

Security Removable Media Manager (secRMM)

# Intune Access Control Setup Guide

Version 9.11.27.0 (April 2024) Protect your valuable data

#### © 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
PREREQUISTES	4
SETUP OVERVIEW	5
SETUP DETAILS	5
Setup an Azure "application"	5
Login to your Azure tenant	
Create Azure Application	
Delegated permission (userid/password)	
DeviceManagementManagedDevices.Read.All permission	
User.Read.All permission	15
Application.Read.All permission	
Application permission (client secret)	
DeviceManagementManagedDevices.Read.All permission	24
User.Read.All permission	27
Application.Read.All permission	
Updating the Manifest	35
CONFIGURE SECRMM TO GET MOBILE DEVICE STATE	
Delegated permission (userid/password)	
Application permission (client secret)	
TEST THE CONFIGURATION	40
EVENT DATA	41
CONTACTING SQUADRA TECHNOLOGIES SUPPORT	43
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:

- 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 officiers 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 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.

### **Prerequistes**

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

defininitions, 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 <u>https://portal.azure.com.</u> 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**".

Δ	Home - N	licrosoft	Azure	×	+
$\leftarrow$	→ C	$\hat{\mathbf{D}}$	🗎 po	rtal.azure.	com/
A	pps	STC	STS	, Techr	nology
Mic	rosoft /	Azure			
»					
+					
<b>^</b>					
⊨					
- * -					
٠					
두					

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

Δ S	quadra Technologies - Overview 🗙 🕂
← -	→ C 🏠 🌲 portal.azure.com/#bla
👪 Ap	ops 🛄 STC 🛄 STS 🛄 Technology
Micr	osoft Azure
>>	Home $>$ Squadra Technologies - Overvie
+	Squadra Technologies -
<b>^</b>	( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( )
	D Search (Ctrl+/)
⊨	Overview
*-	💅 Getting started
٠	Manage
Ę	A Users
	🝰 Groups
	Organizational relationships
[]	A Roles and administrators
۲	Enterprise applications
	Devices
8	App registrations
- 🚸 -	Identity Governance

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**".



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)

<ul> <li>* Name         The user-facing display name for this application (this can be changed late secRMMIntuneApp_Delegated         Supported account types         Who can use this application or access this API?         Accounts in this organizational directory only Squadra Technologies of Accounts in any organizational directory (Any Azure AD directory - Multiple Accounts in any organizational directory (Any Azure AD directory - Multiple Accounts in any organizational directory (Any Azure AD directory - Multiple Accounts in any organizational directory (Any Azure AD directory - Multiple Accounts in any organizational directory (Any Azure AD directory - Multiple Accounts in any organizational directory (Any Azure AD directory - Multiple Accounts in any organizational directory (Any Azure AD directory - Multiple Accounts in any organizational directory (Any Azure AD directory - Multiple Accounts in any organizational directory (Any Azure AD directory - Multiple Accounts in any organizational directory (Any Azure AD directory - Multiple Accounts in Acco</li></ul>
The user-facing display name for this application (this can be changed late secRMMIntuneApp_Delegated Supported account types Who can use this application or access this API? Accounts in this organizational directory only Squadra Technologies of Accounts in any organizational directory (Any Azure AD directory - Mu
secRMMIntuneApp_Delegated Supported account types Who can use this application or access this API? Accounts in this organizational directory only Squadra Technologies of Accounts in any organizational directory (Any Azure AD directory - Mu
Supported account types Who can use this application or access this API? Accounts in this organizational directory only Squadra Technologies of Accounts in any organizational directory (Any Azure AD directory - Mu
Supported account types Who can use this application or access this API? Accounts in this organizational directory only Squadra Technologies of Accounts in any organizational directory (Any Azure AD directory - Mu
Who can use this application or access this API?  Accounts in this organizational directory only  Accounts in any organizational directory (Any Azure AD directory - Mu
Accounts in this organizational directory only Squadra Technologies of Accounts in any organizational directory (Any Azure AD directory - Mu
Accounts in any organizational directory (Any Azure AD directory - Mu
<ul> <li>Accounts in any organizational directory (Any Azure AD directory - Mu</li> </ul>
Personal Microsoft accounts only
Help me choose
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authe
changed later, but a value is required for most authentication scenarios.

### secRMMIntuneApp\_Delegated ☆

	📋 Delete   ⊕ Endpoints 💀 Preview features
Overview	↑ Essentials
🍊 Quickstart	Display name : secRMMIntuneApp_Delegated
💉 Integration assistant	Application (client) ID : c5c492e1-6981-4eb2-98d0-21e6a3c8e910
	Directory (tenant) ID : 805a3915-a0ac-4d2a-9ec8-4bb702169c30
Manage	Object ID : fbd45900-2b15-4321-83f9-57bee1167b0a
🔤 Branding	
Authentication	Welcome to the new and improved App registrations. Looking to learn how it's cha
📍 Certificates & secrets	
Token configuration	Starting June 30th, 2020 we will no longer add any new features to Azure Active Dire no longer provide feature updates. Applications will need to be upgraded to Micros
API permissions	
🔷 Expose an API	Call APIs
🚨 App roles   Preview	
Owners	
🔓 Roles and administrators   Previ	
11 Manifest	💴 💿 👳 🚺
Support + Troubleshooting	Build more powerful apps with rich user and business data
Troubleshooting	from Microsoft services and your own company's data sources.
New support request	View API permissions

# 

	Search (Ctrl+/)	~	🔘 Refresh 🔋 💙 Got feedba	ack?		
88 464 1/2	Overview Quickstart Integration assistant		Configured permissions Applications are authorized to cal include all the permissions the ap	l APIs when they are g plication needs. Learn	granted permissions by users/admin more about permissions and conse	is as part ent
Ma	nage		+ Add a permission 🗸 Gra	nt admin consent for	Squadra Technologies	
	Branding		API / Permissions name	Туре	Description	
Э	Authentication		∽ Microsoft Graph (1)			
•	Certificates & secrets		User.Read	Delegated	Sign in and read user profile	
	Token configuration					
Mic	rosoft Azure	𝒫 Search reso	ources, services, and docs (G+/)			? 🙂
Mic → + ← … ★ ◆ … … *	rosoft Azure Home > Squadra Technologies > secRMI	Search reso VintuneApp_De Delegate O Refresh Configured p Applications ar include all the p + Add a pel API / Pe	purces, services, and docs (G+/)         elegated         ed   API permissions         Image: Got feedback?         permissions         re authorized to call APIs when they are granted permissions permissions the application needs. Learn more about permission         rmission       Grant admin consent for Squadra Techno ermissions name         Type       Description	Request API perm Select an API Microsoft APIs APIs my or Commonly used Microsoft Commonly used Microsoft G Take advantage Access Azure A single endpoin	ISSIONS rganization uses My APIs ft APIs raph e of the tremendous an pount of data in Office 365, Enterprise Mo ND, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, Sharef t.	? (3) obility + Security, Point, Planner, an

Micr	osoft Azure	$\mathcal P$ Search resources, services, and c	locs (G+/)			Þ.	Ŗ	₽	۲	? ©	Anthony@anthonysqua SQUADRA TECHNOLOGIES
» + ♠	Home > Squadra Technologies > secRM 	MIntuneApp_Delegated _ <b>Delegated</b>   API perm	nissions	\$	Request API permissions						×
<b>⊠1</b> ≔	Search (Ctrl+/)     «      Overview	Configured permissions	?		Witrosoft Graph https://graph.microsoft.com/ Docs range What type of permissions does your application require?						
* •	<ul> <li>Quickstart</li> <li>Integration assistant</li> </ul>	Applications are authorized to call Al include all the permissions the applic	Pls when they are ation needs. Lear	granted permiss m more about pe r Squadra Techno	Delegated permissions Your application needs to access the API as the signed-in user.		Applio Your a signed	ation per pplication I-in user.	missions n runs as	a backgro	ind service or daemon without a
<ul> <li></li></ul>	Branding Authentication Certificates & secrets	API / Permissions name Microsoft Graph (1) User.Read	Type Delegated	Description Sign in and rea							

#### 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**

K All API	s Aicrosoft Graph	
What tu	ttps://graph.microsoft.com/ Docs 🕑	
Delega Your a	ated permissions 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 p	permissions	expand
🔎 devi	icemanagementmanageddevices	
Pe	rmission	Admin consent required
$\checkmark$ De	eviceManagementManagedDevices (1)	
	DeviceManagementManagedDevices.PrivilegedOperation Perform user-impacting remote actions on Microsoft Intu	s.All (i) Yes ne devices
	DeviceManagementManagedDevices.Read.All ③ Read Microsoft Intune devices	Yes
	DeviceManagementManagedDevices.ReadWrite.All ③ 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.

+	secRMMIntuneApp_	_ <b>Delegated</b>   API permissions 🔗	
<b>^</b>			
≝h	✓ Search (Ctrl+/) «	🕐 Refresh 🛛 🛇 Got feedback?	
=	4 Overview	A You are editing permission(s) to your application, users will have to consent even if they've already done so previou	sly.
*	📣 Quickstart		
-	💉 Integration assistant	Configured permissions	
<b>R</b>	Manage	Applications are authorized to call APIs when they are granted permissions by users/admins as part of the com- include all the permissions the application needs. Learn more about permissions and consent	sent process. Th
<u> </u>	🧮 Branding	+ Add a permission 🗸 Grant admin consent for Squadra Technologies	
	Authentication	ADI / Dermissions name Tune Description	Admin conco
	📍 Certificates & secrets	API / Permissions name Type Description	Aumin conse
	Token configuration	✓ Microsoft Graph (2)	
SQL	<ul> <li>API permissions</li> </ul>	DeviceManagementManagedI Delegated Read Microsoft Intune devices	Yes
8	le Expose an API	User.Read Delegated Sign in and read user profile	-
•	🎥 App roles   Preview		
-			



#### 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	
Delegated permissions Your application needs to access the API as the signed-in user.	Application permissior Your application runs a signed-in user.
Select permissions          Permission	
> IdentityRiskyUser	
V 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.

+	<sub>-</sub> secRMMIntuneApp	_ <b>Delegated</b>   API permissions 🛷	
<b>^</b>	<b>.</b>		
<b>≊h</b>		🕐 Refresh 🔰 💙 Got feedback?	
=	Overview	A You are editing permission(s) to your application, users will have to consent even if they've already done so previou	ısly.
*	🔲 Quickstart		
-	🚀 Integration assistant	Configured permissions	
<b>.</b>	Manage	Applications are authorized to call APIs when they are granted permissions by users/admins as part of the con include all the permissions the application needs. Learn more about permissions and consent	sent process. Th
	🧮 Branding	+ Add a permission 🗸 Grant admin consent for Squadra Technologies	
[e]	Authentication	APL / Permissions name Type Description	Admin conse
	📍 Certificates & secrets		
<u> </u>	II Token configuration	✓ Microsoft Graph (2)	
501	→ API permissions	DeviceManagementManaged[ Delegated Read Microsoft Intune devices	Yes
8	Expose an API	User.Read Delegated Sign in and read user profile	-
<b>•</b>	App roles   Draview		
$\equiv$			



#### 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?



### Select permissions

Add permissions

Discard

۶	Application.Read.All
	The "Admin consent required" column shows the default value for an organization. However, user permission, user, or app. This column may not reflect the value in your organization, or in organization more
	Permission
`	Application (1)
	Application.Read.All ③ Read applications

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

rosoft Azure	${\cal P}$ Search resources, services, and doc	s (G+/)			E	Q	P	۲	?
Home > Squadra Technologies > secRM 	MIntuneApp_Delegated _ <b>Delegated</b>   API permis	ssions	\$						
	🕐 Refresh 🛛 🛇 Got feedback?								
<ul> <li>Overview</li> <li>Quickstart</li> </ul>	Successfully granted admin consent	for the reques	ted permissions.						
💉 Integration assistant									
Manage	The "Admin consent required" colun organizations where this app will be	nn shows the d used. Learn m	default value for an organization. However, use tore	r consent can be customized per permission,	user, or ap	p. This co	olumn ma	ay not r	reflec
🗮 Branding									
Authentication	Configured permissions								
📍 Certificates & secrets	Applications are authorized to call APIs include all the permissions the application	when they are on needs. Lea	e granted permissions by users/admins as Irn more about permissions and consent	part of the consent process. The list of	configured	l permis	sions sh	ould	
Token configuration									
<ul> <li>API permissions</li> </ul>	Add a permission	nin consent to	or squadra Technologies						
Expose an API	API / Permissions name	Туре	Description	Admin consent req	Status				
App roles   Preview	✓ Microsoft Graph (4)								•••
Owners	Application.Read.All	Delegated	Read applications	Yes	🥑 Grai	nted for S	ŝquadra T	ſec	
Roles and administrators   Previ	DeviceManagementManaged	Delegated	Read Microsoft Intune devices	Yes	🕑 Grai	nted for S	Squadra T	fec	
Manifest	User.Read	Delegated	Sign in and read user profile	No	🥑 Gran	nted for S	Squadra T	lec	

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

Micr	osoft Azure	${\cal P}$ Search resources, services, and doc	s (G+/)			Þ		e			Anthony@anthonysqua squadra technologie
» + €	Home > Squadra Technologies > secRM 	MintuneApp_Delegated _Delegated   API permis © Refresh   © Got feedback?	ssions	A							
	<ul> <li>Quickstart</li> <li>Integration assistant</li> </ul>	Do you want to grant consent for the listed below.	requested p	ermissions for all accounts in Squadra Technologies? T	his will update any existir	ng admin	consen	t record	is this ap	pplicatio	n already has to match what is
•	Branding	organizations where this app will be	used. Learn m	ore							
	Authentication     Certificates & secrets     Token configuration     APL 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									
	Expose an API     App roles   Preview	API / Permissions name ~ Microsoft Graph (4)	Туре	Description	Admin consent req	Status					
	Roles and administrators   Previ	Application.Read.All DeviceManagementManaged	Delegated Delegated	Read applications Read Microsoft Intune devices	Yes	🕑 Gra 🥑 Gra	nted for nted for	õquadra õquadra	Tec <sub></sub> •		
	Manifest Support + Troubleshooting	User.Read User.Read.All	Delegated Delegated	Sign in and read user profile Read all users' full profiles	No Yes	🥑 Gra	nted for nted for	õquadra õquadra	Tec •	••	
	Troubleshooting New support request	To view and manage permissions and u	ser consent, t	ry Enterprise applications.							

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

Micro	osoft Azure	${\cal P}$ Search resources, services, and do	cs (G+/)			Þ		<u>(</u> 2			
» +	Home > Squadra Technologies > secRM 	<sup>IMIntuneApp_Delegated</sup> _ <b>Delegated</b>   API permi	ssions	\$ ···				<b>େ</b> Gra	Grant co ant conse	onsent nt successfu	ul I
20		🕐 Refresh 🛛 🛇 Got feedback?									
≔ ★	<ul> <li>Overview</li> <li>Quickstart</li> </ul>	<ol> <li>Successfully granted admin consen</li> </ol>	t for the reques	ted permissions.							
٠	💉 Integration assistant										
<b>R</b>	Manage	The "Admin consent required" colu organizations where this app will be	mn shows the o	default value for an organization. However, user consent can tore	be customized per permission,	, user, or ap	p. This c	olumn ma	y not refle	ct the value ir	n your o
	🔤 Branding										
	Authentication	Configured permissions									
0	📍 Certificates & secrets	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									
	Token configuration										
	API permissions	+ Add a permission 🗸 Grant ad	min consent fo	or Squadra Technologies							
~	Expose an API	API / Permissions name	Туре	Description	Admin consent req	Status					
•	🐣 App roles   Preview	✓Microsoft Graph (4)									
•	Owners	Application.Read.All	Delegated	Read applications	Yes	🥑 Grai	nted for !	iquadra Te	•••		
	Roles and administrators   Previ	DeviceManagementManaged	C Delegated	Read Microsoft Intune devices	Yes	🥑 Grai	nted for !	iquadra Te	•••		
3	10 Manifest	User.Read	Delegated	Sign in and read user profile	No	🥑 Grai	nted for	iquadra Te			
-	Support + Troubleshooting	User.Read.All	Delegated	Read all users' full profiles	Yes	🥑 Gra	nted for !	iquadra Te	•••		

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

»	Home > Squadra Technologies >
-	Register an application
1	5 11
-	* Name
	The user-facing display name for this application (this can be changed later).
	secRMMIntuneApp_Application
	Supported account types
	supported account types
	Who can use this application or access this API?
	Accounts in this organizational directory only Squadra Technologies only -:
	Accounts in any organizational directory (Any Azure AD directory - Multitena
	Accounts in any organizational directory (Any Azure AD directory - Multitena
	O Personal Microsoft accounts only
	Help me choose
	Redirect LIRI (optional)
	We'll return the authentication response to this LIRL after successfully authenticati
	changed later, but a value is required for most authentication scenarios.
	Web
	By proceeding, you agree to the Microsoft Platform Policies 🗗
	Register
	<

### Application permission (client secret)

# secRMMIntuneApp\_Application 🔗

₽ Search (Ctrl+/) «	📋 Delete   ⊕ Endpoints 💀 Preview features
Overview	↑ Essentials
🗳 Quickstart	Display name : secRMMIntuneApp_Application
💉 Integration assistant	Application (client) ID :23767375-7c40-4968-bc0e-9c4fd87c58b7
	Directory (tenant) ID :805a3915-a0ac-4d2a-9ec8-4bb702169c30
Manage	Object ID : 4b97f85e-88de-4f61-adde-952ee47d8352
🧮 Branding	
Authentication	Welcome to the new and improved App registrations. Looking to learn how it's char
📍 Certificates & secrets	
Token configuration	Starting June 30th, 2020 we will no longer add any new features to Azure Active Direct no longer provide feature updates. Applications will need to be upgraded to Microsc
<ul> <li>API permissions</li> </ul>	
🔷 Expose an API	
🚨 App roles   Preview	
💀 Owners	
🔓 Roles and administrators   Previ	
10 Manifest	
Support + Troubleshooting	Build more powerful apps with rich user and business data
Troubleshooting	from Microsoft services and your own company's data sources.
New support request	View API permissions

#### 

✓ Search (Ctrl+/) «	🕐 Refresh 🛛 🛇 Got feedback?						
Sverview	Configured permissions						
🗳 Quickstart	Applications are authorized to call APIs when they are granted permissions by users/admins						
💉 Integration assistant	include all the permissions the application needs. Learn more about permissions and consent						
Manage	+ Add a permission 🗸 Grant admin consent for Squadra Technologies						
🔜 Branding	API / Permissions name Type Description						
Authentication	∽Microsoft Graph (1)						
📍 Certificates & secrets	User.Read Delegated Sign in and read user profile						
Token configuration							

Micr	osoft Azure	$\mathcal{P}$ Search resources, services, and	docs (G+/)			D G	😃 🐵 ? 🙄	
* +	Home > Squadra Technologies > secRM	MIntuneApp_Application _Application   API per	rmissions	\$	Request API permissions			
	<ul> <li>✓ Search (Ctrl+/) «</li> <li>₩ Overview</li> </ul>	◯ Refresh   ♡ Got feedback	k?	_	Select an API <u>Microsoft APIs</u> APIs my organization uses M	/ APIs		
	<ul> <li>Quickstart</li> <li>Integration assistant</li> </ul>	Applications are authorized to call A include all the permissions the appli	APIs when they are	e granted permiss arn more about pe	Commonly used Microsoft APIs  Microsoft Graph Take advantage of the tremendous amoo Access Azure AD, Excel, Intune, Outlook	nt of data in Office 365, En Ex hange, OneDrive, OneP	iterprise Mobility + Security, - Note, SharePoint, Planner, an	an nd i
	Manage Branding Authentication	API / Permissions name	Type	Description	single endpoint.			
	Certificates & secrets     Token configuration     API permissions     Concerts # 11	User.Read	Delegated	Sign in and rea	C Azure DevOps Integrate with Azure DevOps and Azure DevOps server	are Rights Management rvices dated users to read and wri content	ite Programmatic ac functionality ava portal	.rvi cce sila
	App roles   Preview  App roles   Preview  Roles and administrators   Previ  Manifest				Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data	namics 365 Business Cent natic access to data and lity in Dynamics 365 Busini	tral Frogrammatic ac	ccł



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 Al	Pls	
	Microsoft Graph	
$\checkmark$	https://graph.microsoft.com/ Docs 🗹	
What t	type of permissions does your application require?	
Dele	asted nermissions	Application permissions
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
🔎 de	vicemanagementmanageddevices	
P	ermission	Admin consent required
$\sim$ D	eviceManagementManagedDevices (1)	
	Device Management Managed Devices. Privileged Operations	.0 IIA
$\Box$	Perform user-impacting remote actions on Microsoft Intun	Yes e devices
	DeviceManagementManagedDevices.Read.All ①	
$\sim$	Read Microsoft Intune devices	Yes
_	DeviceManagementManagedDevices.ReadWrite All	
$\Box$	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.

>

+	- <b></b> secRMMIntuneAp	p_Application   API permissions 🛷						
<b>≥</b> h	₽ Search (Ctrl+/)	<ul> <li>Kefresh</li> <li>Got feedback?</li> </ul>						
≔ ★	<ul> <li>Overview</li> <li>Quickstart</li> </ul>	A You are editing permission(s) to your application, users will have to consent even if they've already done so previously.						
٠	💉 Integration assistant	Configured permissions						
<b>R</b>	Manage	Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The include all the permissions the application needs. Learn more about permissions and consent						
Ĩ	💳 Branding	+ Add a permission 🗸 Grant admin consent for Squadra Technologies						
[]	Authentication	API / Permissions name Type Description Admin conse						
3	📍 Certificates & secrets	✓Microsoft Graph (2)						
SQL	Token configuration	DeviceManagementManaged[ Application _ Read Microsoft Intune devices Vec						
	API permissions	Use Based						
<b></b>	Expose an API	User,kead Delegaled 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 treme Access Azure AD, Excel, Intu single endpoint.	ndous amount of <sub>d</sub> ata in Office 365, Enterprise ne, Outlook/Exchange, OneDrive, OneNote, Sha	Mobility + Security, and Windows 10. arePoint, Planner, and more through a
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
Secure, massively scalable object and data lake storage for unstructured and semi-structured data	<b>Dynamics 365 Business Central</b> Programmatic access to data and functionality in Dynamics 365 Business Central	Programmatic access to Intune data



#### 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	
<ul> <li>✓ All APIs</li> <li>Microsoft Graph https://graph.microsoft.com/ Docs ♂</li> <li>What type of permissions does your application require?</li> </ul>	
Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background sen signed-in user.
Select permissions	
Permission	Admin cons
> IdentityRiskyUser	
∨ User (1)	
User.Read.All Read all users' full profiles	Yes
Add permissions Discard	

D03052021

5

+ <b>^</b>	secRMMIntuneAp	p_Application   API permissions 🖈						
Zh		🕐 Refresh 🔰 🛇 Got feedback?						
≔ ★	<ul> <li>Overview</li> <li>Quickstart</li> </ul>	A You are editing permission(s) to your application, users will have to consent even if they've already done so previously.						
٠	🚀 Integration assistant	Configured permissions						
<b>R</b>	Manage	Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The include all the permissions the application needs. Learn more about permissions and consent						
Ť	🚍 Branding	+ Add a permission 🗸 Grant admin consent for Squadra Technologies						
[]	Authentication	API / Permissions name Type Description Admin	conser					
٢	Certificates & secrets	Microsoft Graph (2)						
2	<ul> <li>API permissions</li> </ul>	DeviceManagementManaged[ Application Read Microsoft Intune devices Yes						
<u>8</u>	🗠 Expose an API	User.Read Delegated Sign in and read user profile -						
v	•• • • • • •							

### **Request API permissions**

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph Take advantage of the treme Access Azure AD, Excel, Intu single endpoint.	endous amount of ata in Office 365, Enterprise ne, Outlook/Exchange, OneDrive, OneNote, Sh	: Mobility + Security, and Windows 10. arePoint, Planner, and more through a
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
Secure, massively scalable object and data lake storage for unstructured and semi-structured data	<b>Dynamics 365 Business Central</b> Programmatic access to data and functionality in Dynamics 365 Business Central	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	Application permissions
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 al
	×
Permission	Admin consent required
✓ Application (1)	
Application.Read.All (i) Read all applications	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.

	💍 Refresh 🛛 💙 Got	feedback?				
Overview	A You are editing permis	ission(s) to your appli	lication, us	ers will have to consent even if they've alrea	ly done so previously.	
🗳 Quickstart						
🐔 Integration assistant						
Manage	The "Admin consent r organizations where the second sec	required' column sho his app will be used.	ows the de	efault value for an organization. However, us re	er consent can be customized per permission	n, user, or app. This column may not r
Branding						
Authentication	Configured permission	ns				
<ul> <li>Authentication</li> <li>Certificates &amp; secrets</li> </ul>	Configured permission Applications are authorized	ns d to call APIs when t	they are	granted permissions by users/admins a	s part of the consent process. The list of	f configured permissions should
<ul> <li>Authentication</li> <li>Certificates &amp; secrets</li> <li>Token configuration</li> </ul>	Configured permission Applications are authorized include all the permissions	ns d to call APIs when i the application nee	they are eds. Lean	granted permissions by users/admins a n more about permissions and consent	s part of the consent process. The list of	f configured permissions should
Authentication Certificates & secrets Token configuration API permissions	Applications are authorized include all the permissions	ns d to call APIs when i the application nee Grant admin co	they are eds. Lean	granted permissions by users/admins a n more about permissions and consent r Squadra Technologies	s part of the consent process. The list of	f configured permissions should
Authentication  Certificates & secrets  Token configuration  API permissions  Expose an API	Configured permission Applications are authorized include all the permissions + Add a permission API / Permissions m	ns d to call APIs when t the application nee Grant admin co name Type	they are geeds. Lean onsent for be	granted permissions by users/admins a n more about permissions and consent Squadra Technologies Description	s part of the consent process. The list of Admin consent req	f configured permissions should Status
	Configured permission Applications are authorized include all the permission + Add a permission API / Permissions m Microsoft Greph (4	ns d to call APIs when 1 the application net Grant admin co name Type a)	they are eeds. Lean onsent for	granted permissions by users/admins a n more about permissions and consent squadra Technologies Description	s part of the consent process. The list of Admin consent req	f configured permissions should Status
	Configured permission Applications are authorized include all the permissions + Add a permission API / Permissions in Microsoft Graph (4 Application Ree	ns d to call APIs when i the application nee Grant admin co name Type ad All App	they are reds. Lean onsent for pe	granted permissions by users/admins a n more about permissions and consent squadra Technologies Description Read all applications	s part of the consent process. The list of Admin consent req Yes	f configured permissions should Status
Authentication Cetficiates & secrets Cetficiates & secrets Cetficates & secrets Cetficates & secrets Cetficates & secrets API permissions Expose an API App roles  Preview Owners Cetficates Preview Cetficates	Configured permission Applications are authorized include all the permissions + Add a permission and API / Permissions in Microsoft Graph (4 Application Res DeviceManager	d to call APIs when 1 the application nee Grant admin com name Type ad All App mentManaged[ App	they are teeds. Lean onsent for pe plication	granted permissions by users/admins an more about permissions and consent Squadra Technologies Description Read all applications Read Microsoft Intune devices	s part of the consent process. The list of Admin consent req Yes Ves	configured permissions should Status A Not granted for Squadra G Granted for Squadra Tec
Authentication     Certificates & secrets     Totan configuration     Appendixes     Approxemises     Approals   Preview     Owners     Romers     Manifest	Configured permission: Applications are authorized include all the permissions API / Permissions n MPI / Permissions n Microseft Graph (4 Application Ree DeviceManagem UserRead	ns d to call APIs when i the application ner Grant admin con name Type ad All App mentManaged App Dele	they are seeds. Learn onsent for one plication plication legated	granted permissions by uners/admins an more about permissions and consent Squadra Technologies Description Read all applications Read Microsoft Intune devices Sign in and read user profile	s part of the consent process. The list of Admin consent req., Ves Ves No	Configured permissions should  Status  A Not granted for Squarda,  G Granted for Squarda,  G Granted for Squarda Tec.,  G Granted for Squarda Tec.,

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

+	secRMMIntuneApp_	Application   API perm	issions	¢			×	
20	✓ Search (Ctrl+/) «	🕐 Refresh 🛛 🛇 Got feedback?						
≡ ★	<ul><li>Overview</li><li>Quickstart</li></ul>	Do you want to grant consent for the listed below.	requested pe	ermissions for all accounts in Squadra Technol	logies? This will update any existin	g admin consent records this applic	ation already has to match what is	
2	💉 Integration assistant	Yes No						
1	Manage	organizations where this app will be	used. Learn mo	ставит чагае гоган огданізаціонь пом'єчеї, user соны Уге	en can be customiced per permission,	изег, от арр. тиз социнитиву постепесс	the value in your organization, or in	
<u> </u>	Branding							
	Authentication	Configured permissions						
	📍 Certificates & secrets	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 paeds. Learn more about permissions and consent						
2	Token configuration							
	✤ API permissions	+ Add a permission 🗸 Grant adr	nin consent fo	r Squadra Technologies				
~	🔺 Expose an API	API / Permissions name	Туре	Description	Admin consent req	Status		
•	App roles   Preview	✓ Microsoft Graph (4)						
=	Owners	Application.Read.All	Application	Read all applications	Yes	🛕 Not granted for Squadra ***		
<->	Roles and administrators   Previ	DeviceManagementManaged	Application	Read Microsoft Intune devices	Yes	🥝 Granted for Squadra Tec 🚥		
O	Manifest	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 🚥		
0	Support + Troubleshooting							

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

Home > Squadra Technologies > secR		missions	<b>A</b>		Grant consent
	-Application   API pe	11115510115	<i>M</i>		Grant consent succession
P Search (Ctrl+/) ≪	💍 Refresh 🕴 💝 Got feedbar	ck?			
Overview	G Successfully granted admin co	onsent for the request	ted permissions.		
Quickstart					
💉 Integration assistant					
Manage	The "Admin consent required" organizations where this app w	column shows the d vill be used. Learn m	lefault value for an organization. However, user ore	consent can be customized per permission,	user, or app. This column may not reflect the value in
Eranding					
Authentication	Configured permissions				
📍 Certificates & secrets	Applications are authorized to call include all the nermissions the app	APIs when they are	e granted permissions by users/admins as	part of the consent process. The list of	configured permissions should
Token configuration					
+ API permissions	+ Add a permission 🗸 Gran	it admin consent fo	or Squadra Technologies		
🙆 Expose an API	API / Permissions name	Туре	Description	Admin consent req	Status
🚑 App roles   Preview	✓ Microsoft Graph (4)				
Owners	Application.Read.All	Application	Read all applications	Yes	Granted for Squadra Tec ***
Roles and administrators   Previ	DeviceManagementMan	aged Application	Read Microsoft Intune devices	Yes	Sranted for Squadra Tec ***
Manifest	User.Read	Delegated	Sign in and read user profile	No	S Granted for Squadra Tec •••
Compart + Traublashapting	User.Read.All	Application	Read all users' full profiles	Yes	Sranted for Squadra Tec •••
a support + iroubleshooting					
/ Troubleshooting					

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

Microsoft Azure		$\mathcal P$ Search resources, services, and docs (G+/)
» +	Home > <u>Squadra Technologies</u> >	Application 🛷
<ul> <li>▲</li> <li>★</li> <li>◆</li> <li>♀</li> </ul>	<ul> <li>Security for the security of the</li></ul>	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-952ee47d8252
	<ul> <li>Branding</li> <li>Authentication</li> <li>Certificates &amp; secrets</li> </ul>	Object ID : 4b9/f85e-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 upgra
	<ul> <li>Token configuration</li> <li>API permissions</li> <li>Expose an API</li> <li>App roles   Preview</li> </ul>	Call APIs
■ ⇔ ⊗ •	<ul> <li>Owners</li> <li>Roles and administrators   Previ</li> <li>Manifest</li> </ul>	Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.
0	Support + Troubleshooting	View API permissions

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

$\langle$	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).

Certificate	es & secrets 🛷
💛 Got feedbac	k?
Add a client	secret
Description	
secRMMIntuneA	AppClientSecret
Expires	
🔵 In 1 year	
🔘 In 2 years	
<ul> <li>Never</li> </ul>	
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 🗅 📋

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.

	permissions
	🕐 Refresh
Overview	ddmin conser
<i>Quickstart</i>	Configured pe
Manage	Applications are a
🗮 Branding	all the permission
Authentication	+ Add a pern
📍 Certificates & secrets	API / Perm
Token configuration (preview)	∨Intune (2
API permissions	get_d
🙆 Expose an API	get_d
Owners	✓ Microsot
Roles and administrators (Previ	Devic
0 Manifest	User.I
Support + Troubleshooting	
Troubleshooting	
New support request	

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

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	<pre>"appId": "5a8b3630-4a06-45c6-b229-b80d9ba8ec6f",</pre>
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.



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: AADSTS7000218: 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

🞥 Computer Management			– 🗆 X
File Action View Help			
🗢 🄿 🖄 🖬 🛛 🖬			
E Computer Management (Local	Computer Configuration		Actions
V 👔 System Tools	Name	Value	secRMM 🔺
> ( Task Scheduler	AllowBitLockerOnly		89. SafeCony Approver
> 🛃 Event Viewer	AllowedDirectories		SaleCopy Approver
> 👅 secRMM	AllowedFileExtensions		A Device Tracker
> 👸 Shared Folders	AllowedInternalIds		secRMM License
> 🌆 Local Users and Groups	AllowedPrograms		
> 🐚 Performance	AllowedSerialNumbers		seckivily Configurations
🛔 Device Manager	AllowedUsers		View 🕨
🗸 🔄 Storage	BlockCDROMAndDVDWrites		2 Help
📅 Disk Management	BlockOfficeMacrosOnDevice		и нер
> 🛃 Services and Applications	BlockProgramsOnDevice		RequireMDMEnrollment
	EnableRMS		5.0
	FailWritelfSourceFileUnknown		Edit
	HashAlgorithm		Refresh
	LogSecurityEventsAsFailures		
	LogWriteDetails		и нер
	MonitorCDROMAndDVD	on	
	MonitorFloppyDrive		
	PreApproveSafeCopy		
	RequireMDMEnrollment doul	ble click this row	
	RequireSmartPhoneLogin		
	ScanDevice		
	SUCMConnection		
	SendEmail		
	SNMP		
	Syslog	0.0.4.0	
	version	3.3.4.0	

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 MDM	Require MDM Enrollment	-		×
Mode: Computer , Co	mputer Config: W10			
On Er	force when device is plugged in.			
Required state:	~			
Intune				
Use Intune				
Azure Intune Co	nnection Credentials			
Method:			$\sim$	
TenantID:				
ApplicationID:				
UserID:				
Password:				
	Test			
	OK Cancel C	Clear All		

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)

Micr	rosoft Azure	${\cal P}$ Search resources, services, and docs (G+/)	SecRMM MDM - Require MDM Enrollment -	×
»	Home > Squadra Technologies - App re	Mode: Computer , Computer Config: W10		
+	secRMMIntuneApp		On Enforce when device is plugged in.	
			Required state:	
		📋 Delete   ⊕ Endpoints	Intune	
	Overview	Got a second? We would love your feedback on Microsoft identity platf	tfc Use Intune Azure Intune Connection Credentials	
*	Quickstart	Display name : secRMMIntuneApp	Method: UserIdPassword ~	
٠	Manage	Application (client) ID : fb1abf2e-1225-43c2-bb28-872c96acc816 Directory (tenant) ID : 805a3915-a0ac-4d2a-9ec8-4bb702169c30	TenantID: ApplicationID:	
Ę	🔤 Branding	Object ID : 68ee9250-e227-4708-91b7-3e261ea4a61a	UserID: Azure userid	
•	Authentication		Password: Azure password	
	📍 Certificates & secrets	Welcome to the new and improved App registrations. Looking to	Test	
<b>[</b> ]		· · · · · · · · · · · · · · · · · · ·		

#### Application permission (client secret)

Microsoft Azure $P$ Search resources, services, and docs (G+/)					- ₽		£63	?	$\odot$	Anth	ony@a	nthonys		
» + ✿	Home > Squ secR	adra Technologies >	Арр	Ŵ		Mode:	Computer	V - Ree Compu Enforc	quire MD ter Config e when de	M Enrol : SURFA evice is p	Ilment CEPRO4 olugged in.	-		×
<b>≃</b> li	🔎 Search (Ct	rl+/)	] «	闦 Delete 🌐 Endpoints 🐼 Pro	eview fea	Intune	equired state	e:			~			
⊨	Solution Overview		^	∧ Essentials		√ U:	se Intune							
*-	🍊 Quickstart			Display name secRMMIntuneApp			Azure Intune Method:	e Conne A	ection Creo ppSecret	dentials			~	
<b>◆</b>	💉 Integration	n assistant		Application (client) ID 80591fd3-e68e-4f8c-bb5a-df92994b18	8e3		TenantID:							
<b>-</b>	Manage			Directory (tenant) ID			APplication	iD.	•					5
	🔤 Branding			805a3915-a0ac-4d2a-9ec8-4bb702169	9c30									
	Authentica	ation		Object ID f2ea8fb5-c675-4abf-b7bd-f8fb3f6fc028	8		App Secret:			Test				
(•) •	📍 Certificate	s & secrets												
<b>S</b>	Token con	figuration		<b>()</b> Starting June 30th, 2020 we will no	o longer a									

Micro	osoft Azure	℅ Search resources, service	es, and docs (G+/)			On 🗌 Enfo	orce wh	nen device is plugged in.	
» +	Home > Squ	adra Technologies > secRM	IMIntuneApp   Certificates & seci	rets ጵ	Re Intune Vs	equired state:		~	
	Search (Ct	rl+/) «	Got feedback?		م - ا	Azure Intune Cor Method: TenantID:	AppSe	n Credentials ecret ~	
*	Overview     Quickstart     Integration	n assistant	Thumbprint	Start date	-	ApplicationID:	Azur	re client secret	
<b>R</b>	Manage		No certificates have been added	for this application.		Appseciet.	71201	Test	
	<ul> <li>Branding</li> <li>Authentica</li> </ul>	ation	Client secrets	n usas ta prova ite idant	ity				
<ul> <li>3</li> <li>3</li> <li>4</li> <li>4</li></ul>	Certificate     Token con	figuration	A secret suring that the application     password.	in uses to prove its ident	ity		ок	Cancel Clear All	
8 8	<ul> <li>API permis</li> <li>Expose an</li> </ul>	API	Description	Expires	Value			ID	
	🏝 App roles	Preview	secRMMIntuneAppClientS	12/31/2299	srF.N6CRw	v2g-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 MDM - Require MDM Enrollment - 🗆 🗙	SecRMM MDM - Require MDM Enrollment – 🗆 🗙
Mode: Computer , Computer Config: W10	Mode: Computer , Computer Config: SURFACEPRO4
n Enforce when device is plugged in.	🗹 🕐 🔲 Enforce when device is plugged in.
Required state: Enrolled V	Required state: Enrolled ~
Intune	Intune
☑ Use Intune	Use Intune
Azure Intune Connection Credentials	Azure Intune Connection Credentials
Method: UserIdPassword ~	Method: AppSecret ~
TenantID: 805a3915-a0ac-4d2a-9ec8-4bb702169c30	TenantID: 805a3915-a0ac-4d2a-9ec8-4bb702169c30
ApplicationID: [b1abf2e-1225-43c2-bb28-872c96acc816	ApplicationID: 80591fd3-e68e-4f8c-bb5a-df92994b18e3
UserID: anthony@anthonysquadratechnologies.onmic	
Password:	App Secret:
Test	Test
OK Cancel Clear All	OK Cancel Clear All
	1
Microsoft Intune connection	test X
IntuneGraphApi Te	stintuneConnections succeeded
Intune Authentical	tion Token (first 10 bytes): eyJ0eXAiOi
-	
	ОК

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.

📴 se	Ber secRMM Event Viewer: localhost, event log secRMM						
Row	β	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&1cbba703&0&0000#{6ac27878-a6fa-4155-ba85f9&f491d4f33}					
	Additional Info	SerialNumber=F17STK9XHG7K, BluetoothAddress=d0:c5f3:31:59:b0, EthemetAddress=d0:c5f3:31:59:b1, WiFiAddress=	d0:c5.f3:31:	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.

Ber secRMM Event Viewer: archive file X:\temp.evtx − □					
Row: 11	Previous Next				
Nome	Velue				
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&000#{6ac27878-a6fa	a-4155-b	a85-f98f4		
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	СОРУ				
	·				
<			>		

# **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)

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/