



Security Removable Media Manager
(secRMM)

Intune Installation Guide

Version 9.11.27.0

(April 2024)

Protect your valuable data



secRMM Intune Installation Guide

© 2011 Squadra Technologies, LLC. ALL RIGHTS RESERVED.

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

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

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

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

TRADEMARKS

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

Disclaimer

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

Squadra Technologies Administrator Guide
Created - March 2011

Contents

- INTRODUCTION4
- PREREQUISITES.....4
- SETUP OVERVIEW.....4
- SETUP DETAILS6
 - Deploy secRMM using an Intunewin file.....6*
 - secRMM License file22*
 - Create an Intunewin file22
 - Deploy the Intunewin file within Intune23
 - Configure a secRMM policy using Intune Powershell scripts.....42*
 - User deployment requirements.....48*
- TROUBLESHOOTING49
- CONTACTING SQUADRA TECHNOLOGIES SUPPORT49
- ABOUT SQUADRA TECHNOLOGIES, LLC.49

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.

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.

This document is focused on how to install (deploy) and configure secRMM using the Microsoft Azure Intune software.

secRMM is also integrated into Intune so that mobile devices will not be allowed to either mount over USB or to prevent file copies to the mobile device over USB if that mobile device is not enrolled (or compliant) within Intune. To setup this feature, there is a separate secRMM document titled "Intune Access Control Setup Guide" which is available on the Squadra Technologies web site.

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 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 deploy and configure secRMM using Microsoft Azure Intune.

1. Deploy secRMM using an Intunewin file
2. Deploy secRMM license file using an Intunewin file
3. Configure secRMM computer and/or user policies using the secRMM Policy Configurator tool.
The secRMM Policy Configurator tool generates Intune Powershell scripts which can be deployed to 'Windows devices' and/or 'user groups'.
The secRMM Policy Configurator tool has a separate secRMM Administrator Guide which you can

secRMM Intune Installation Guide

download from the Squadra Technologies website.

secRMM Optional Features



SCCM Admin Guide (PDF)



SCOM Admin Guide (PDF)



secRMMCentral Admin Guide (PDF)



Excel AddIn Admin Guide (PDF)



Azure Intune Admin Guide (MDM) (PDF)



Azure Monitor Admin Guide (PDF)



Azure Sentinel Admin Guide (SIEM) (PDF)



**Azure Defender for Cloud Admin
Guide (PDF)**



**Azure Verifiable Credentials Admin
Guide (PDF)**

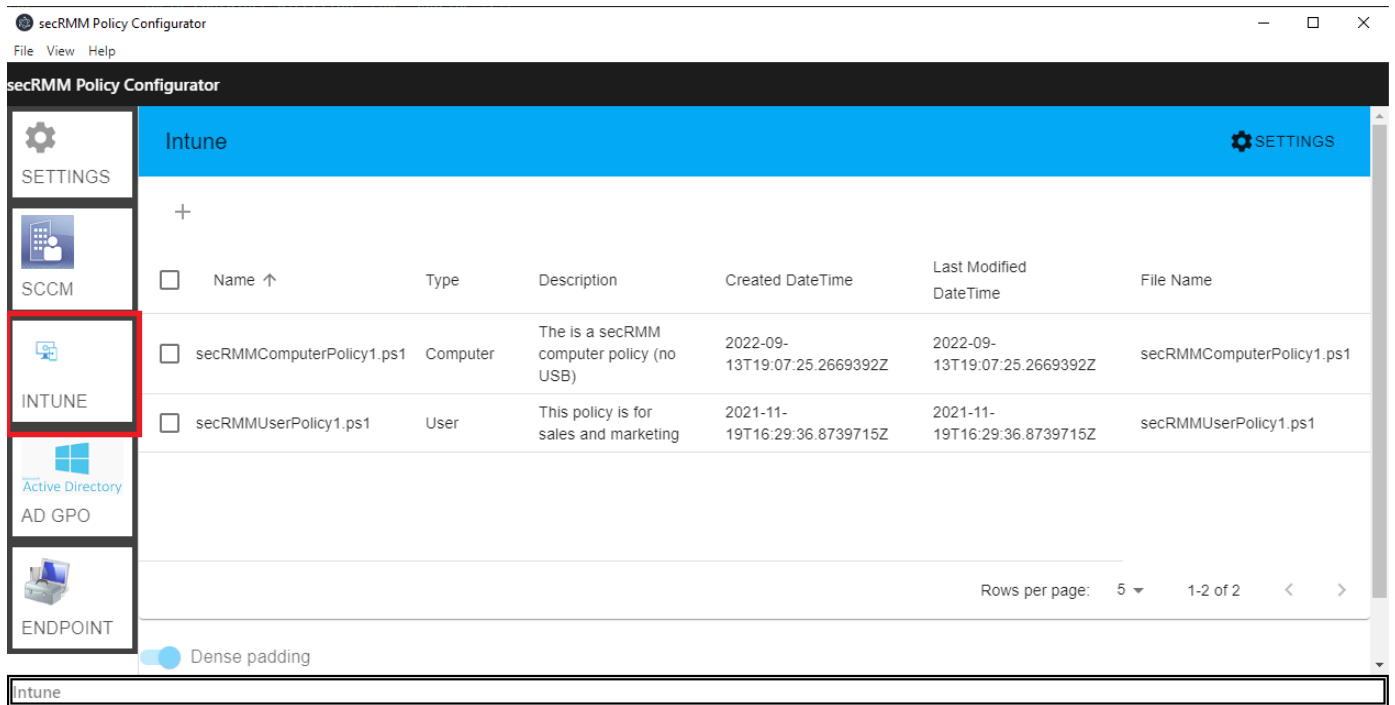


**Policy Configurator Admin Guide (Intune,
SCCM, AD GPO, Endpoints) (PDF)**



SDK Programmers Guide (PDF)

secRMM Intune Installation Guide



Setup details

Deploy secRMM using an Intunewin file

The Microsoft documentation titled "Intune Standalone - Win32 app management" at:

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-win32-app-management>

describes how to deploy the secRMM installation file using a Intunewin file (within Intune).

Download the IntuneWin file for secRMM from the Squadra Technologies web site. Extract the zip file so that you have the secRMMInstallx64.intunewin file extracted. Just remember where you downloaded/extracted the secRMMInstallx64.intunewin file because you are going to need to upload to Intune in a step below.

secRMM Downloads

▷ Overview

▷ Download

▷ Documentation

▷ Video

Screenshots

▷ Features

▷ Release Notes

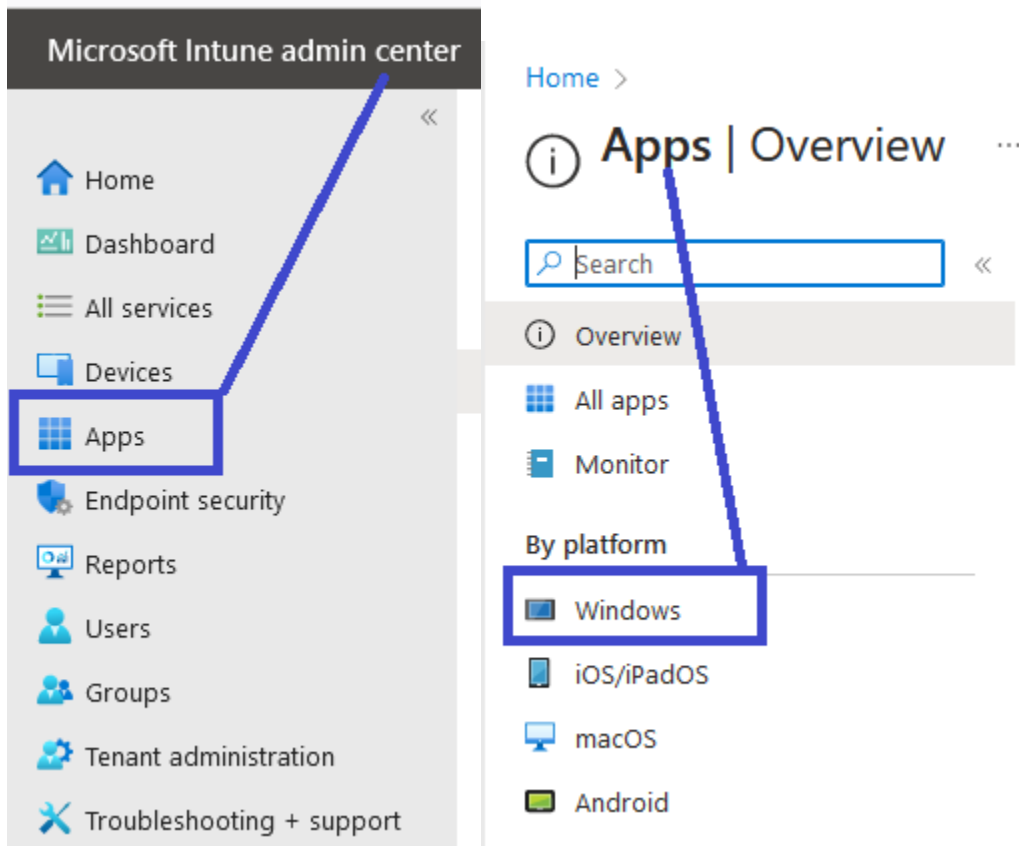


Home >> secRMM >> Downloads

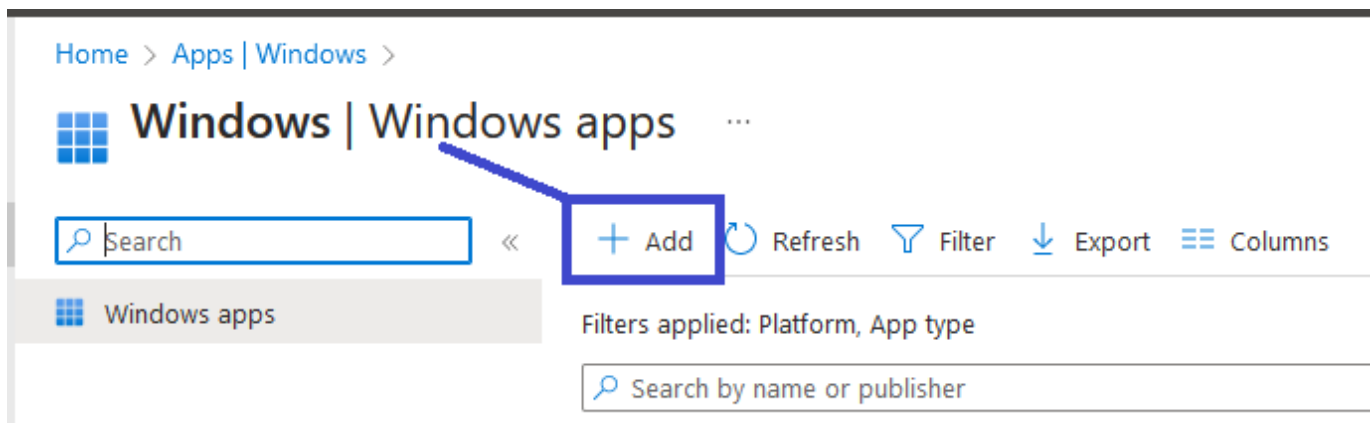
Please select a link(s) from the list below. Fully functional 30 day free trial.

Item	Download link
Prerequisite: Microsoft Universal C Runtime Update 3 (current MS patches contain this) Please note that secRMM will not install without this Microsoft software.	Microsoft download center
secRMM x64 install (msi)	secRMMInstallx64.zip
secRMM x86 install (msi)	secRMMInstallx86.zip
secRMM x64 IntuneWin file	secRMMInstallx64IntuneWin.zip
Administrators Guide	secRMMAdministratorGuide.pdf left click to view online right click and then "Save As" to download
Additional downloads	Additional optional downloads

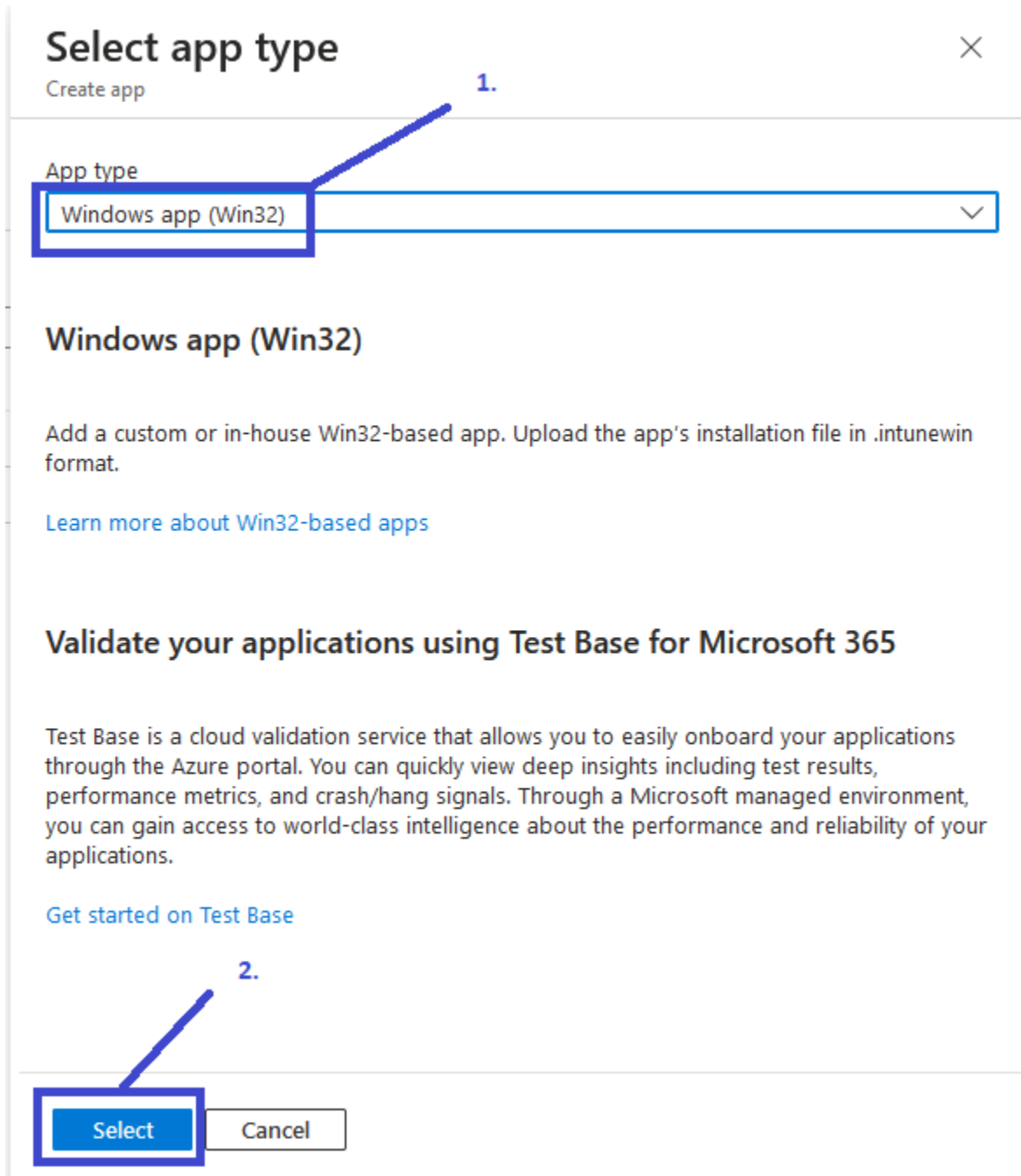
Using your web browser, go into the Microsoft Intune admin center at <https://intune.microsoft.com/#home>. Select 'Apps' and then under Apps->'By platform', select Windows.



Click the Add button



For App type, select 'Windows app (Win32)' and click the 'Select' button.



Select app type ×

Create app

App type

Windows app (Win32) ▼

Windows app (Win32)

Add a custom or in-house Win32-based app. Upload the app's installation file in .intunewin format.

[Learn more about Win32-based apps](#)

Validate your applications using Test Base for Microsoft 365

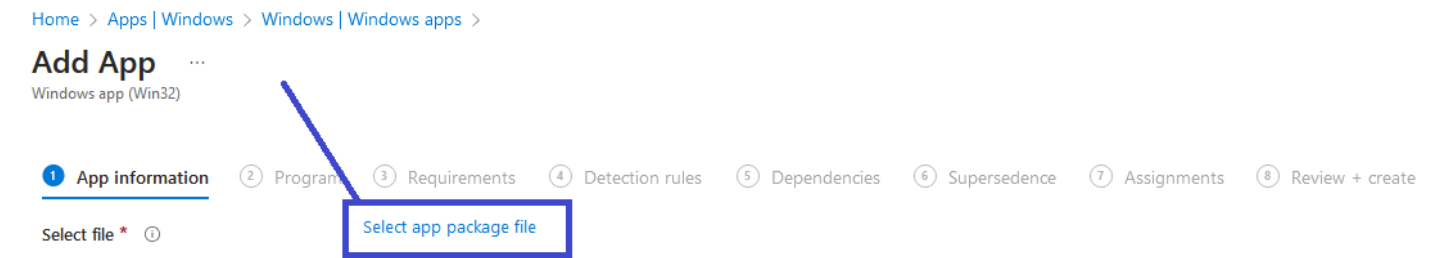
Test Base is a cloud validation service that allows you to easily onboard your applications through the Azure portal. You can quickly view deep insights including test results, performance metrics, and crash/hang signals. Through a Microsoft managed environment, you can gain access to world-class intelligence about the performance and reliability of your applications.

[Get started on Test Base](#)

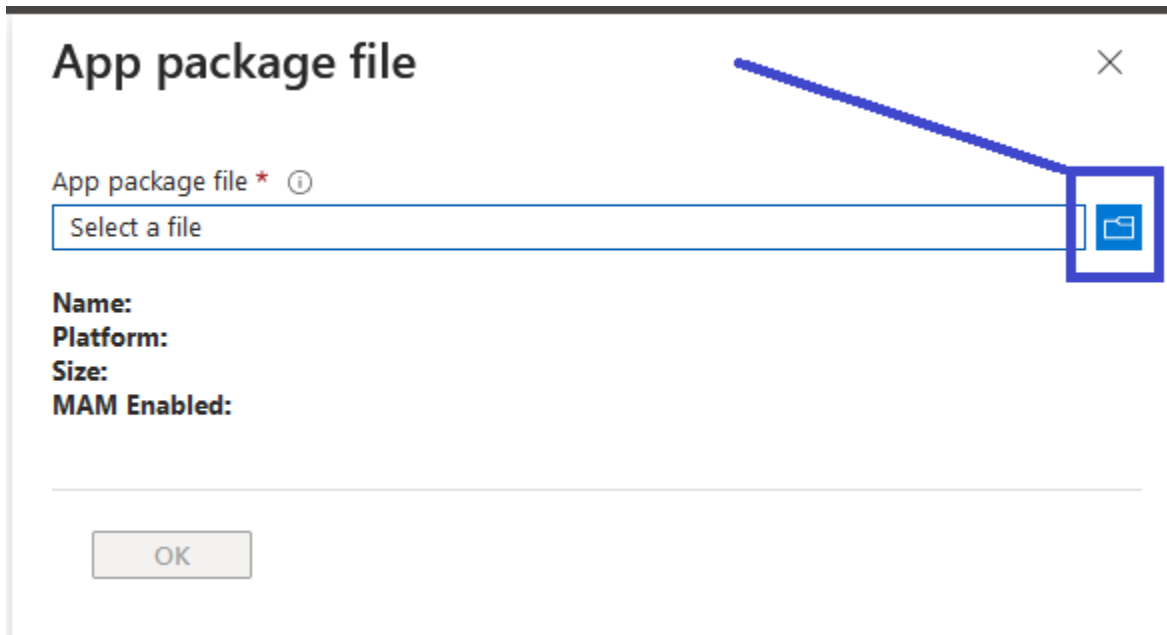
Select Cancel

Click the 'Select app package file' link.

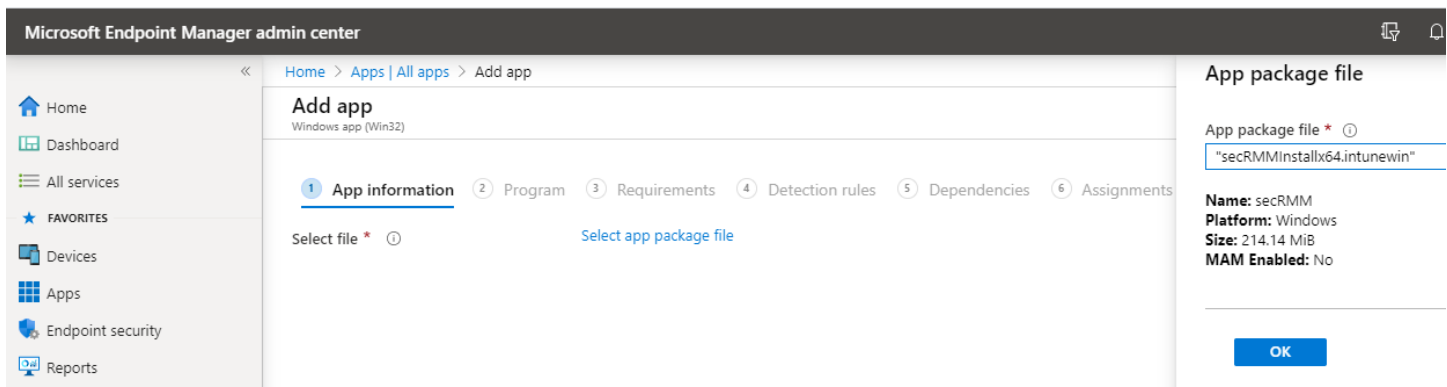
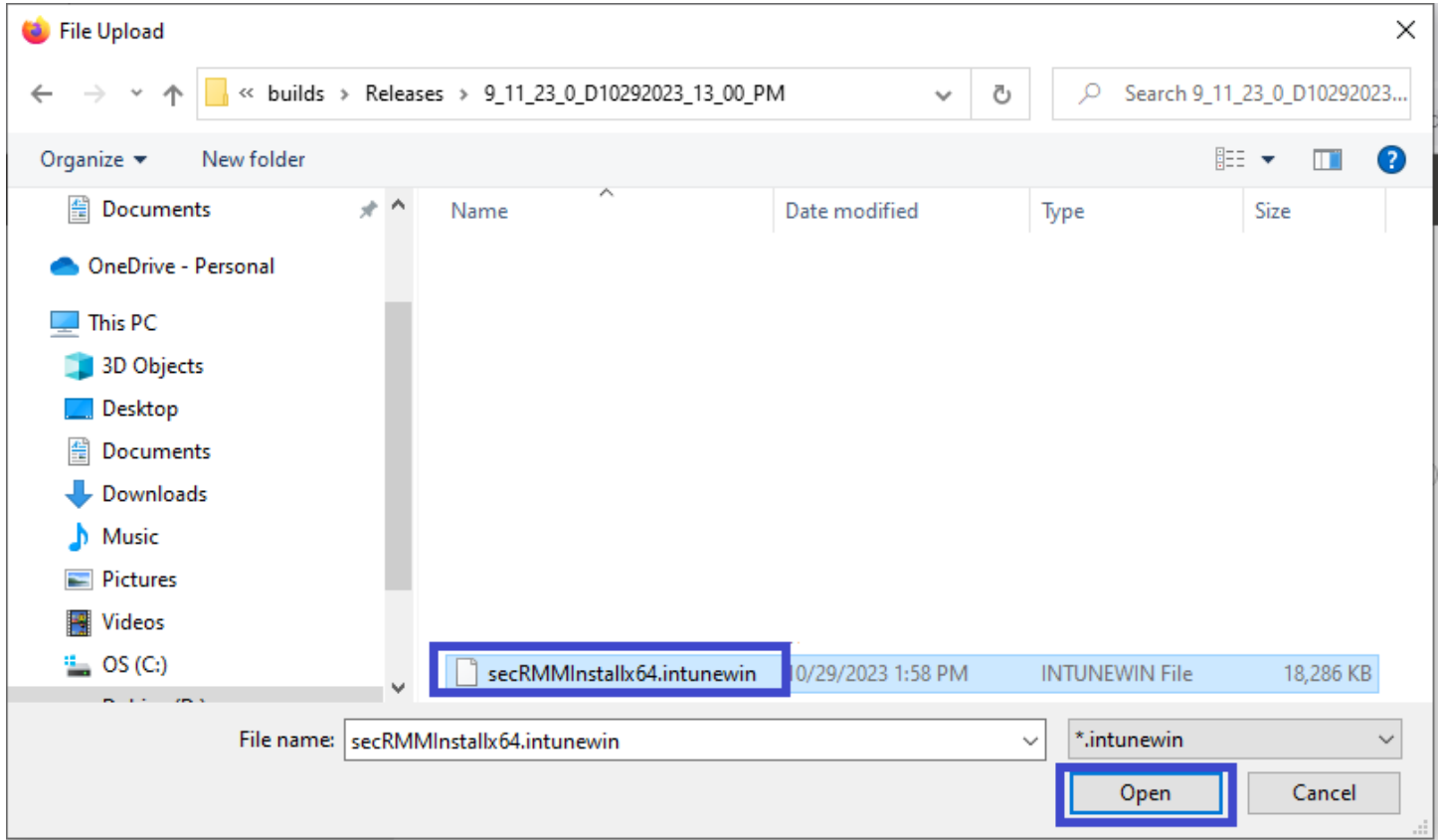
secRMM Intune Installation Guide



Now upload the secRMMInstallx64.intunewin file into Intune.




secRMM Intune Installation Guide



App package file


×

App package file * ⓘ



Name: secRMM
Platform: Windows
App version: 9.11.23.0
Size: 17.86 MiB
MAM Enabled: No

OK



secRMM Intune Installation Guide

Home > Apps | Windows > Windows | Windows apps >

Add App

Windows app (Win32)

1 App information 2 Program 3 Requirements 4 Detection rules 5 Dependencies 6 Supersedence

Select file * ⓘ [secRMMInstallx64.intunewin](#)

Name * ⓘ

Description * ⓘ

[Edit Description](#)

Publisher * ⓘ 1.

App Version ⓘ

Category ⓘ 2. ▼

Show this as a featured app in the Company Portal ⓘ ☐ Yes ☒ No

Information URL ⓘ

Privacy URL ⓘ

Developer ⓘ

Owner ⓘ

Notes ⓘ

Logo ⓘ [Select image](#)

3.

Suppressing a reboot during a secRMM upgrade

You can prevent secRMM from rebooting after a secRMM upgrade by specifying:

secRMM Intune Installation Guide

msiexec /i "secRMMInstallx64.msi" /qn **REBOOT=ReallySuppress /norestart** in the 'Install command' field.

[Home](#) > [Apps | Windows](#) > [Windows | Windows apps](#) >

Add App ...

Windows app (Win32)

- ☒ App information **☒ 2 Program** ☐ 3 Requirements ☐ 4 Detection rules ☐ 5 Dependencies ☐ 6 Supersedence

Specify the commands to install and uninstall this app:

Install command * ⓘ	<input qn"="" secrmminstallx64.msi"="" type="text" value="msiexec /i "/>	✓
Uninstall command * ⓘ	<input qn"="" type="text" value="msiexec /x " {e2a5417a-4b16-44d5-9171-a68967f82c22}"=""/>	✓
Installation time required (mins) ⓘ	<input type="text" value="60"/>	
Allow available uninstall ⓘ	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Install behavior ⓘ	<input checked="" type="radio"/> System <input type="radio"/> User	
Device restart behavior ⓘ	<input type="text" value="App install may force a device restart"/>	▼

Specify return codes to indicate post-installation behavior:

Return code	Code type	
<input type="text" value="0"/>	<input type="text" value="Success"/>	▼ 🗑️
<input type="text" value="1707"/>	<input type="text" value="Success"/>	▼ 🗑️
<input type="text" value="3010"/>	<input type="text" value="Soft reboot"/>	▼ 🗑️
<input type="text" value="1641"/>	<input type="text" value="Hard reboot"/>	▼ 🗑️
<input type="text" value="1618"/>	<input type="text" value="Retry"/>	▼ 🗑️

+ Add

secRMM Intune Installation Guide

Home > Apps | Windows > Windows | Windows apps >

Add App

Windows app (Win32)

✓ App information ✓ Program **3 Requirements** ④ Detection rules ⑤ Dependencies ⑥ Supersedeance ⑦ Assignments ⑧ Review + create

Specify the requirements that devices must meet before the app is installed:

Operating system architecture * ① **64-bit** 1.

Minimum operating system * ① **Windows 10 1607** 2. *might be different in you environment*

Disk space required (MB) ①

Physical memory required (MB) ①

Minimum number of logical processors required ①

Minimum CPU speed required (MHz) ①

Configure additional requirement rules

Type	Path/Script
No requirements are specified.	

+ Add 3.

For 'Add a Requirement rule' (you may want to copy-and-paste these values so they are not mistyped):
Path = C:\Windows\system32\
File or folder = vcruntime140.dll

Add a Requirement rule

Create a requirement.

Requirement type * ① **File** 1.

Path * ① **C:\Windows\system32** 2. ✓

File or folder * ① **vcruntime140.dll** 3. ✓

Property * ① **File or folder exists** 4.

Associated with a 32-bit app on 64-bit clients ① ☐ Yes ☒ No

OK 5.

secRMM Intune Installation Guide

[Home](#) > [Apps | Windows](#) > [Windows | Windows apps](#) >

Add App ...

Windows app (Win32)

✓ App information ✓ Program **3 Requirements** ④ Detection rules ⑤ Dependencies ⑥ Supersede

Specify the requirements that devices must meet before the app is installed:

Operating system architecture * ⓘ	64-bit	▼
Minimum operating system * ⓘ	Windows 10 1607	▼
Disk space required (MB) ⓘ	<input type="text"/>	
Physical memory required (MB) ⓘ	<input type="text"/>	
Minimum number of logical processors required ⓘ	<input type="text"/>	
Minimum CPU speed required (MHz) ⓘ	<input type="text"/>	

Configure additional requirement rules

Type	Path/Script	
File	C:\Windows\system32\	...

+ Add

Previous

Next

secRMM Intune Installation Guide

Home > Apps | Windows > Windows | Windows apps >

Add App

Windows app (Win32)

✓ App information ✓ Program ✓ Requirements **4 Detection rules** 5 Dependencies 6 Supersedence 7 Assignments 8 Review + create

Configure app specific rules used to detect the presence of the app.

Rules format * ⓘ Manually configure detection rules 1.

Type	Path/Code
No rules are specified. 2.	

+ Add ⓘ

Note that Intune figures out the 'MSI product code' (see screenshot below) for you by reading the secRMMInstallx64.intunewin file you supplied above. Every secRMM version will have a unique 'MSI product code'. If you want to ever check what secRMM product code is installed on one of your computers, you can run the program:

C:\Program Files\secRMM\AdminUtils\GetSecRMMProductCode.cmd

Detection rule

Create a rule that indicates the presence of the app.

Rule type * ⓘ MSI

MSI product code * ⓘ {E2A5417A-4B16-44D5-9171-A68967F82C22} ✓

MSI product version check ⓘ Yes No

OK

secRMM Intune Installation Guide

Home > Apps | Windows > Windows | Windows apps >

Add App

Windows app (Win32)

✓ App information ✓ Program ✓ Requirements **4 Detection rules** 5 Dependencies 6 Supersedece 7 Assignments 8 Review + create

Configure app specific rules used to detect the presence of the app.

Rules format * ⓘ Manually configure detection rules

Type	Path/Code
MSI	{E2A5417A-4B16-44D5-9171-A68967F82C22} ...

+ Add ⓘ

Previous Next

Home > Apps | Windows > Windows | Windows apps >

Add App

Windows app (Win32)

✓ App information ✓ Program ✓ Requirements ✓ Detection rules **5 Dependencies** 6 Supersedece 7 Assignments 8 Review + create

Software dependencies are applications that must be installed before this application can be installed. To automatically install a child dependency app before installing the current parent app, enable the automatically install option. To only install the current parent app if the child dependency app is already detected on the device, disable the automatically install option. There is a maximum of 100 child dependency apps, including references to other apps outside of this view, forming a graph of apps. The total size of the dependency app graph is limited to the maximum of 100 plus the parent app (101 total). [Learn more](#)

Name	Automatically Install
No results.	

+ Add ⓘ

Previous Next

secRMM Intune Installation Guide

Home > Apps | Windows > Windows | Windows apps >

Add App

Windows app (Win32)

✓ App information ✓ Program ✓ Requirements ✓ Detection rules ✓ Dependencies **6 Supersede** 7 Assignments 8 Review + create

When you supersede an application, you can specify which apps will be directly updated or replaced. To update an app, disable the uninstall previous version option. To replace an app, enable the uninstall previous version option. There is a maximum of 10 updated or replaced apps, including references to other apps outside of this view, forming a graph of apps. The total size of the supersedence app graph is limited to the maximum of 10 plus the parent app (11 total). [Learn more](#)

Apps that this app will supersede

Name	Publisher	Version	Uninstall previous version
No results.			

+ Add ⓘ

Previous **Next**

The Assignments page is where you will assign the secRMM installation to either a group of computer or users. Logically, we think it makes the most sense to make assignments to computers but it works just the same if you chose to use user groups.

Home > Apps | Windows > Windows | Windows apps >

Add App

Windows app (Win32)

✓ App information ✓ Program ✓ Requirements ✓ Detection rules ✓ Dependencies ✓ Supersede **7 Assignments** 8 Review + create

ⓘ Any Win32 app deployed using Intune will not be automatically removed from the device when the device is retired. The app and the data it contains will remain on the device. If the app is not removed prior to retiring the device, the end user will need to take explicit action on the device to remove the app.

Required ⓘ

Group mode	Group	Filter mode	Filter	End user notifications	Availability	Installation deadline	Restart grace period	Delivery optimization ...
No assignments								

+ Add group ⓘ + Add all users ⓘ + Add all devices ⓘ

Available for enrolled devices ⓘ

Group mode	Group	Filter mode	Filter	End user notifications	Availability	Restart grace period	Delivery optimization pri...
No assignments							

+ Add group ⓘ + Add all users ⓘ + Add all devices ⓘ

Uninstall ⓘ

Group mode	Group	Filter mode	Filter	End user notifications	Availability	Installation deadline	Restart grace period	Delivery optimization ...
No assignments								

+ Add group ⓘ + Add all users ⓘ + Add all devices ⓘ

Previous **Next**

secRMM Intune Installation Guide

The next screenshot is an example of the steps. Your environment will likely have different group names (than our Intune development/demo environment) however, at least you can see what it will look like when you make the assignments.

The screenshot displays the Microsoft Intune console interface for adding an application. The left pane, titled 'Add App', shows the 'Required' section with a 'Group mode' dropdown set to 'No assignments'. A blue box highlights the '+ Add group' button, with a callout '1.' pointing to it. Below this, the 'Available for enrolled devices' section also has a 'Group mode' dropdown set to 'No assignments'. The right pane, titled 'Select groups', shows a list of groups. A blue box highlights the 'secRMMComputerGroup' row, which is selected, with a callout '2.' pointing to it. At the bottom of the right pane, a blue box highlights the 'Select' button, with a callout '3.' pointing to it. The 'Selected (1)' pane on the far right shows the 'secRMMComputerGroup' has been added to the selection.

Name	Type	Details
<input type="checkbox"/> A group with a space	Group	
<input type="checkbox"/> AAD DC Administrators	Group	
<input type="checkbox"/> ContainsSubGroups	Group	
<input type="checkbox"/> SalesAndMarketing	Group	
<input checked="" type="checkbox"/> secRMMComputerGroup	Group	

secRMM Intune Installation Guide

Home > Apps | Windows > Windows | Windows apps >

Add App

Windows app (Win32)

✓ App information ✓ Program ✓ Requirements ✓ Detection rules ✓ Dependencies ✓ Supersedence ✓ Assignments **8 Review + create**

Summary

App information

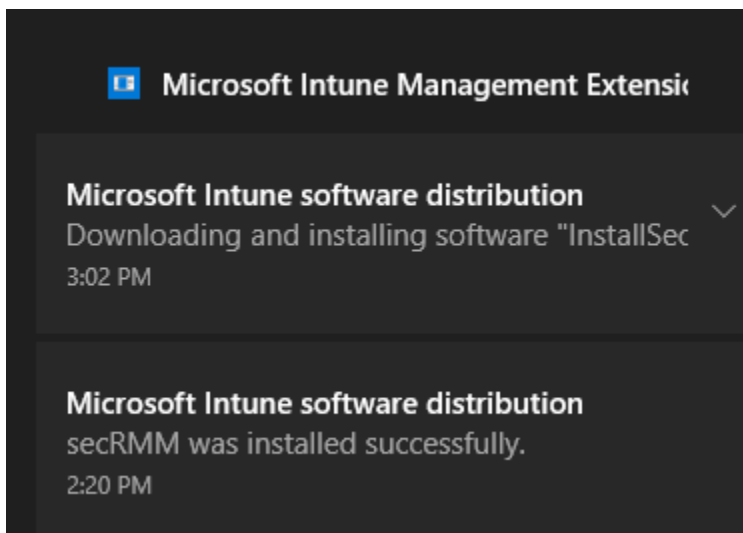
App package file	secRMMInstallx64.intunewin
Name	secRMM
Description	<input type="text" value="secRMM"/>
Publisher	squadra technologies
App Version	9.11.23.0
Category	No Category
Show this as a featured app in the Company Portal	No
Information URL	No Information URL
Privacy URL	No Privacy URL
Developer	No Developer
Owner	No Owner
Notes	No Notes
Logo	No logo

Program

Install command	msiexec /i "secRMMInstallx64.msi" /qn
Uninstall command	msiexec /x {E2A5417A-4B16-44D5-9171-A68967F82C22} /qn
Installation time required (mins)	60
Allow available uninstall	Yes
Install behavior	System
Device restart behavior	App install may force a device restart

[Previous](#) [Create](#)

Now secRMM will be deployed to the Windows 10/11 computers being managed by Microsoft Azure Intune.



secRMM Intune Installation Guide

secRMM License file

Create an Intunewin file

The secRMM license file needs to be copied to each computer running secRMM in your environment. You receive the secRMM license file from Squadra Technologies. If you are deploying secRMM with Intune for a test and do not yet have a secRMM license file, you can skip this step. secRMM will run (fully functional) for 30 days. Once you do get a secRMM license file, you can come back to this section.

The secRMM license file is deployed with Intune using an Intunewin file. The install and uninstall scripts are in the secRMMDeployment.zip (in the Licensing\Distribution\Intune directory) which you can download from the Squadra Technologies web site.

<https://www.squadratechnologies.com/Products/secRMM/secRMMDownloads3.aspx>

Developed in USA

search...
☐ only search Squadra Technologies

[home](#) [software](#) [hardware](#) [services](#) [partners](#) [company](#) [Video](#) [Blog](#) [Microsoft System Center](#) [Microsoft Azure](#)

secRMM Optional Downloads

- Overview
- Download**
- Documentation
- Video
- Blogs
- Screenshots
- Features
- Release Notes
- Pricing



[Home >> secRMM >> Downloads > Optional Downloads](#)

Item	Download link
Microsoft System Center/Azure	secRMM System Center/Azure
secRMM Policy Configurator	secRMMPolicyConfigurator.zip (9_11_18_0)
secRMM Excel Addin	secRMMExcelAddin
secRMM Charts	secRMMCharts.zip (9_11_18_0)
secRMM Central	secRMMCentral
secRMM Reports	secRMMReports
secRMM Deployment tools	secRMMDeployment.zip
secRMM SNMP MIB file	secRMMSNMP-MIB.txt right click and then "Save As" to download
secRMM Smart Phone Apps	secRMM Smart Phone Apps
Hardware Vendor Freeware version(s)	Apricorn secRMM Freeware version
NIST SP 800-171 compliance tool	secRMM_NIST_SP_800-171.zip

**Get In Touch**

Would you like to find out more or begin working with Squadra? We look forward to hearing from you. Please contact us today to get started!

Contact Us

" We searched around for a solution like secRMM and couldn't quite find the right fit. secRMM is exactly what we were looking for. "

 Windows Systems Administrator.

secRMM Intune Installation Guide

After you have unzipped the secRMMDeployment.zip, follow the steps below:

1. copy the secRMM license file(s) for your company to the source_folder directory (Licensing\Distribution\Intune\source_folder). You get the secRMM license file(s) from Squadra technologies. Please email support@squadratechnologies.com to request your license file(s).

If you want to customize the secRMM error message to the end-user, copy a secRMMErrorMessageToEndUser.txt file to the source_folder directory (Licensing\Distribution\Intune\source_folder).

If you want to customize the secRMM.ini file, copy a secRMM.ini file to the source_folder directory (Licensing\Distribution\Intune\source_folder).

2. Run the batch file CreateIntuneWinAppForSecRMMLicense.cmd which is in the directory Licensing\Distribution\Intune. NOTE: You must run this as an Administrator account and 'Run As Administrator'.

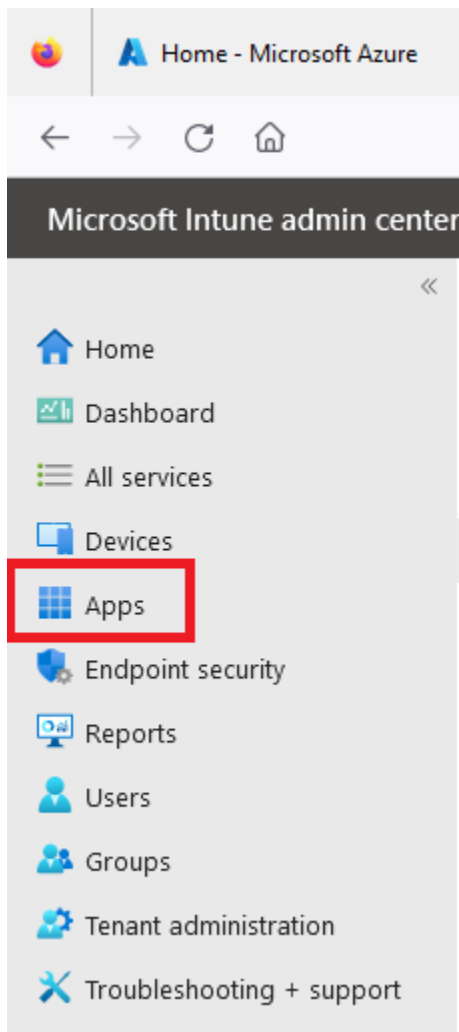
3. The output of step 2 above is the Intune WinApp file. It is located in the output_folder directory ((Licensing\Distribution\Intune\output_folder)). The name of the Intune WinApp file is InstallSecRMMLicenseViaIntune.intunewin.

Deploy the Intunewin file within Intune

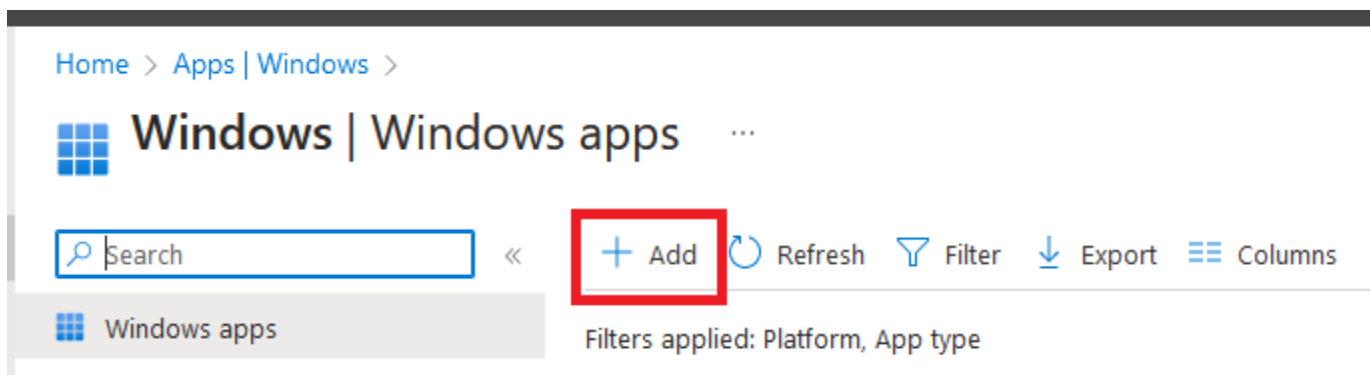
Now that you have created an Intunewin file that will deploy the secRMM license file (from the section above), you can deploy the Intunewin file using Intune.

From the Intune admin center, click Apps as shown in the screenshot below.

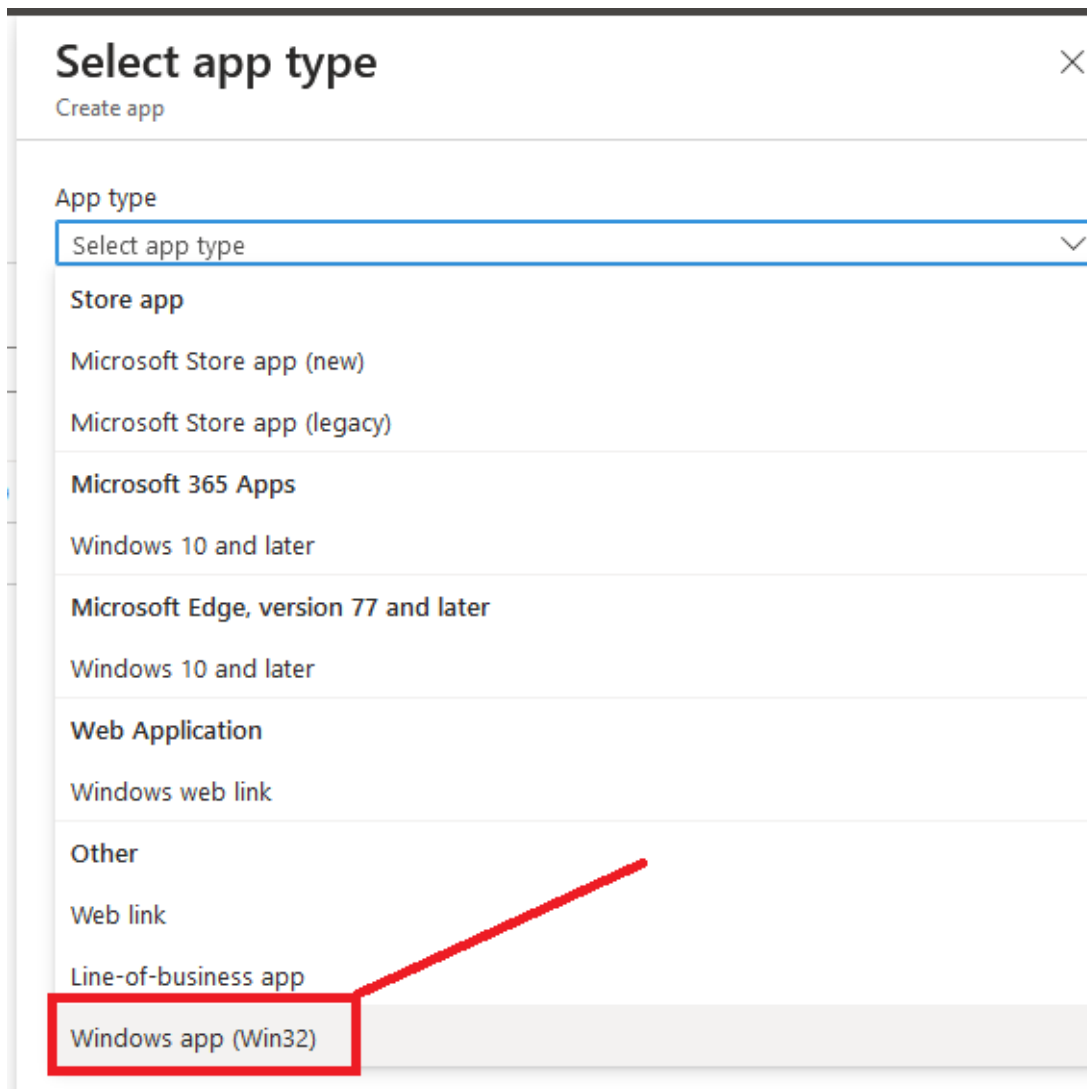
secRMM Intune Installation Guide



Click Add as shown in the screenshot below.



Select 'Windows app (Win32)' as the 'App type' as shown in the screenshot below.



Select app type ×

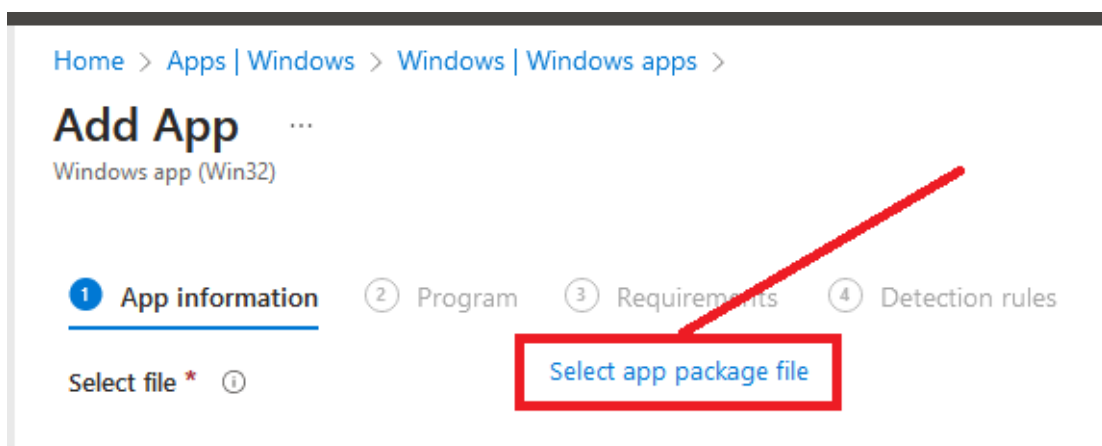
Create app

App type

Select app type ▼

- Store app
 - Microsoft Store app (new)
 - Microsoft Store app (legacy)
- Microsoft 365 Apps
 - Windows 10 and later
 - Microsoft Edge, version 77 and later
 - Windows 10 and later
- Web Application
 - Windows web link
- Other
 - Web link
 - Line-of-business app
 - Windows app (Win32)**

Click the 'Select app package file' as shown in the screenshot below.



Home > Apps | Windows > Windows | Windows apps >

Add App ...

Windows app (Win32)

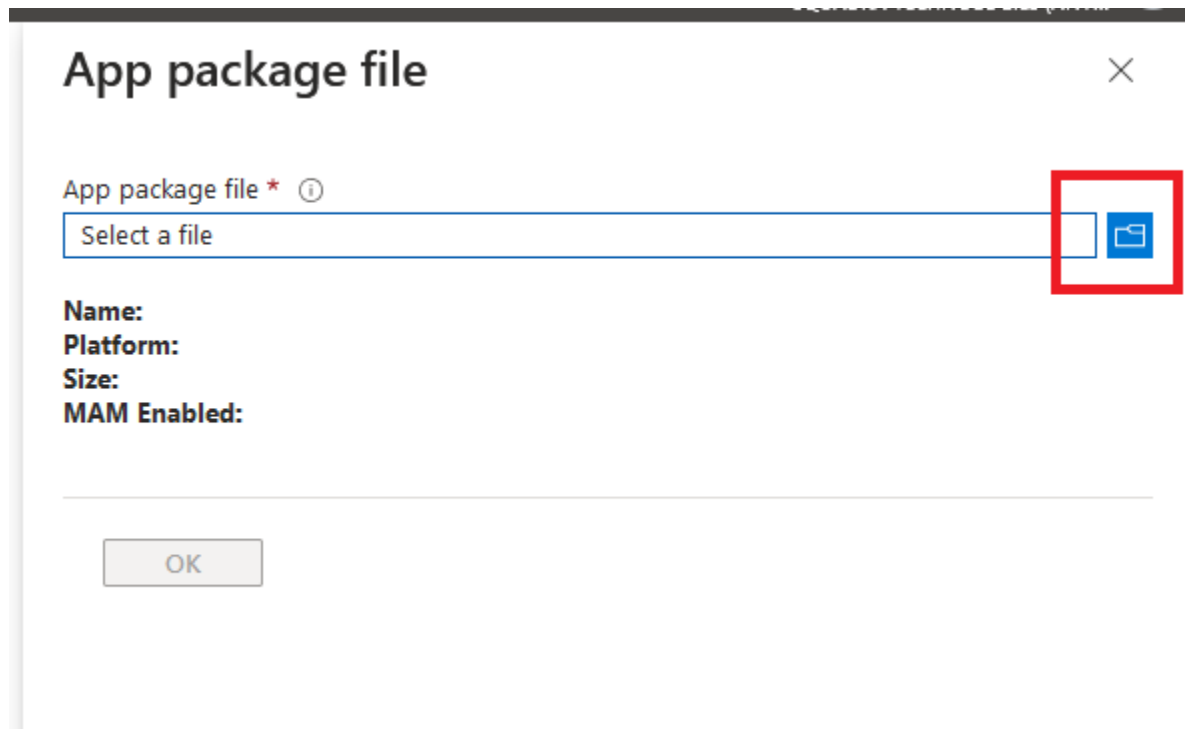
1 App information 2 Program 3 Requirements 4 Detection rules

Select file * ⓘ

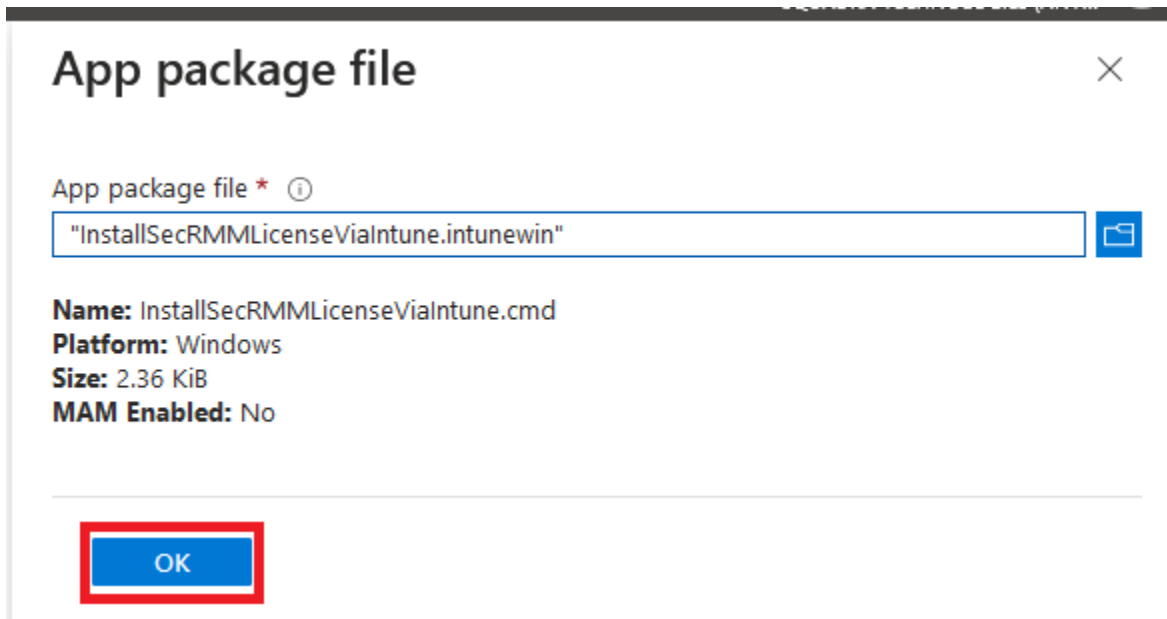
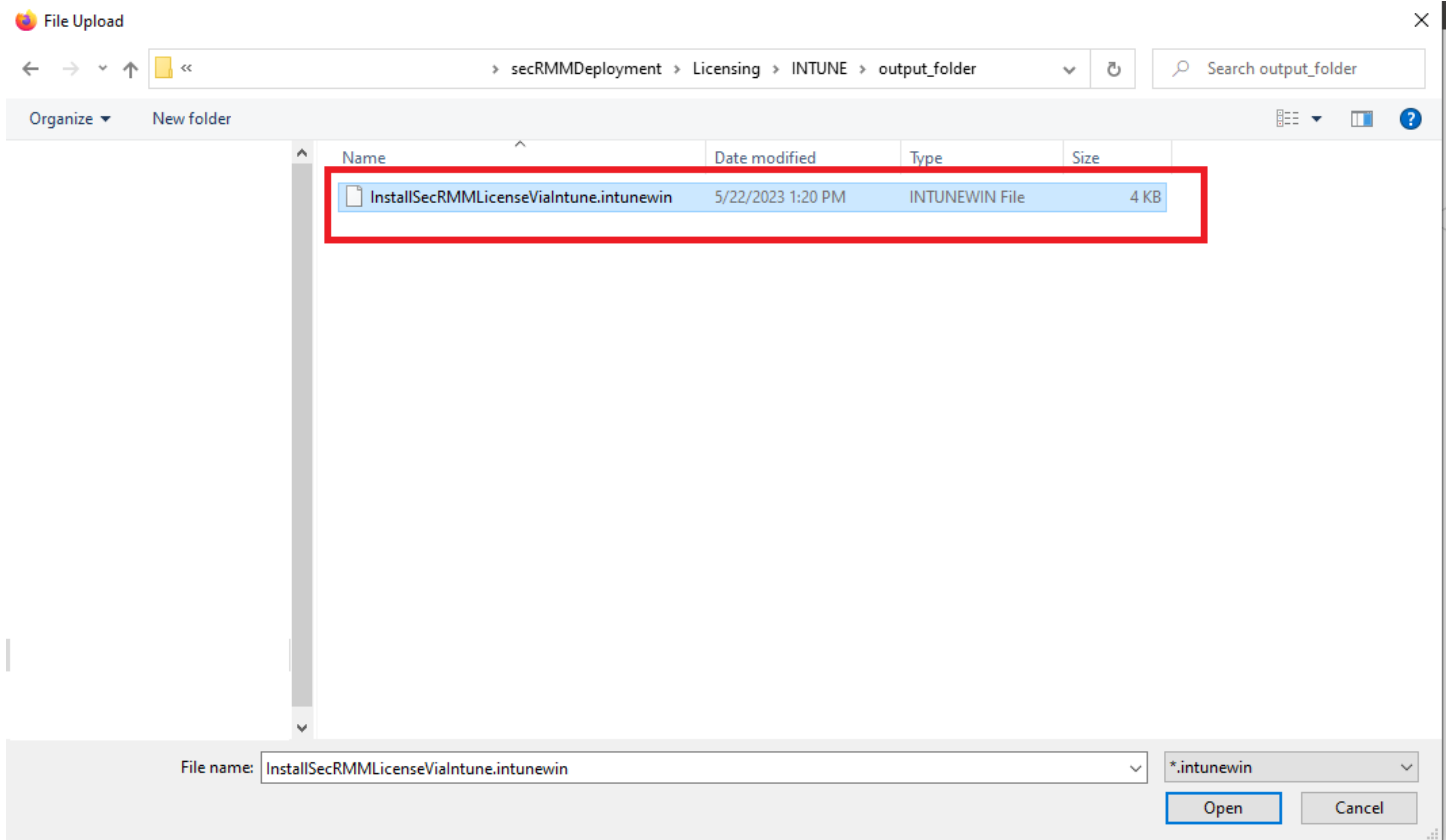
Select app package file

secRMM Intune Installation Guide

Select the InstallSecRMMLicenseViaIntune.intunewin file that is in the output_folder (you created this Intunewin file above in the section subtitled 'Create an Intunewin file') as shown in the 3 screenshots below.



secRMM Intune Installation Guide



In the 'App information' tab, enter 'Squadra Technologies' as the 'Publisher' and then click the 'Next' button as shown in the screenshot below.

secRMM Intune Installation Guide

[Home](#) > [Apps | Windows](#) > [Windows | Windows apps](#) >

Add App ...

Windows app (Win32)

- 1 App information** 2 Program 3 Requirements 4 Detection rules 5 Dependencies 6 Supersedence

Select file * ⓘ

[InstallSecRMMLicenseViaIntune.intunewin](#)

Name * ⓘ

InstallSecRMMLicenseViaIntune.cmd

Description * ⓘ

InstallSecRMMLicenseViaIntune.cmd

[Edit Description](#)

Publisher * ⓘ

Squadra Technologies

App Version ⓘ

Enter the app version

Category ⓘ

0 selected

Show this as a featured app in the Company Portal ⓘ

Yes

No

Information URL ⓘ

Enter a valid url

Privacy URL ⓘ

Enter a valid url

Developer ⓘ

Owner ⓘ

Notes ⓘ

Logo ⓘ

[Select image](#)

Previous

Next

In the 'Program' tab, for 'Install command', enter:
cmd.exe /c InstallSecRMMLicenseViaIntune.cmd

secRMM Intune Installation Guide

For 'Uninstall command', enter:

cmd.exe /c UninstallSecRMMLicenseViaIntune.cmd

For 'Device restart behavior', click the drop-down listbox and select:

No specific action

Now click the 'Next' button as shown in the screenshot below.

secRMM Intune Installation Guide

[Home](#) > [Apps | Windows](#) > [Windows | Windows apps](#) >

Add App ...

Windows app (Win32)

- ☒ App information **☒ 2 Program** ☐ 3 Requirements ☐ 4 Detection rules ☐ 5 Dependencies ☐ 6 Supersede

Specify the commands to install and uninstall this app:

Install command * ⓘ ✓

Uninstall command * ⓘ ✓

Install behavior ⓘ ☒ System ☐ User

Device restart behavior ⓘ ▼

Specify return codes to indicate post-installation behavior:

Return code	Code type	
<input type="text" value="0"/>	<input type="text" value="Success"/> ▼	
<input type="text" value="1707"/>	<input type="text" value="Success"/> ▼	
<input type="text" value="3010"/>	<input type="text" value="Soft reboot"/> ▼	
<input type="text" value="1641"/>	<input type="text" value="Hard reboot"/> ▼	
<input type="text" value="1618"/>	<input type="text" value="Retry"/> ▼	

[+ Add](#)

[Previous](#)

[Next](#)

secRMM Intune Installation Guide

In the 'Requirements' tab, you will need to select both the 'Operating system architecture' and the 'Minimum operating system'. If you have both secRMM running in both 32-bit and 64-bit, be sure to check both checkboxes for the 'Operating system architecture'. For the 'Configure additional requirement rules', click the '+ Add' link. Select 'Registry' for the 'Requirement type' as shown in the screenshot below.

[Home](#) > [Apps | Overview](#) > [InstallSecRMMLicenseViaIntune.cmd](#) | [Properties](#) >

Edit application

Windows app (Win32)

[App information](#) [Program](#) [Requirements](#) [Detection rules](#) [Review + save](#)

Specify the requirements that devices must meet before the app is installed:

Operating system architecture * ⓘ

64-bit

Minimum operating system * ⓘ

Windows 10 1607

Disk space required (MB) ⓘ

Physical memory required (MB) ⓘ

Minimum number of logical processors required ⓘ

Minimum CPU speed required (MHz) ⓘ

Configure additional requirement rules

Type	Path/Script
No requirements are specified.	

+ Add

Add a Requirement rule ×

Create a requirement.

Requirement type * ⓘ

Select one ▾

File

Registry

Script

The 'Registry Requirement rule' we want to create will tell Intune to only run this App for computers running secRMM. To do this, the 'Key path' value will need the 'Windows product code' for the secRMM version you are running on your endpoint Windows computers. The 'Windows product code' is different/unique for each version of secRMM.

Add a Requirement rule ×

Create a requirement.

Requirement type * ⓘ Registry ▾

Key path * ⓘ

Value name ⓘ

Registry key requirement * ⓘ Select one ▾

Associated with a 32-bit app on 64-bit clients ⓘ Yes **No**

To get the 'Windows product code' for the version of secRMM you are running on your Windows endpoint computers, you can run a secRMM script on one of the Windows endpoint computers in your environment.

For this section, you will need to install secRMM (the version you are deploying using Intune) manually (you can download the msi file from the Squadra web site) on a test machine. Once you complete this section, you can then uninstall secRMM (and let Intune do the deployment).

secRMM Intune Installation Guide

The script is in the 'C:\Program Files\secRMM\AdminUtils' directory (so you need to be logged in as an Administrator). The 2 screenshots below show running the script named GetSecRMMProductCode.cmd which returns the 'secRMM version' and the secRMM 'Windows product code' which we need to specify the 'Key path' value.

```
Administrator: cmd

C:\Program Files\secRMM\AdminUtils>GetSecRMMProductCode.cmd

Please wait, this script takes some time to finish...
secRMM 9.11.15.0 is product code {12A51B80-C39F-41B3-9065-3E1EF7E75890}

C:\Program Files\secRMM\AdminUtils>
```

The secRMM version

The secRMM product code

Programs and Features

Control Panel > Programs > Programs and Features

Control Panel Home

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
secRMM	SquadraTechnologies	11/17/2023	34.7 MB	9.11.15.0

Registry Editor

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{12A51B80-C39F-41B3-9065-3E1EF7E75890}

Name	Type	Data
DisplayName	REG_SZ	secRMM
DisplayVersion	REG_SZ	9.11.15.0
EstimatedSize	REG_DWORD	0x00008b0c (35596)

Back in the Intune portal, specify the 'Key path' value as Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} where {xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} is the 'Windows product code' that was returned from the script named GetSecRMMProductCode.cmd that you ran above. If we used the example in this document, the value of the 'Key path' would be:

secRMM Intune Installation Guide

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ {12A51B80-C39F-41B3-9065-3E1EF7E75890}

For 'Value name', specify 'DisplayVersion'.

For 'Registry key requirement', specify 'String comparison'

For 'Operator', specify 'Equals'

For 'Value', specify the version of secRMM that is running on your Windows endpoint computers. The version of secRMM is returned along with the 'Windows product code' when you run the script named GetSecRMMProductCode.cmd.

For 'Associated with a 32-bit app on 64-bit clients', specify 'No'

Once you have specified the values above, click the 'OK' button as shown in the screenshot below.

Add a Requirement rule ×

Create a requirement.

Requirement type * ⓘ Registry

Key path * ⓘ Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ {12A51B80-C39F-41B3-9065-3E1EF7E75890} ✓

Value name ⓘ DisplayVersion ✓

Registry key requirement * ⓘ String comparison

Operator * ⓘ Equals

Value * ⓘ 9.11.15.0 ✓

Associated with a 32-bit app on 64-bit clients ⓘ Yes No

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}

OK

The 'Requirements' tab will now show the 'additional requirement rule' as shown in the screenshot below.

secRMM Intune Installation Guide

[Home](#) > [Apps](#) | [Windows](#) > [Windows](#) | [Windows apps](#) >

Add App

Windows app (Win32)

✓ App information ✓ Program **3 Requirements** ④ Detection rules ⑤ Dependencies ⑥ Supersedece ⑦ Assignments

Specify the requirements that devices must meet before the app is installed:

Operating system architecture * ⓘ

Minimum operating system * ⓘ

Disk space required (MB) ⓘ

Physical memory required (MB) ⓘ

Minimum number of logical processors required ⓘ

Minimum CPU speed required (MHz) ⓘ

Configure additional requirement rules

Type	Path/Script
Registry	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\... ***

[+ Add](#)

Now click the 'Next' button as shown in the screenshot below.

secRMM Intune Installation Guide

[Home](#) > [Apps](#) | [Windows](#) > [Windows](#) | [Windows apps](#) >

Add App ...

Windows app (Win32)

✓ App information ✓ Program **3 Requirements** ④ Detection rules ⑤ Dependencies ⑥ Supersedence

Specify the requirements that devices must meet before the app is installed:

Operating system architecture * ⓘ	64-bit
Minimum operating system * ⓘ	Windows 10 1607
Disk space required (MB) ⓘ	
Physical memory required (MB) ⓘ	
Minimum number of logical processors required ⓘ	
Minimum CPU speed required (MHz) ⓘ	

Configure additional requirement rules

Type	Path/Script
Registry	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\... ***

+ Add

Previous

Next

secRMM Intune Installation Guide

In the 'Detection rules' tab, for the 'Rules format', select 'Manually configure detection rules' from the drop-down menu and then click the '+ Add' link as shown in the screenshot below.

[Home](#) > [Apps | Windows](#) > [Windows | Windows apps](#) >

Add App

Windows app (Win32)

✓ App information ✓ Program ✓ Requirements **4 Detection rules** 5 Dependencies 6 Supersedece 7 Assignments

Configure app specific rules used to detect the presence of the app.

Rules format * ⓘ

Manually configure detection rules

Type

Path/Code

No rules are specified.

[+ Add](#) ⓘ

For 'Rule type', specify 'File'.

For 'Path', specify the path where secRMM is installed.

The default secRMM installation path is 'C:\Program Files\secRMM'.

For 'File or folder', specify the name of the secRMM license file that was sent to you from Squadra Technologies. Note in the screenshot below, that we used a made up name for the secRMM license file. You must NOT use literal text NameOfsecRMMLicenseFile.lic as the 'File or folder' value.

For 'Detection method', specify 'File or folder exists'.

Detection rule ×

Create a rule that indicates the presence of the app.

Rule type * ⓘ File ▼

Path * ⓘ C:\Program Files\secRMM ✓

File or folder * ⓘ NameOfSecRMMLicenseFile.lic ✓

Detection method * ⓘ File or folder exists ▼

Associated with a 32-bit app on 64-bit clients ⓘ Yes No

Now click the 'OK' button as shown in the screenshot below.

Detection rule ×

Create a rule that indicates the presence of the app.

Rule type * ⓘ File ▼

Path * ⓘ C:\Program Files\secRMM ✓

File or folder * ⓘ NameOfSecRMMLicenseFile.lic ✓

Detection method * ⓘ File or folder exists ▼

Associated with a 32-bit app on 64-bit clients ⓘ Yes No

OK

secRMM Intune Installation Guide

The 'Detection rules' tab will now show the 'File rule' we defined above as shown in the screenshot below.

[Home](#) > [Apps | Windows](#) > [Windows | Windows apps](#) >

Add App ...

Windows app (Win32)

- ✓ App information
- ✓ Program
- ✓ Requirements
- 4 Detection rules**
- 5 Dependencies
- 6 Supersedence

Configure app specific rules used to detect the presence of the app.

Rules format * ⓘ

Manually configure detection rules

Type	Path/Code	
File	C:\Program Files\secRMM	...

+ Add ⓘ

Now click the 'Next' button as shown in the screenshot below.

[Home](#) > [Apps | Windows](#) > [Windows | Windows apps](#) >

Add App ...

Windows app (Win32)

- ✓ App information
- ✓ Program
- ✓ Requirements
- 4 Detection rules**
- 5 Dependencies
- 6 Supersedence

Configure app specific rules used to detect the presence of the app.

Rules format * ⓘ

Manually configure detection rules

Type	Path/Code	
File	C:\Program Files\secRMM	...

+ Add ⓘ

Previous

Next

secRMM Intune Installation Guide

You will not need to specify anything on the 'Dependencies' tab. Click the 'Next' button as shown in the screenshot below.

[Home](#) > [Apps](#) | [Windows](#) > [Windows](#) | [Windows apps](#) >

Add App

Windows app (Win32)

✓ App information ✓ Program ✓ Requirements ✓ Detection rules **5 Dependencies** 6 Supersede

Software dependencies are applications that must be installed before this application can be installed. To automatically install a child dependency app before installing the current parent app, enable the automatically install option. To only install the current parent app if the child dependency app is already detected on the device, disable the automatically install option. There is a maximum of 100 child dependency apps, including references to other apps outside of this view, forming a graph of apps. The total size of the dependency app graph is limited to the maximum of 100 plus the parent app (101 total). [Learn more](#)

Name	Automatically Install
No results.	

[+ Add](#) ⓘ

[Previous](#) [Next](#)

secRMM Intune Installation Guide

You will not need to specify anything on the 'Supersedence' tab. Click the 'Next' button as shown in the screenshot below.

[Home](#) > [Apps | Windows](#) > [Windows | Windows apps](#) >

Add App ...

Windows app (Win32)

✓ App information ✓ Program ✓ Requirements ✓ Detection rules ✓ Dependencies **6 Supersedence**

When you supersede an application, you can specify which apps will be directly updated or replaced. To update an app, disable the uninstall previous version option. To replace an app, enable the uninstall previous version option. There is a maximum of 10 updated or replaced apps, including references to other apps outside of this view, forming a graph of apps. The total size of the supersedence app graph is limited to the maximum of 10 plus the parent app (11 total). [Learn more](#)

Apps that this app will supersede

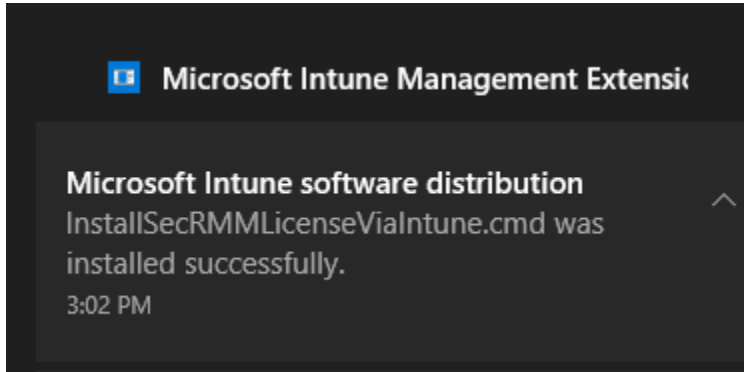
Name	Publisher	Version	Uninstall previous version
No results.			

[+ Add](#) ⓘ



The 'Assignments' tab is where you will deploy the secRMM license file. It is more logical and less of a load on resources to deploy to devices instead of users but if you do choose to use users, it will work just the same way as devices.


Now the secRMM license file(s) will be deployed to the Windows 10/11 computers being managed by Microsoft Azure Intune.



Configure a secRMM policy using Intune Powershell scripts

As explained above in the 'Setup overview' section, creating secRMM policies in Intune is done using the 'secRMM Policy Configurator' tool. The information below is for advanced scenarios where you might need a custom script to accomplish a unique scenario in your environment. This is rare and you should lean toward using the 'secRMM Policy Configurator' tool over writing your own Powershell secRMM scripts. If you are not going to require a custom script (i.e. advanced scenario), then please follow the secRMM 'Policy Configurator Admin Guide' which you can download from <https://www.squadratechnologies.com/Products/secRMM/secRMMDocumentation.aspx> as shown in the screenshot below.

secRMM Intune Installation Guide



Developed in USA

search...
☐ only search Squadra Technologies

home software hardware services partners company

Video Blog

Microsoft System Center
Microsoft Azure

secRMM Documentation

Overview

Download

Documentation

Video

Blogs

Screenshots

Features

Release Notes

Pricing

Home >> secRMM >> Documentation

secRMM Documentation

Technical Verticals Whitepapers More

secRMM Optional Features

SCCM Admin Guide (PDF)

SCOM Admin Guide (PDF)

secRMMCentral Admin Guide (PDF)

Excel Admin Admin Guide (PDF)

Azure Intune Admin Guide (MDM) (PDF)

Azure Monitor Admin Guide (PDF)


Azure Sentinel Admin Guide (SIEM) (PDF)

Azure Defender for Cloud Admin Guide (PDF)

Azure Verifiable Credentials Admin Guide (PDF)

Policy Configurator Admin Guide (Intune, SCCM, AD GPO, Endpoints) (PDF)


SDK Programmers Guide (PDF)

 **Get In Touch**

Would you like to find out more or begin working with Squadra? We look forward to hearing from you. Please contact us today to get started!

Contact Us

" We searched around for a solution like secRMM and couldn't quite find the right fit. secRMM is exactly what we were looking for. "

 Windows Systems Administrator.

Page 43

secRMM Intune Installation Guide

The secRMM 'policy configurator' tool can be downloaded from the Squadra technologies website as shown in the screenshot below.

https://www.squadratechnologies.com/Products/secRMM/secRMMDownloads3.aspx

squadra technologies
Developed in USA

home software hardware services partners company

search... Search
only search Squadra Technologies

Microsoft System Center
Microsoft Azure

secRMM Optional Downloads

Home >> secRMM >> Downloads > Optional Downloads

Download

Documentation

Video

Blogs

Screenshots

Features

Release Notes

Pricing

Item	Download link
Microsoft System Center/Azure	secRMM System Center/Azure
secRMM Policy Configurator	secRMMPolicyConfigurator.zip (9_11_18_0)
secRMM Excel Addin	secRMMExcelAddin
secRMM Charts	secRMMCharts.zip (9_11_18_0)
secRMM Central	secRMMCentral
secRMM Reports	secRMMReports
secRMM Deployment tools	secRMMDeployment.zip
secRMM SNMP MIB file	secRMMSNMP-MIB.txt right click and then "Save As" to download
secRMM Smart Phone Apps	secRMM Smart Phone Apps
Hardware Vendor Firmware version(s)	Apricom secRMM Firmware version
NIST SP 800-171 compliance tool	secRMM_NIST_SP_800-171.zip

Get In Touch

Would you like to find out more or begin working with Squadra? We look forward to hearing from you. Please contact us today to get started!

Contact Us

"We searched around for a solution like secRMM and couldn't quite find the right fit. secRMM is exactly what we were looking for."

Windows Systems Administrator

secRMM Policy Configurator

File View Help

secRMM Policy Configurator

SETTINGS

SCCM

INTUNE

Active Directory
AD GPO

ENDPOINT

Intune

SETTINGS

+

Name ↑	Type	Description	Created DateTime	Last Modified DateTime	File Name
secRMMComputerPolicy1.ps1	Computer	The is a secRMM computer policy (no USB)	2022-09-13T19:07:25.2669392Z	2022-09-13T19:07:25.2669392Z	secRMMComputerPolicy1.ps1
secRMMUserPolicy1.ps1	User	This policy is for sales and marketing	2021-11-19T16:29:36.8739715Z	2021-11-19T16:29:36.8739715Z	secRMMUserPolicy1.ps1

Rows per page: 5 1-2 of 2

Dense padding

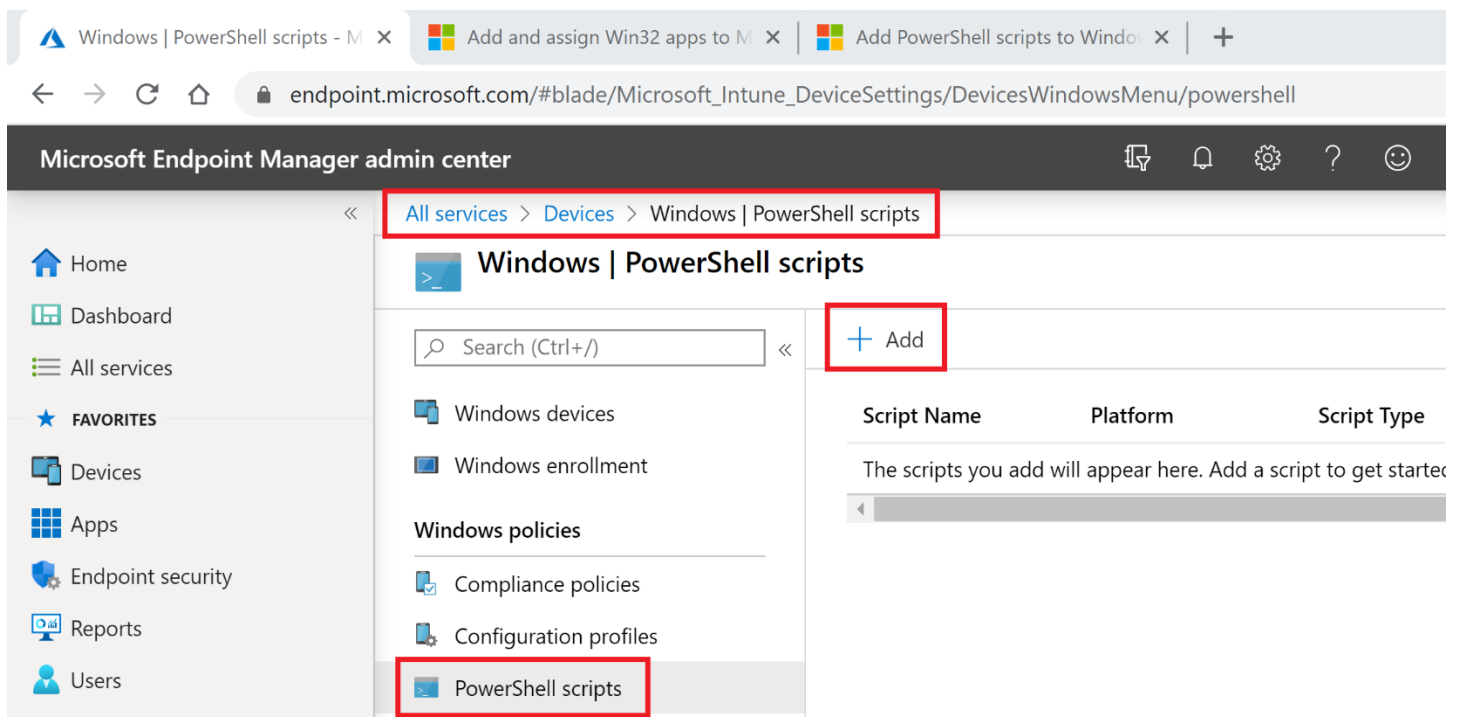
secRMM Intune Installation Guide

This section shows you the low level steps of creating a Powershell script that controls secRMM and then deploying it using Intune. Again, we recommend that instead of following the process below you instead use the "secRMM Policy Configurator" tool which performs the process below for you and removes you from having to work with the Powershell script code.

The Microsoft documentation titled "Use PowerShell scripts on Windows 10 devices in Intune" at:

<https://docs.microsoft.com/en-us/mem/intune/apps/intune-management-extension>

describes the screenshots that are listed below.



The following (example) PowerShell script will be used for this documentation. You will need to modify the PowerShell script for your environment. If you need assistance modifying the PowerShell script, please contact Squadra Technologies support at support@squadratechnologies.com. The script below is saved into the file named secRMMComputerPolicy.ps1.

```
$AllowedUsers = "contoso\Barbara;contoso\Angela";  
$SecRMM_Properties = @{  
    "AllowedUsers" = $AllowedUsers  
};  
$objSecRMM = new-object -comobject secRMMInterface;  
$SecRMM_Properties.GetEnumerator() |  
ForEach-Object {
```

secRMM Intune Installation Guide

```
$objSecRMM.SetProperty($_.key, $_.value);  
Write-Host ("Set " + $_.key + " to " + $_.value);  
}
```

[All services](#) > [Devices](#) > [Windows | PowerShell scripts](#) > Add Powershell script

Add Powershell script

✓ Basics **2 Script settings** 3 Assignments 4 Review + add

Script location * ⓘ

secRMMComputerPolicy.ps1

Run this script using the logged on
credentials ⓘ

Yes

No

Enforce script signature check ⓘ

Yes

No

Run script in 64 bit PowerShell Host ⓘ

Yes

No

[All services](#) > [Devices](#) > [Windows | PowerShell scripts](#) > Add Powershell script

Add Powershell script

✓ Basics ✓ Script settings **3 Assignments** 4 Review + add

Included groups

Assign to

All devices



Excluded groups

Selected groups

No groups selected

+ [Select groups to exclude](#)

secRMM Intune Installation Guide

[All services](#) > [Devices](#) > [Windows | PowerShell scripts](#) > Add Powershell script

Add Powershell script

✓ Basics ✓ Script settings ✓ Assignments **4 Review + add**

Summary

Basics

Name	secRMM Computer Policy
Description	secRMM computer policy which sets AllowedUsers and SendToAzureLog properties.

Script settings

PowerShell script	secRMMComputerPolicy.ps1
Run this script using the logged on credentials	No
Enforce script signature check	No
Run script in 64 bit PowerShell Host	Yes

Assignments

Previous

Add

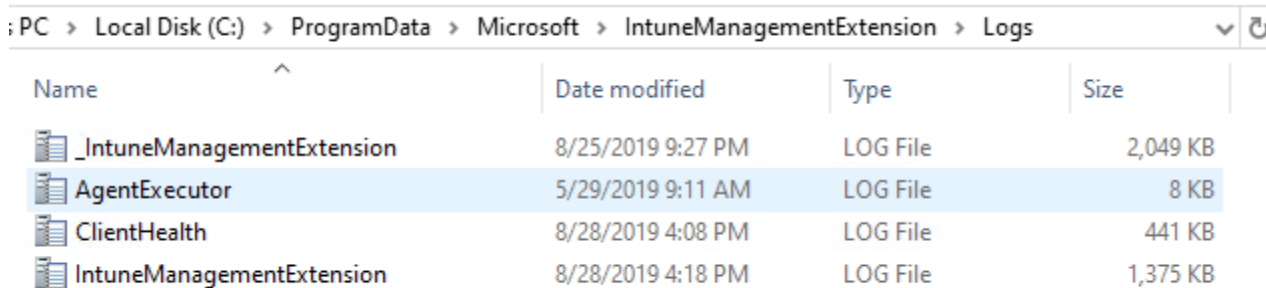
The PowerShell script will now be deployed to the Windows 10 computers being managed by your Intune instance. Again, this PowerShell script will set the secRMM properties for the secRMM computer policy on each of the Windows 10 computers in your environment.

User deployment requirements

If you plan on using a secRMM user policy (i.e. not a secRMM computer policy) then you need to configure the Windows endpoint computers so that they will be generating "successful logon events" (event id 4624) into the Windows security event log.

Troubleshooting

There is an Intune client log file directory on the endpoint computer(s) at
C:\ProgramData\Microsoft\IntuneManagementExtension\Logs.
You should first look at IntuneManagementExtension.log



; PC > Local Disk (C:) > ProgramData > Microsoft > IntuneManagementExtension > Logs			
Name	Date modified	Type	Size
IntuneManagementExtension	8/25/2019 9:27 PM	LOG File	2,049 KB
AgentExecutor	5/29/2019 9:11 AM	LOG File	8 KB
ClientHealth	8/28/2019 4:08 PM	LOG File	441 KB
IntuneManagementExtension	8/28/2019 4:18 PM	LOG File	1,375 KB

If you want to extract an Intunewin file, there is a free utility at:
https://github.com/damienvanrobaeys/Intunewin_RightClick_Extract.
Extracting an Intunewin file helps understand what files will be sent down to the endpoint (i.e. the Intune client).

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

secRMM Intune Installation Guide

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

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