Security Removable Media Manager
(secRMM)

Intune Guide

Version 9.9.25.0

(April 2020)

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 **4**

SETUP DETAILS **4**

Deploy secRMM using an Intunewin file *4*

Configure a secRMM computer policy using Intune Powershell scripts *8*

CONTACTING SQUADRA TECHNOLOGIES SUPPORT **12**

ABOUT SQUADRA TECHNOLOGIES, LLC. **13**

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.

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 deploy and configure secRMM using Microsoft Azure Intune.

1. Deploy secRMM using an Intunewin file
2. Configure a secRMM computer policy using Intune Powershell scripts

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.

secRMM Downloads

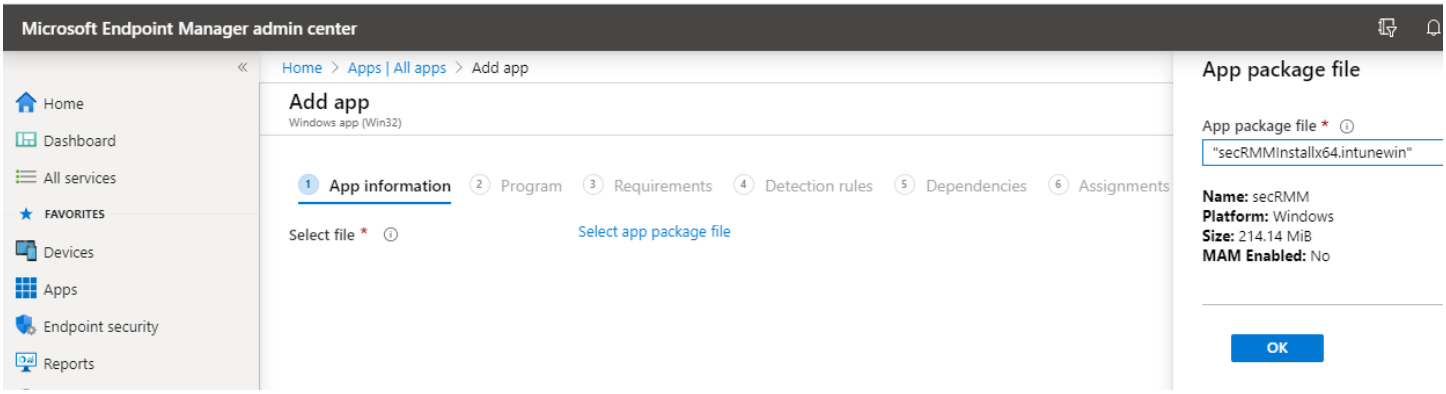
- Overview
- Download
- Documentation
- Video
- Screenshots
- Features
- Release Notes

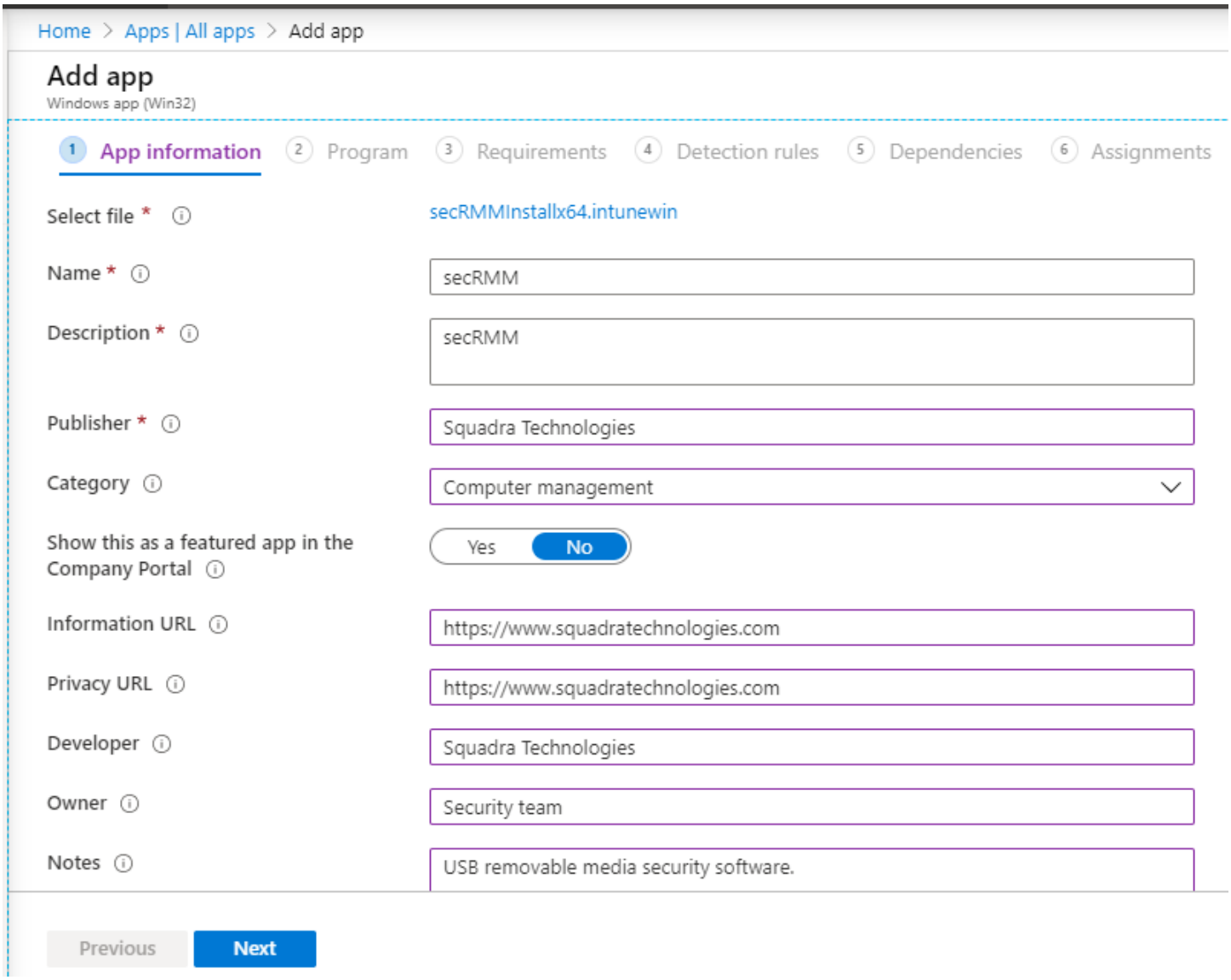
Home >> secRMM >> Downloads

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

Item	Download link
Prerequiste: 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

Now upload the secRMMInstallx64.intunewin file into Intune.


Microsoft Endpoint Manager admin center
Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Home > Apps | All apps > Add app
Add app
Windows app (Win32)
1 App information
2 Program
3 Requirements
4 Detection rules
5 Dependencies
6 Assignments
Select file *
Select app package file
App package file
App package file *
"secRMMInstallx64.intunewin"
Name: secRMM
Platform: Windows
Size: 214.14 MiB
MAM Enabled: No
OK


Home > Apps | All apps > Add app
Add app
Windows app (Win32)
1 App information
2 Program
3 Requirements
4 Detection rules
5 Dependencies
6 Assignments
Select file *
secRMMInstallx64.intunewin
Name *
secRMM
Description *
secRMM
Publisher *
Squadra Technologies
Category
Computer management
Show this as a featured app in the Company Portal
Yes
No
Information URL
https://www.squadratechnologies.com
Privacy URL
https://www.squadratechnologies.com
Developer
Squadra Technologies
Owner
Security team
Notes
USB removable media security software.
Previous
Next

Add app

Windows app (Win32)

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

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) : 4

Physical memory required (MB) :

Minimum number of logical processors required :

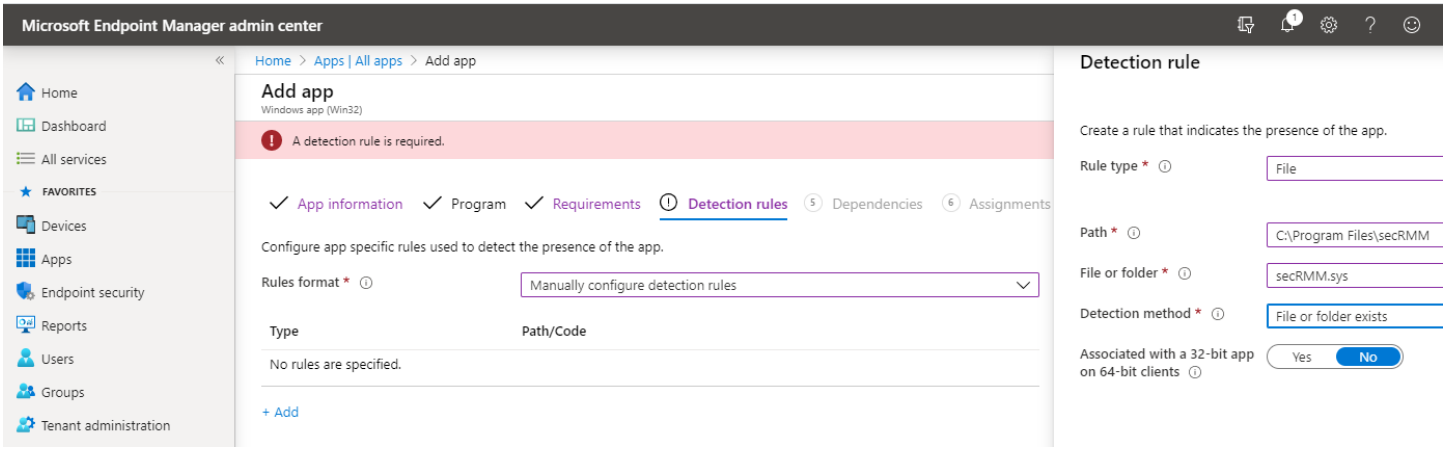
Minimum CPU speed required (MHz) :

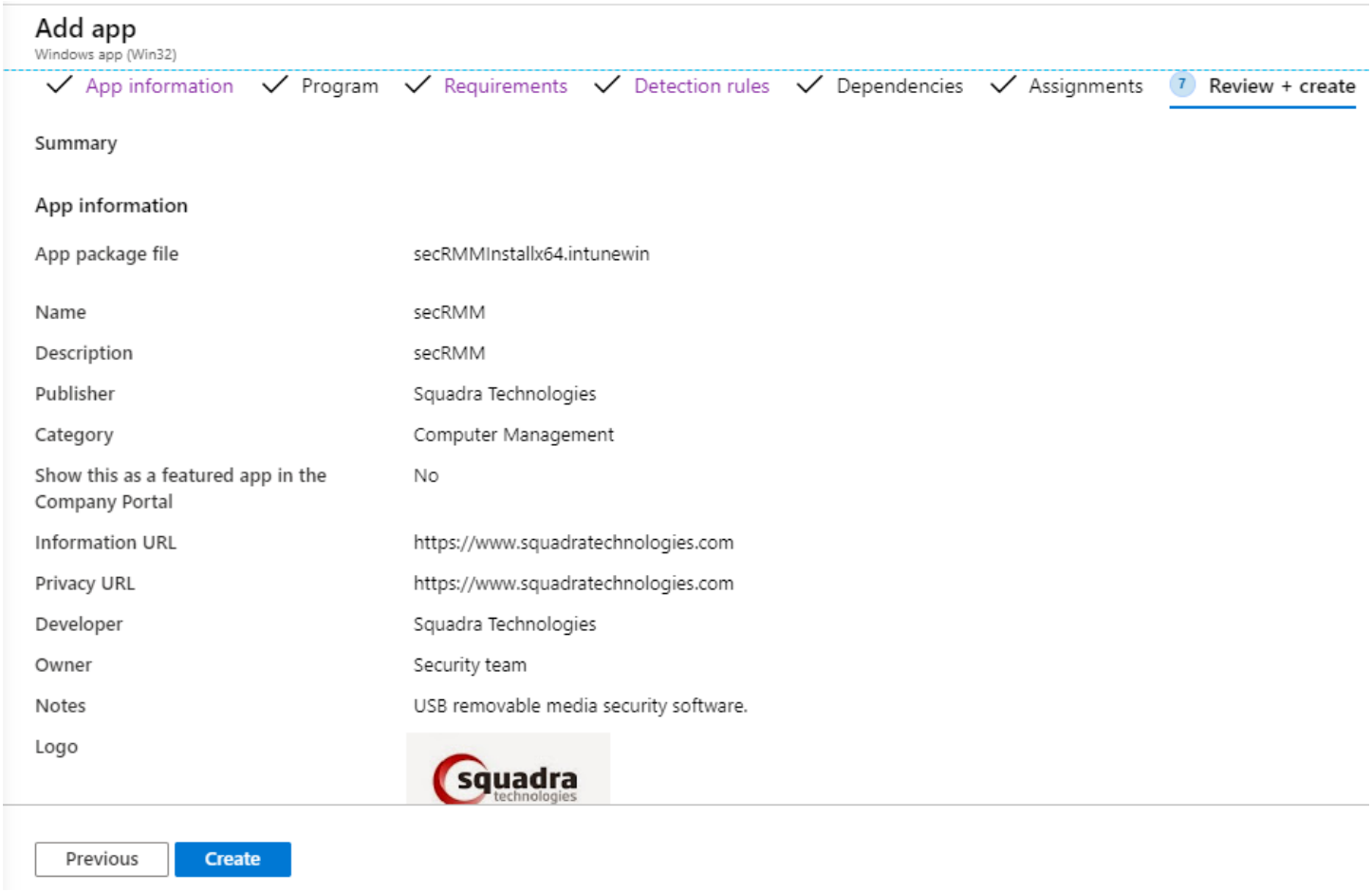
Configure additional requirement rules

Type	Path/Script
No requirements are specified.	

+ Add

Previous **Next**





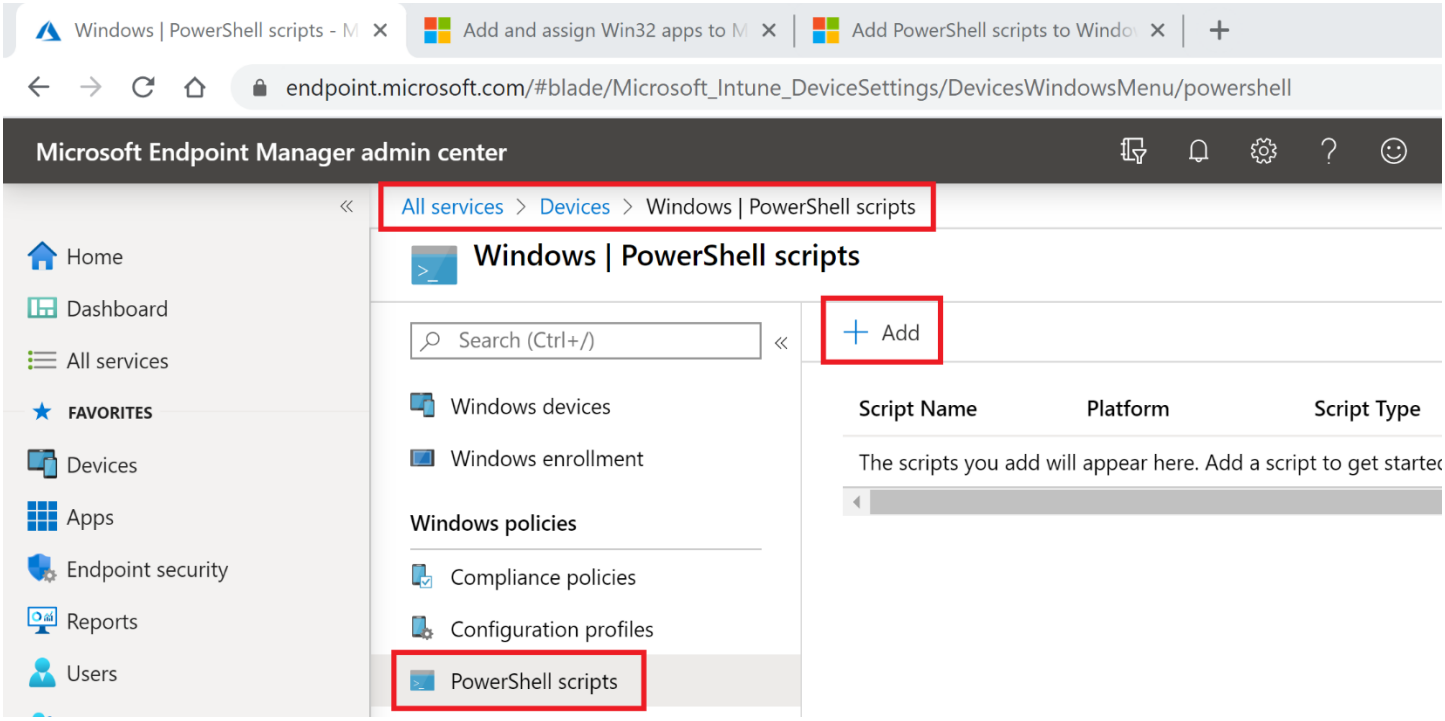
Now secRMM will be deployed to the Windows 10 computers being managed by Microsoft Azure Intune.

Configure a secRMM computer policy using Intune Powershell scripts

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

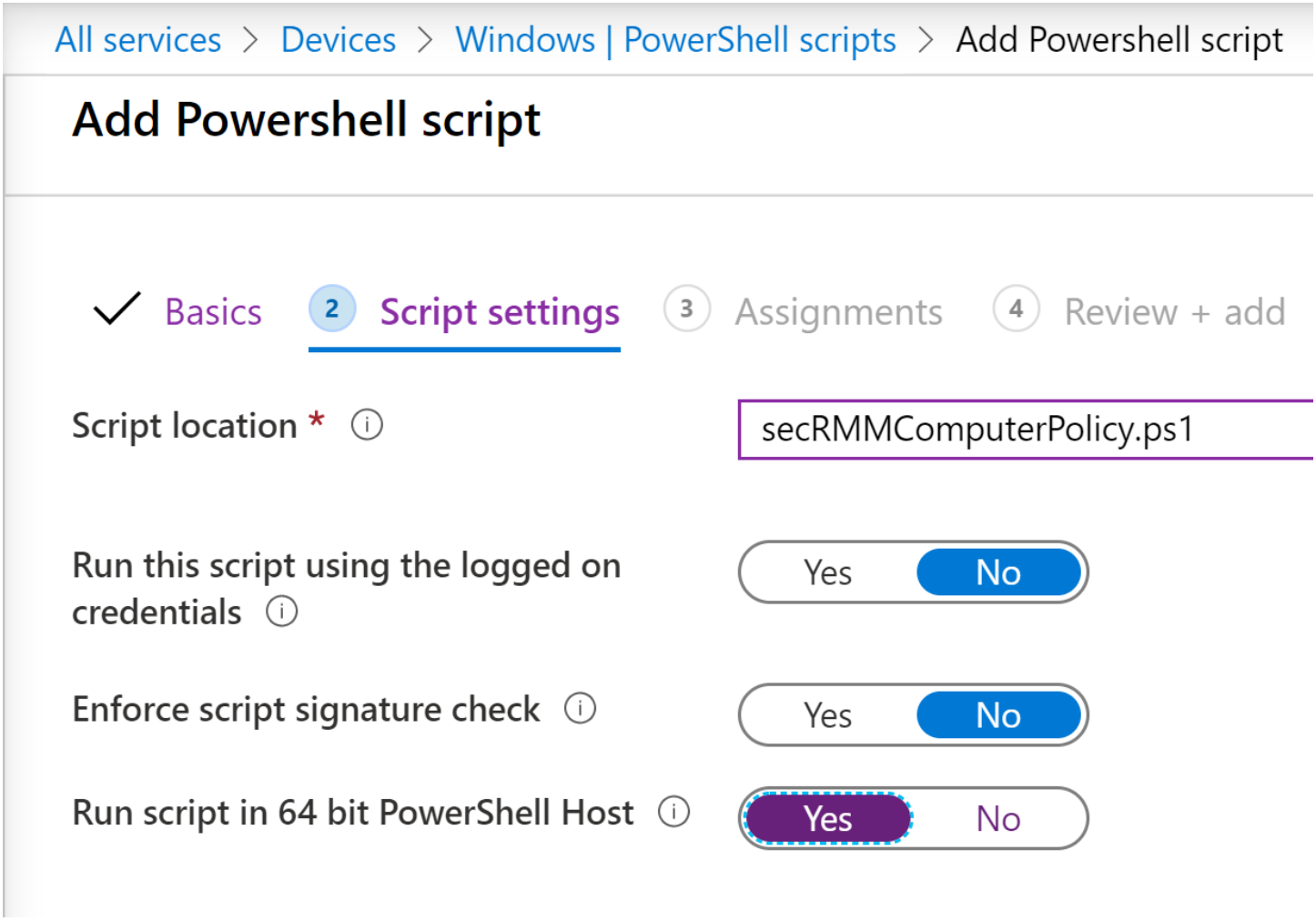
https://docs.microsoft.com/en-us/mem/intune/apps/intune-management-extension

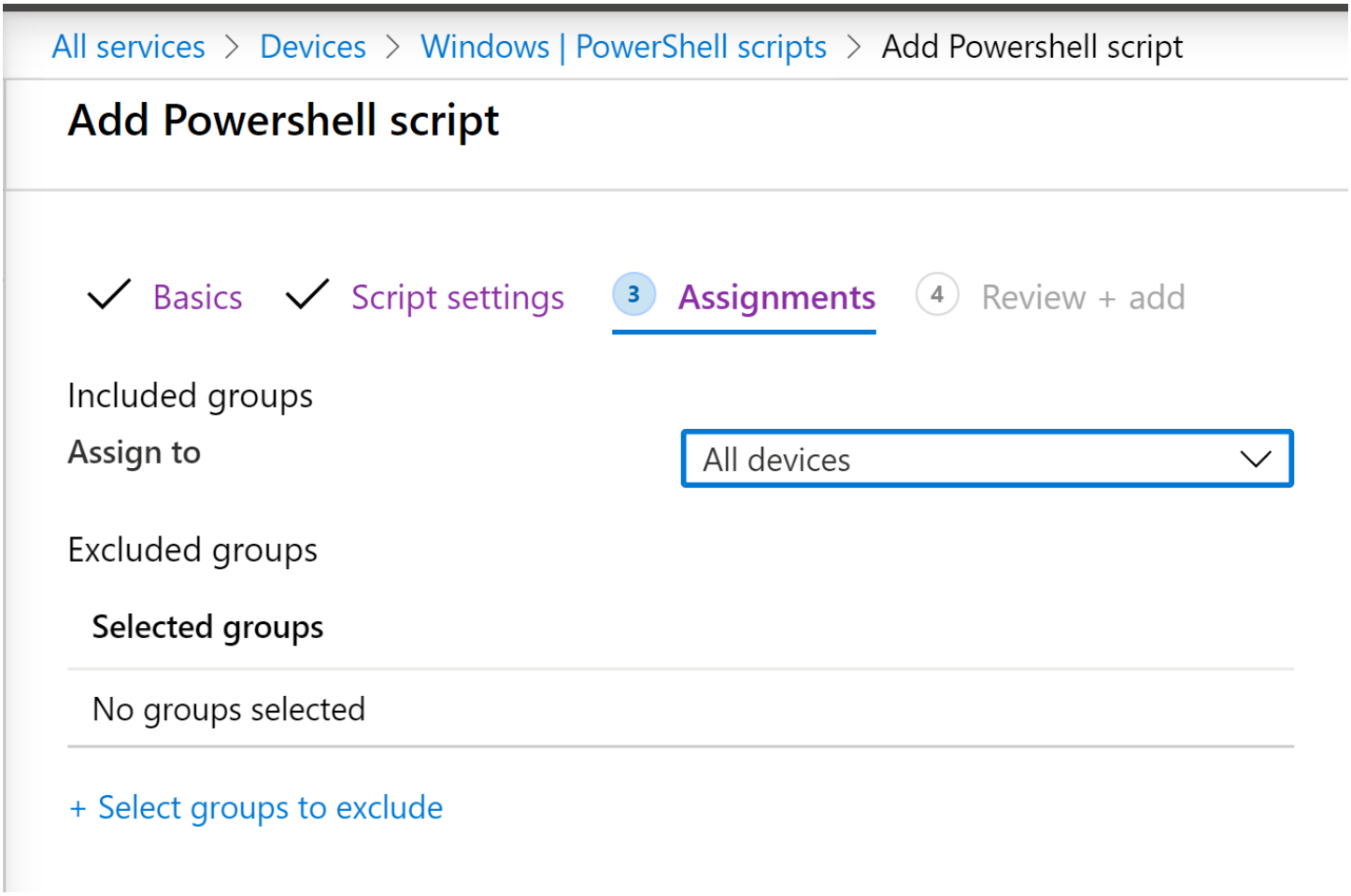
describes the screenshots that are listed below.

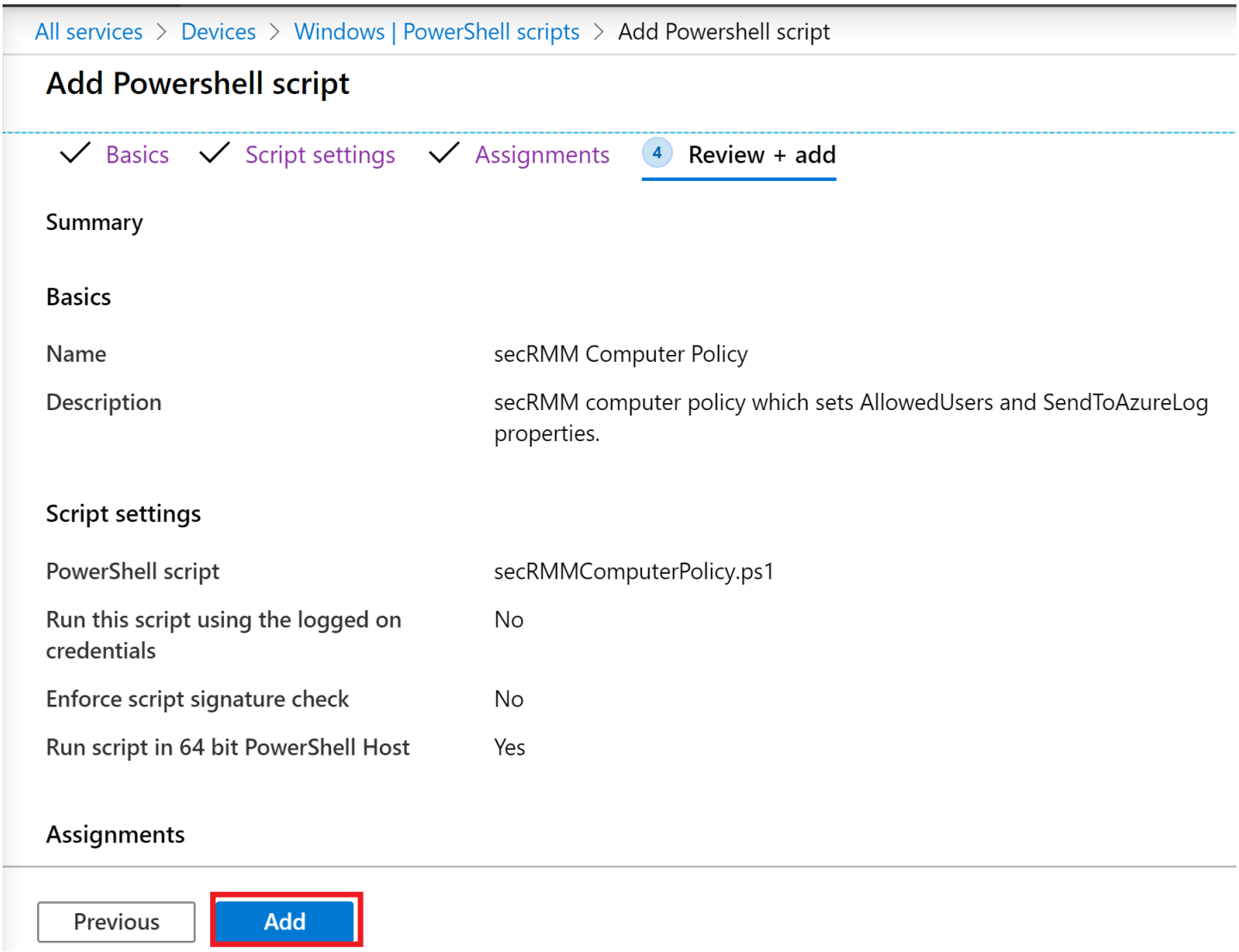


The following (example) PowerShell script will be used for this documentation. You will need to modify the PowerShell script for your environment. If you need assistance modifying the PowerShell script, please contact Squadra Technologies support at support@squadratechnologies.com. The script below is 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 {
    $objSecRMM.SetProperty($_.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



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.

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/