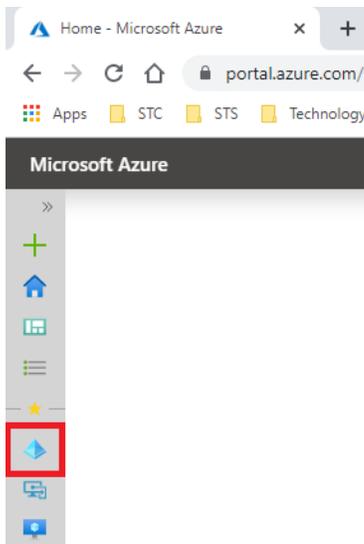
Using a web browser, go to URL <https://portal.azure.com>. You will need to supply your Azure userid and password. The userid you use must be defined as the Azure Global Administrator account. Azure Global Administrators are the only userids that can define Azure applications.

secRMM Intune Access Control Setup Guide



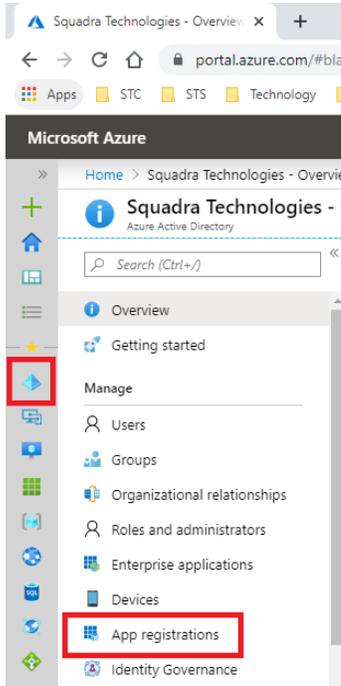
Create Azure Application

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**".

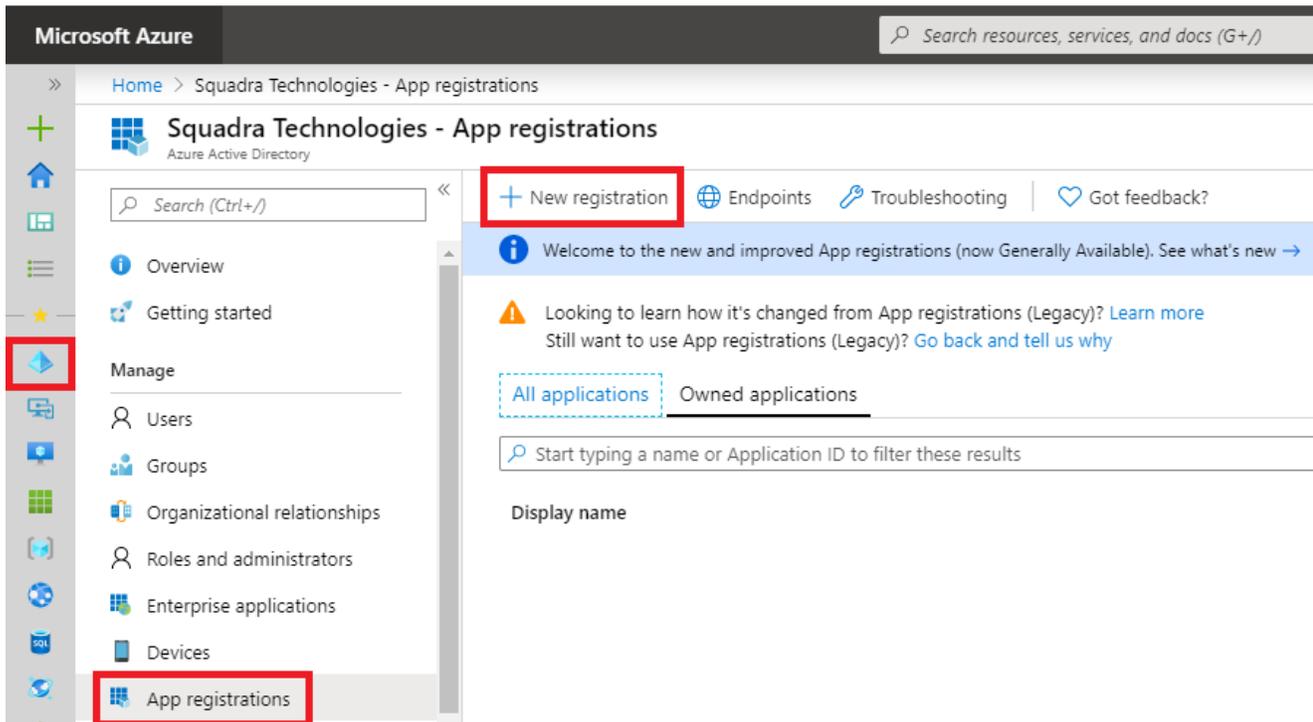


A new column will appear just to the right of the Dashboard column. In the new column, select "**App registrations**".

secRMM Intune Access Control Setup Guide



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**".



A form will appear that wants you to specify the "Application name", "Supported account types" and a "Platform configuration" as shown in the screenshot below. For the "Application name", type **secRMMIntuneApp** (although this is a free form text field and can have any value you want, we recommend you specify secRMMIntuneApp so the documentation below will match your environment).

secRMM Intune Access Control Setup Guide

You do not need to change anything else so now click the **Register** button at the bottom as shown in the screenshot below.

Microsoft Azure Search resources, services, and documentation

Home > Squadra Technologies >

Register an application

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

secRMMIntuneApp

Supported account types
Who can use this application or access this API?

- Accounts in this organizational directory only (Squadra Technologies)
- Accounts in any organizational directory (Any Azure AD directory - My organization)
- Accounts in any organizational directory (Any Azure AD directory - My organization) with administrative consent
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. You can change this value later, but a value is required for most authentication scenarios.

Web ▼

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

Register

secRMM Intune Access Control Setup Guide

Azure AAD will create the application when you click the Register button and will show you the new application as shown in the screenshot below. We will need to use the "Application ID" and "Directory ID" on this screen when we configure secRMM later in this document.

The screenshot shows the Azure AD application registration page for 'secRMMIntuneApp'. The page includes a 'Delete' button and 'Endpoints' link. A blue banner at the top contains a message: 'Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →'. Below this, the application details are listed:

Display name	: secRMMIntuneApp	Supported account types	: My organization only
Application (client) ID	: 5a8b3630-4a06-45c6-b229-b80d9ba8ec6f	Redirect URIs	: Add a Redirect URI
Directory (tenant) ID	: 805a3915-a0ac-4d2a-9ec8-4bb702169c30	Application ID URI	: Add an Application ID URI
Object ID	: 38d3d160-824e-4d9a-9141-61e7e966fd6e	Managed application in ...	: secRMMIntuneApp

A red box highlights the Application (client) ID and Directory (tenant) ID, with a red note: 'We will need these for later.' At the bottom, a blue banner says: 'Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more'.

Next, click the "View API permissions" button (in the middle part of the page) as shown in the screenshot below.

The screenshot shows the 'Call APIs' section in Azure AD. It features a collection of icons representing various Microsoft services like Office, OneDrive, and Teams. Below the icons, the text reads: 'Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.' A blue button labeled 'View API permissions' is highlighted with a red box.

When you click the "View API permissions" button, you will see a new column to the right of the Application information named "API permissions" as shown in the screenshot below.

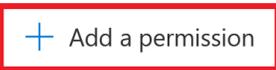
To add the new API/Permission, click the "Add a permission" button.

secRMM Intune Access Control Setup Guide

 Refresh |  Got feedback?

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 cc
▼ Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-

A new window will appear on the right hand side of the screen as shown in the screenshot below. Click the Microsoft Graph button.

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

secRMM Intune Access Control Setup Guide

At this point, you will need to decide which permission (Delegated or Application) you want to use for your environment.

The “Delegated permission” will let you specify an Azure userid and password to have secRMM authenticate with Azure Intune. **Note: As of 12/01/2020, using a “delegated permission” (userid and password) seems to no longer be supported by Azure. If you are currently using “delegated permission”, please contact Squadra Technologies support for help migrating.**

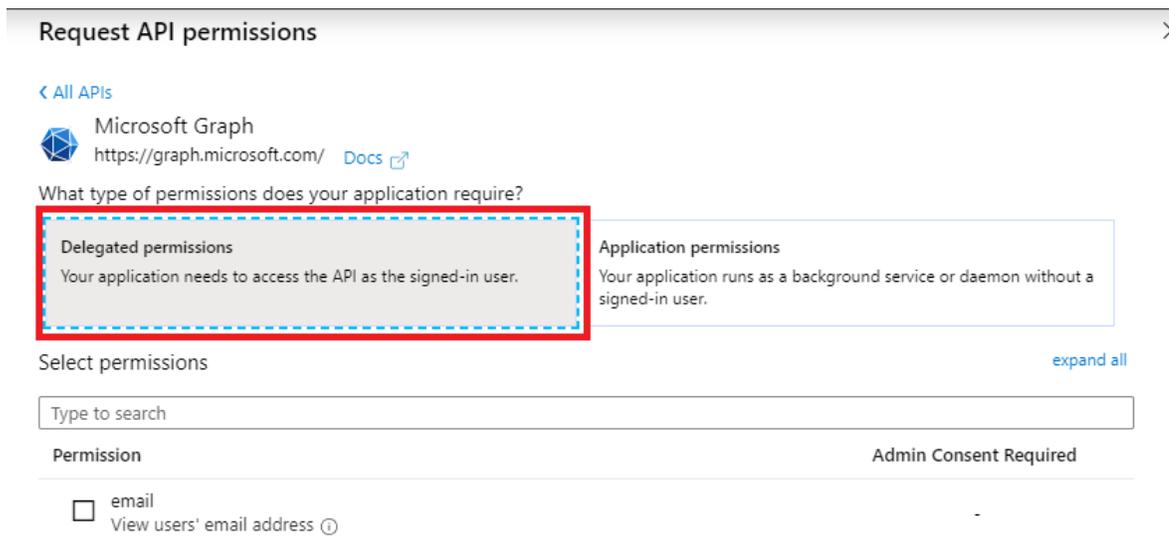
The “Application permission” will let you use an “application secret” (i.e. a password associated with the application) to have secRMM authenticate with Azure Intune.

One of the main reasons for not using “Delegated permission” (i.e. an Azure userid and password) is if your environment requires all userids to use multifactor authentication. If this is the case, then you need to use “Application permission”.

This document will show you how to configure both security types in the two subsections below. If you are unsure about which one to use, please contact Squadra Technologies support (support@squadratechnologies.com) for assistance.

Delegated permission (userid/password)

Click the Delegated button as shown in the screenshot below.



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? **1.**

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

DeviceManagementManagedDevices.Read.All ✓

Permission	Admin Consent Required
▼ DeviceManagementManagedDevices (1)	
2. <input checked="" type="checkbox"/> DeviceManagementManagedDevices.Read.All Read Microsoft Intune devices ⓘ	Yes

3. Add permissions Discard

You will now be back on the "Configured permissions" page. Wait for the "Grant admin consent" button to become active and then click the "Grant admin consent" button as shown in the screenshot below.

Configured permissions

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

+ Add a permission Preparing for consent

API / Permissions name	Type	Description
▼ Microsoft Graph (2)		
DeviceManagementManagedDevices	Delegated	Read Microsoft Intune devices
User.Read	Delegated	Sign in and read user profile

secRMM Intune Access Control Setup Guide

Refresh

⚠ Permissions have been changed, but there is a delay between permissions being configured and when they appear on the consent prompt. Please wait a few minutes before granting admin consent. to consent even if they have already done so previously.

Configured permissions

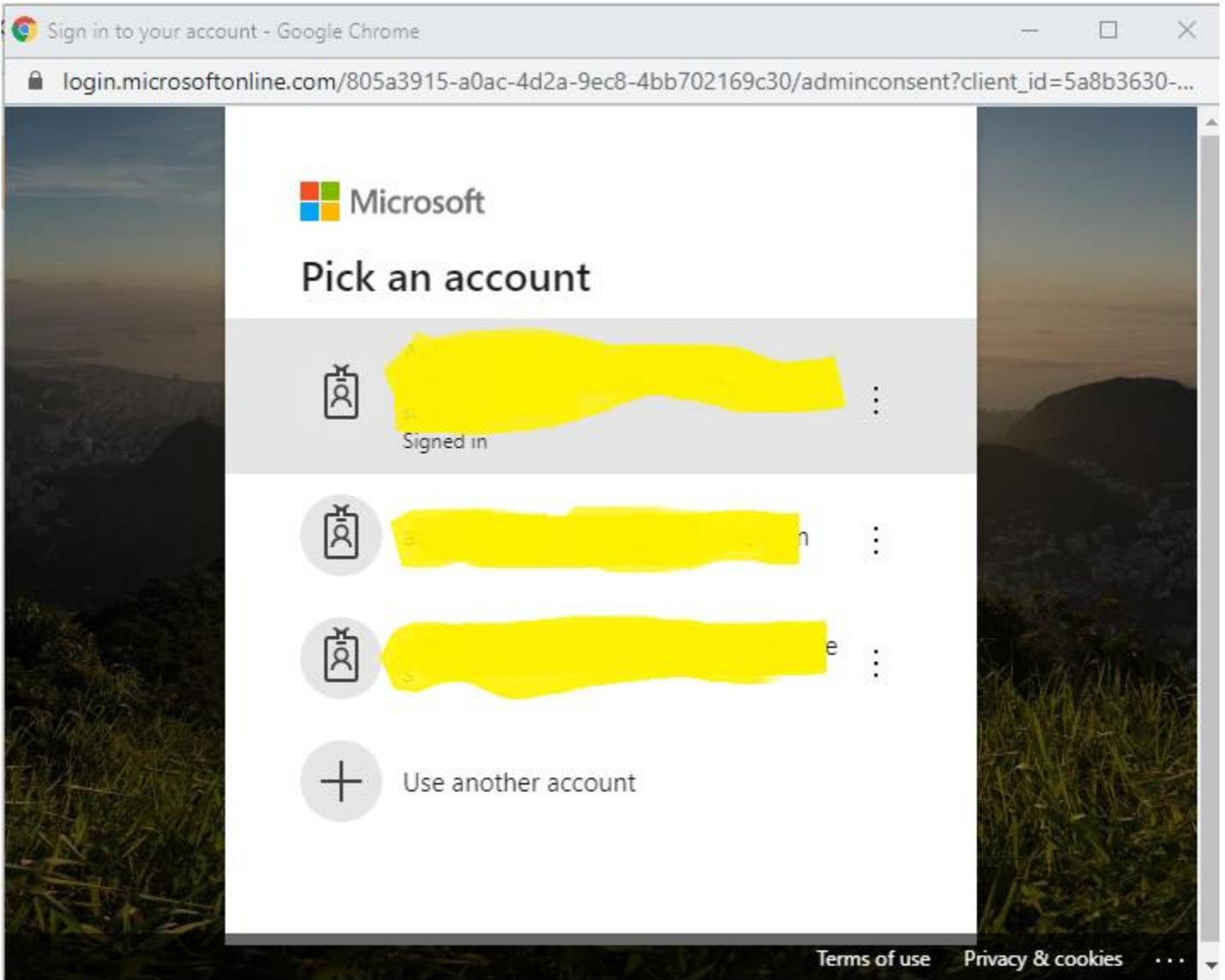
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission **Grant admin consent for Squadra Technologies**

API / Permissions name	Type	Description	Admin Consent Requir...	Status
Microsoft Graph (2)				...
DeviceManagementManagedDevices	Delegated	Read Microsoft Intune devices	Yes	⚠ Not granted for Squadr... ...
User.Read	Delegated	Sign in and read user profile	-	...

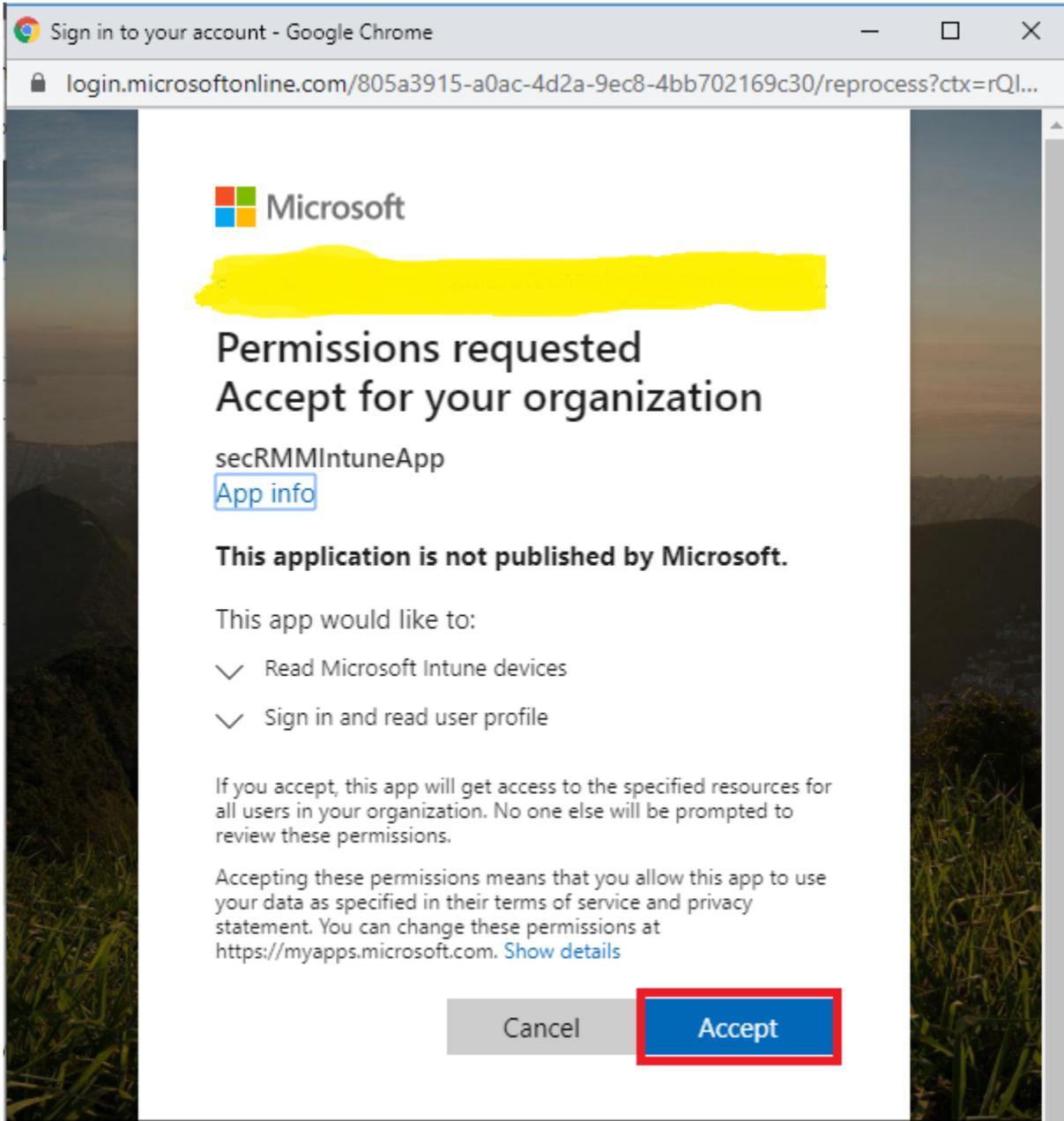
A new window will appear asking you to select an Azure user account as shown in the screenshot below. Make sure you select the Azure global administrator account.

secRMM Intune Access Control Setup Guide



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

secRMM Intune Access Control Setup Guide



You will now see that the permissions have been granted as shown in the screenshot below.

secRMM Intune Access Control Setup Guide

Refresh

Admin consent may not be shown immediately after consent has been granted. Please wait a few minutes and then refresh your page to see the latest consented permissions.

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 Requir...	Status
▼ Microsoft Graph (2)				
DeviceManagementManagedDevices	Delegated	Read Microsoft Intune devices	Yes	✔ Granted for Squadra Tec...
User.Read	Delegated	Sign in and read user profile	-	✔ Granted for Squadra Tec...

Application permission (client secret)

Click the "Application 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.

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

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

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

Select permissions

[expand all](#)

Permission	Admin consent required
✓ DeviceManagementManagedDevices (1)	
<input type="checkbox"/> DeviceManagementManagedDevices.PrivilegedOperations.All ⓘ Perform user-impacting remote actions on Microsoft Intune devices	Yes
<input checked="" type="checkbox"/> DeviceManagementManagedDevices.Read.All ⓘ Read Microsoft Intune devices	Yes
<input type="checkbox"/> DeviceManagementManagedDevices.ReadWrite.All ⓘ Read and write Microsoft Intune devices	Yes

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

secRMM Intune Access Control Setup Guide

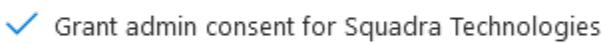
User.Read.All permission

 Refresh |  Got feedback?

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

Configured permissions

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

 Add a permission 

API / Permissions name	Type	Description	Admin consent
Microsoft Graph (2)			
DeviceManagementManagedDevices.Read.All	Application	Read Microsoft Intune devices	Yes
User.Read	Delegated	Sign in and read user profile	-

A new window will appear on the right hand side of the screen as shown in the screenshot below. Click the Microsoft Graph button.

secRMM Intune Access Control Setup Guide

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

Click the "Application 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.

Type "user" in the "Select permissions" textbox 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](#)

Permission Admin consent required

Scroll down the list, expand the user item, select "User.Read.All" and then click the "Add permissions" button as shown in the screenshot below.

1. User (1)

User.Export.All ⓘ
Export user's data

User.Invite.All ⓘ
Invite guest users to the organization

User.ManageIdentities.All ⓘ
Manage all users' identities

2. User.Read.All ⓘ
Read all users' full profiles

User.ReadWrite.All ⓘ
Read and write all users' full profiles

3.

You will now be back on the "Configured permissions" page. Wait for the "Grant admin consent" button to become active and then click the "Grant admin consent" button as shown in the screenshot below.

secRMM Intune Access Control Setup Guide

Refresh | Got feedback?

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

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 (3)				
DeviceManagementManagedE	Application	Read Microsoft Intune devices	Yes	 Not granted for Squadra... 
User.Read	Delegated	Sign in and read user profile	-	
User.Read.All	Application	Read all users' full profiles	Yes	 Not granted for Squadra... 

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

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.

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 (3)				
DeviceManagementManagedE	Application	Read Microsoft Intune devices	Yes	 Not granted for Squadra... 
User.Read	Delegated	Sign in and read user profile	-	
User.Read.All	Application	Read all users' full profiles	Yes	 Not granted for Squadra... 

The permissions will not turn to green icons showing success as shown in the screenshot below.

secRMM Intune Access Control Setup Guide

Refresh | Got feedback?

Successfully granted admin consent for the requested permissions.

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 (3)				
DeviceManagementManagedDevices.Read.All	Application	Read Microsoft Intune devices	Yes	✓ Granted for Squadra Tec... ⋮
User.Read	Delegated	Sign in and read user profile	-	✓ 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.

Home > Squadra Technologies >

secRMMIntuneApp

Search (Ctrl+ /) << Delete Endpoints

- Overview
- Quickstart
- Integration assistant
- Manage**
- Branding
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles | Preview
- Owners

Essentials

Display name
secRMMIntuneApp

Application (client) ID
80591fd3-e68e-4f8c-bb5

Directory (tenant) ID
805a3915-a0ac-4d2a-9e

Object ID
f2ea8fb5-c675-4abf-b7b

Starting June 30th, and Azure AD Graph feature updates. [Learn more](#)

Call APIs

secRMM Intune Access Control Setup Guide

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

 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).

secRMM Intune Access Control Setup Guide

Certificates & secrets

Got feedback?

Add a client secret

Description

secRMMIntuneAppClientSecret

Expires

- In 1 year
- In 2 years
- Never

Add

Cancel

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	~srF.N6CRw2g-XHJL22-Fj..	8e192a33-eb34-46eb-84 ...

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

The screenshot shows the 'API permissions' page for an application named 'secRMMIntuneApp'. The left-hand navigation pane contains several categories: 'Overview', 'Quickstart', 'Manage', and 'Support + Troubleshooting'. The 'Manifest' option under the 'Manage' section is highlighted with a red box. The main content area displays a list of permissions, including 'get_d' under 'Intune (z)' and 'Device' and 'User.I' under 'Microsoft'.

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

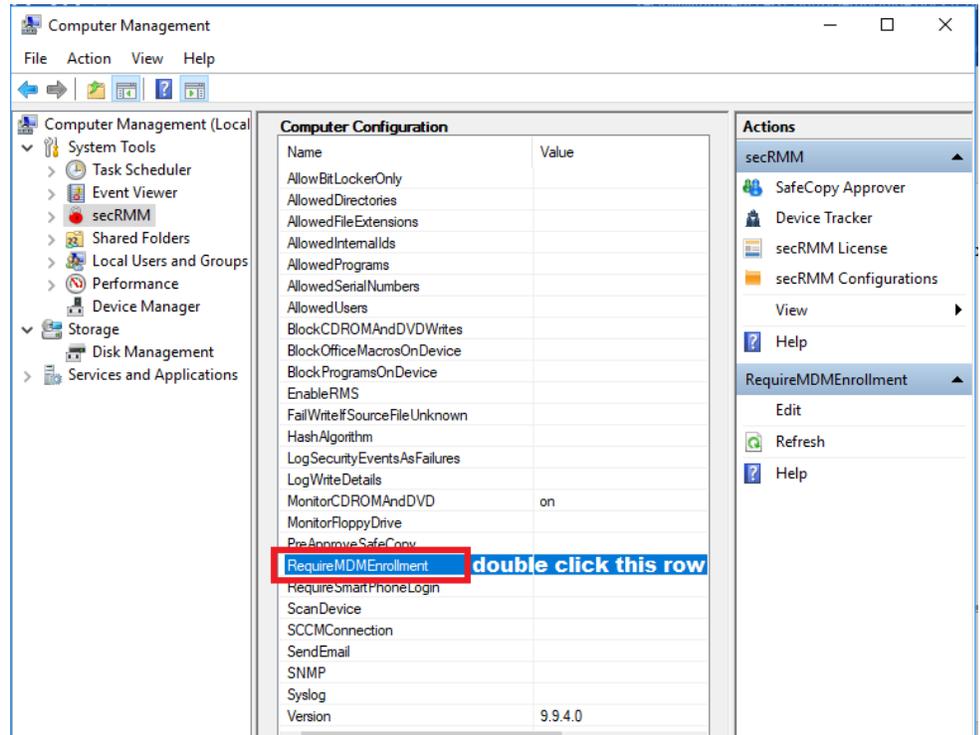
Note that if you do not change the "allowPublicClient" to "true" in the Manifest, when you do a "Test Connection" in the secRMM console, you will get the error:

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

Configure secRMM to get mobile device state

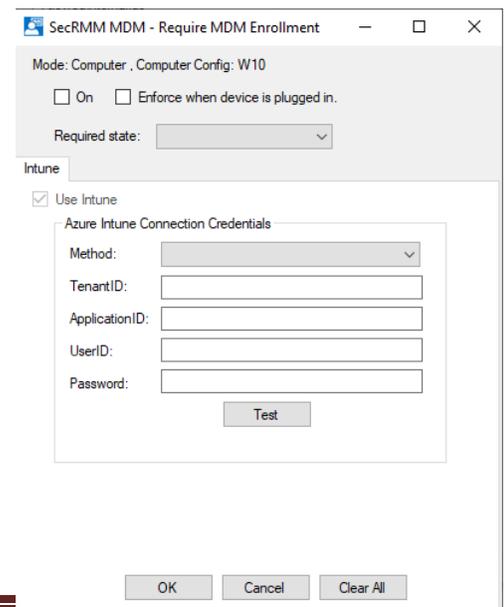
Now that we have setup where secRMM will get the mobile device state, we will give secRMM the information about how to get the mobile device state data. secRMM can be centrally managed with either System Center Configuration Manager (SCCM) or Azure Intune or Active Directory Group Policy Objects (AD 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.

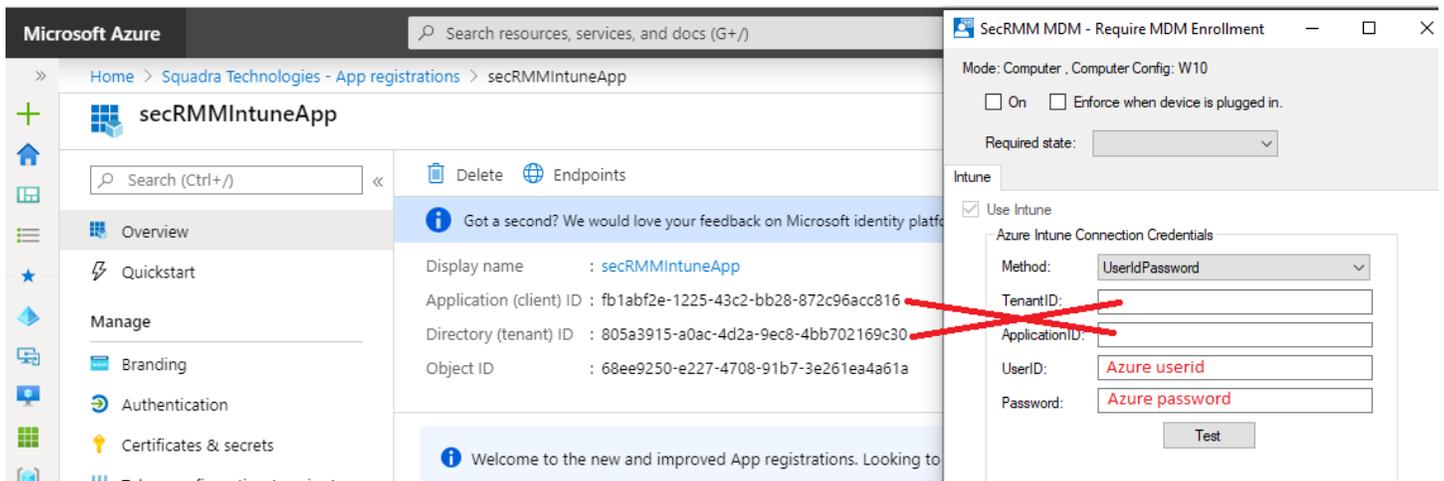


secRMM Intune Access Control Setup Guide

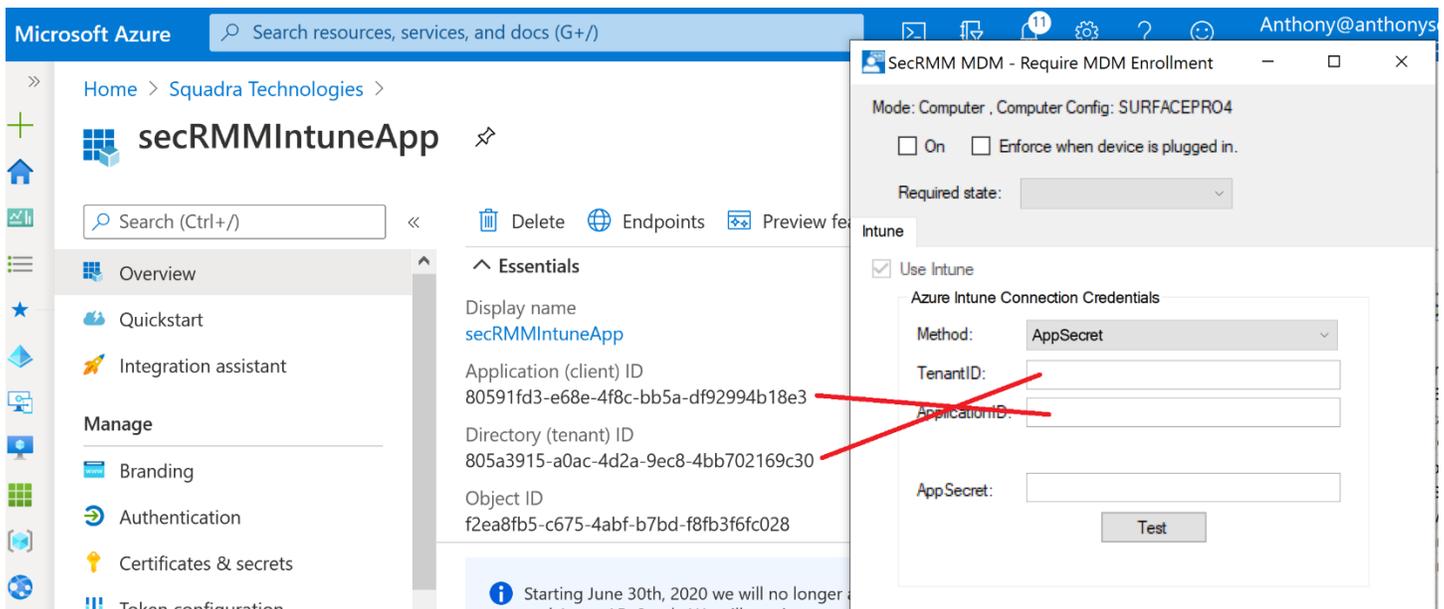
Next, you need to specify the "Azure Intune Connection Credentials" Method. Select the "UserIdPassword" method if you configured the Azure application permission for "Delegation". Select the "AppSecret" method if you configured the Azure application permission for "Application".

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+)

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles | Preview

Got feedback?

uproaa 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

Intune

On Enforce when device is plugged in.

Required state: [v]

Use Intune

Azure Intune Connection Credentials

Method: AppSecret

TenantID: []

ApplicationID: []

AppSecret: Azure client secret

Test

OK Cancel Clear All

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

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

Mode: Computer , Computer Config: W10

On Enforce when device is plugged in.

Required state: **Enrolled**

Intune

Use Intune

Azure Intune Connection Credentials

Method: **UserIdPassword**

TenantID: 805a3915-a0ac-4d2a-9ec8-4bb702169c30

ApplicationID: fb1abf2e-1225-43c2-bb28-872c96acc816

UserID: anthony@anthonyssquaretechnologies.onmiki

Password:

Test

OK Cancel Clear All

Mode: Computer , Computer Config: SURFACEPRO4

On Enforce when device is plugged in.

Required state: **Enrolled**

Intune

Use Intune

Azure Intune Connection Credentials

Method: **AppSecret**

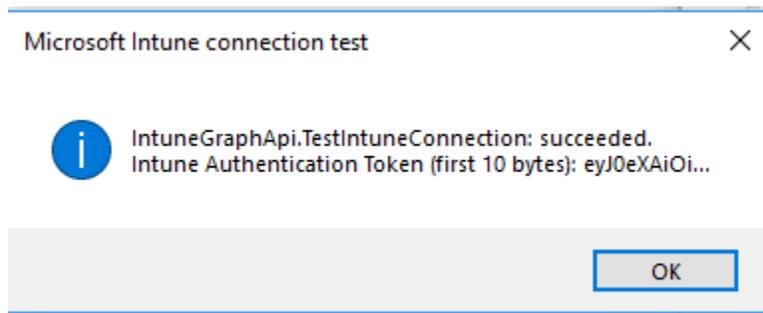
TenantID: 805a3915-a0ac-4d2a-9ec8-4bb702169c30

ApplicationID: 80591fd3-e68e-4f8c-bb5a-df92994b18e3

AppSecret:

Test

OK Cancel Clear All

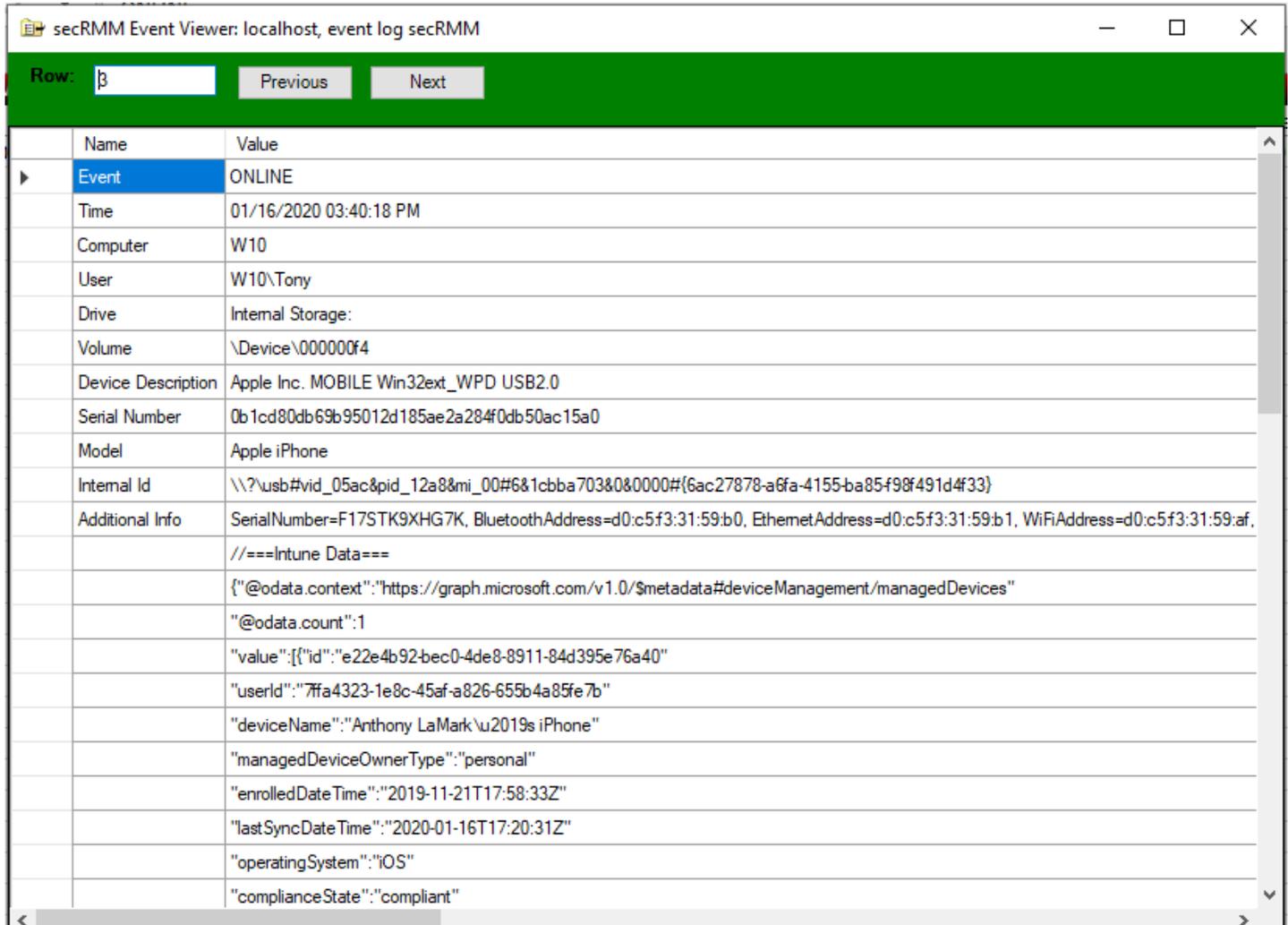


Once you have a successful connection, save the secRMM values by clicking the OK button on the "Require MDM Enrollment" dialog.

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



The screenshot shows the 'secRMM Event Viewer' window. The title bar reads 'secRMM Event Viewer: localhost, event log secRMM'. The interface has a green header bar with 'Row: 3' and 'Previous' and 'Next' buttons. The main area is a table with two columns: 'Name' and 'Value'. The 'Event' row is selected, showing 'ONLINE'. Below this, various system properties are listed, including 'Time', 'Computer', 'User', 'Drive', 'Volume', 'Device Description', 'Serial Number', 'Model', 'Internal Id', and 'Additional Info'. The 'Additional Info' field contains a large JSON object with details about the device's Intune enrollment status, including fields like '@odata.context', '@odata.count', 'value', 'userId', 'deviceName', 'managedDeviceOwnerType', 'enrolledDateTime', 'lastSyncDateTime', 'operatingSystem', and 'complianceState'.

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	0b1cd80db69b95012d185ae2a284fdb50ac15a0
Model	Apple iPhone
Internal Id	\\?\usb#vid_05ac&pid_12a8&mi_00#6&1cbba703&0&0000#{6ac27878-a6fa-4155-ba85-f98f491d4f33}
Additional Info	SerialNumber=F17STK9XHG7K, 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":"7ffa4323-1e8c-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/>