

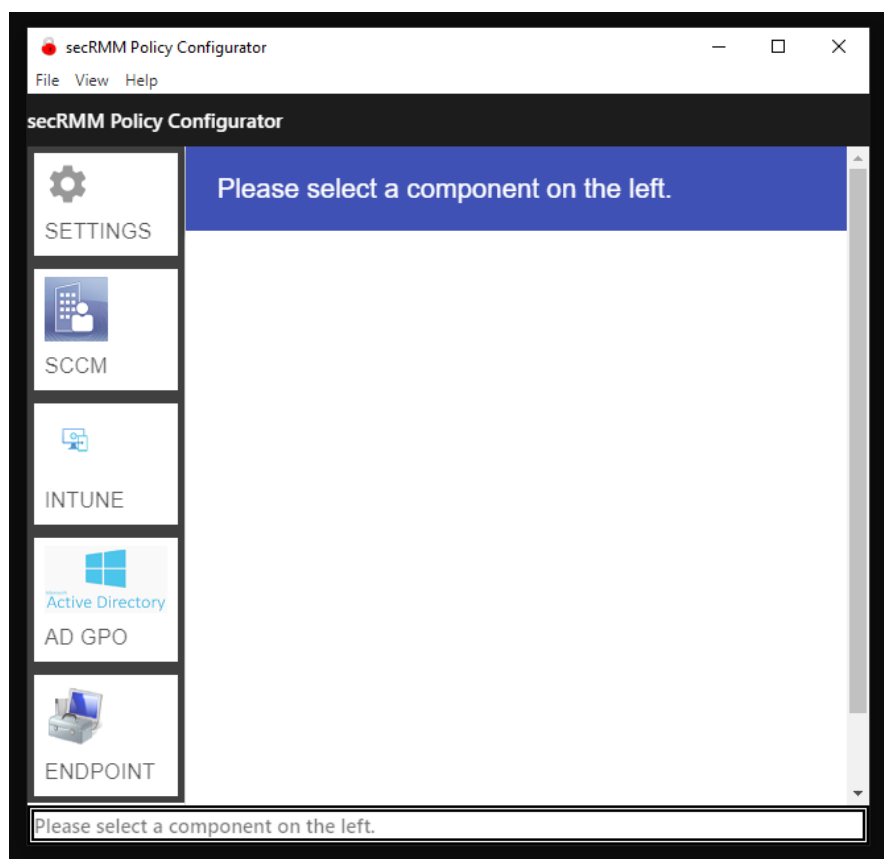


Security Removable Media Manager **Policy Configurator** **Administrator Guide**

Version 9.11.27.0

(April 2024)

Protect your valuable data



secRMM Policy Configurator Administrator 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 Excel AddIn Administrator Guide
Created - August 2011

Table of Contents

INTRODUCTION	4
INSTALLATION	4
TECHNOLOGIES	4
SCCM	4
INTUNE	5
ACTIVE DIRECTORY GROUP POLICY OBJECTS	28
ENDPOINT	29
<i>Configuring the Endpoint Computers.....</i>	<i>29</i>
Enabling WinRM.....	29
Disabling WinRM.....	31
<i>Configuring the “secRMM Policy Configurator” Computer</i>	<i>33</i>
<i>Specifying the WinRM credentials</i>	<i>33</i>
<i>Microsoft documentation for WinRM</i>	<i>34</i>
TECHNICAL DETAILS	34
CONTACTING SQUADRA TECHNOLOGIES SUPPORT	35
ABOUT SQUADRA TECHNOLOGIES, LLC.....	35

secRMM Policy Configurator Administrator Guide

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. Generally, any storage device that supports Microsoft plug-and-play will be managed and monitored by secRMM. 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.

The "secRMM Policy Configurator" is a Windows program that lets you configure the secRMM security policies for your environment using the tools available within your environment. Currently the "secRMM Policy Configurator" supports the following Microsoft technologies:

1. SCCM (on-premise)
2. Active Directory (on-premise)
3. Endpoint (on-premise or standalone)
4. Intune/Endpoint Manager (cloud)

You can use as many of the Microsoft technologies listed above. Modifying the secRMM security policies is the same user interface regardless of which Microsoft technology you are using.

The remaining sections of this document will give the details of how to connect to each Microsoft technology from within the "secRMM Policy Configurator".

Installation

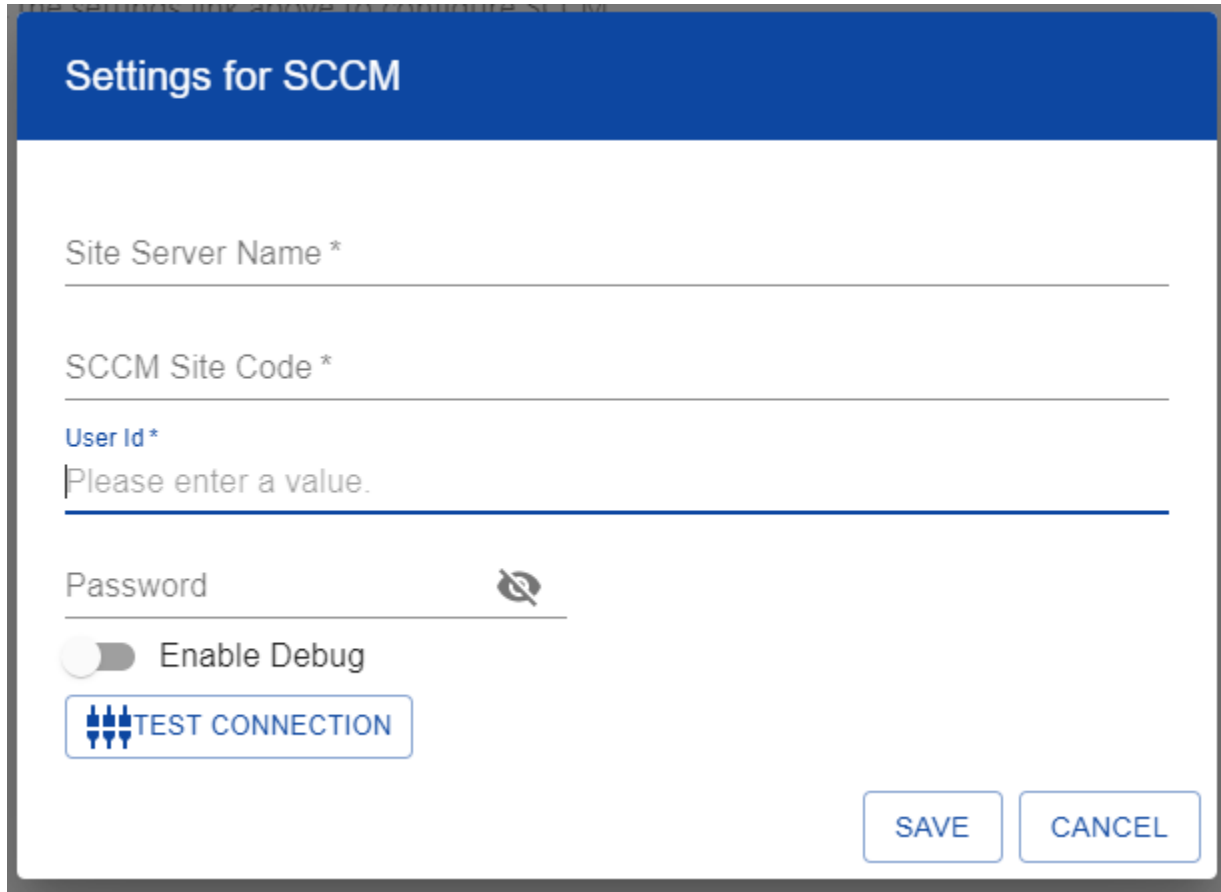
The "secRMM Policy Configurator" installation is a standard Windows msi file which you download from the Squadra Technologies web site. The only prerequisite to run the "secRMM Policy Configurator" tool is that you must have secRMM installed on the same machine. Also, please make sure you have the latest version of secRMM installed (the minimum supported version is 9.11.0.0).

Technologies

SCCM

For the "secRMM Policy Configurator" to connect to SCCM, you only need to supply:

1. Your SCCM Site Server Name (the NetBios name is sufficient).
2. The 3 character SCCM Site Code.
3. A userid/password that is defined within the SCCM console with enough privileges (role based access) to create, read, modify and delete "SCCM Compliance Configuration Items".




Settings for SCCM

Site Server Name *


SCCM Site Code *

User Id *

Please enter a value.

Password 

☐ Enable Debug

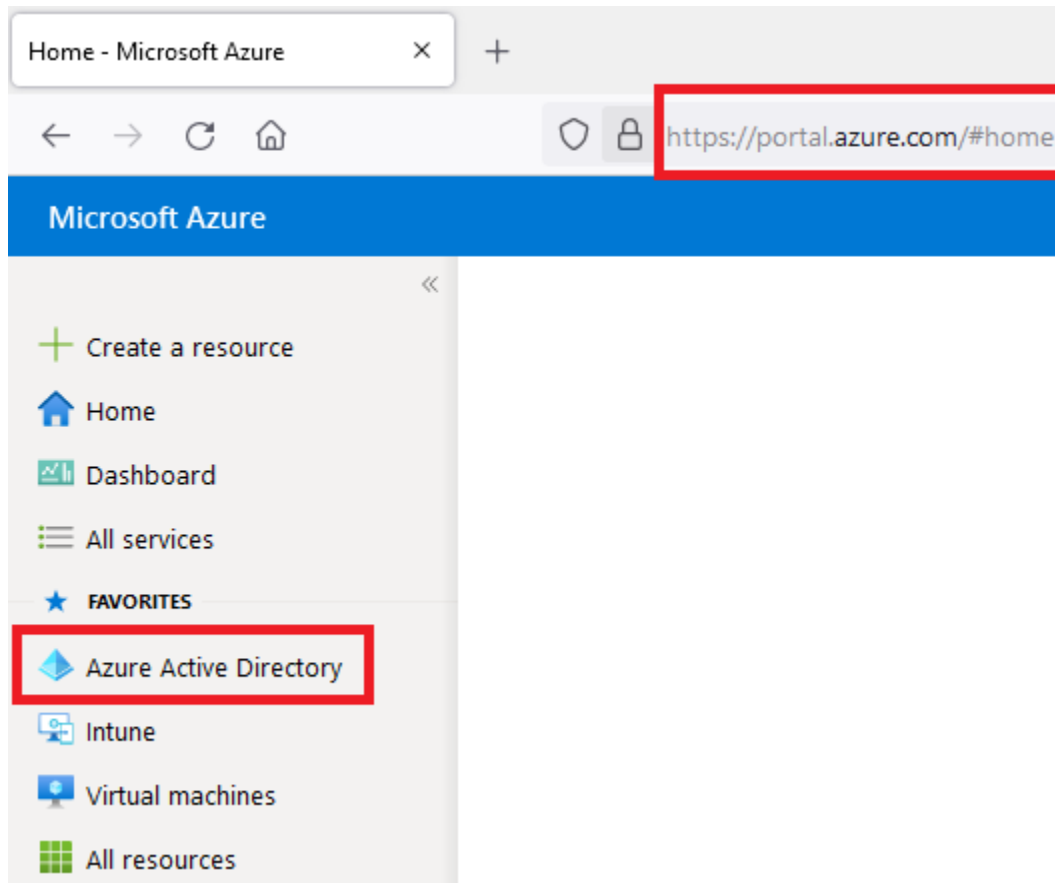
 TEST CONNECTION

SAVE CANCEL

Intune

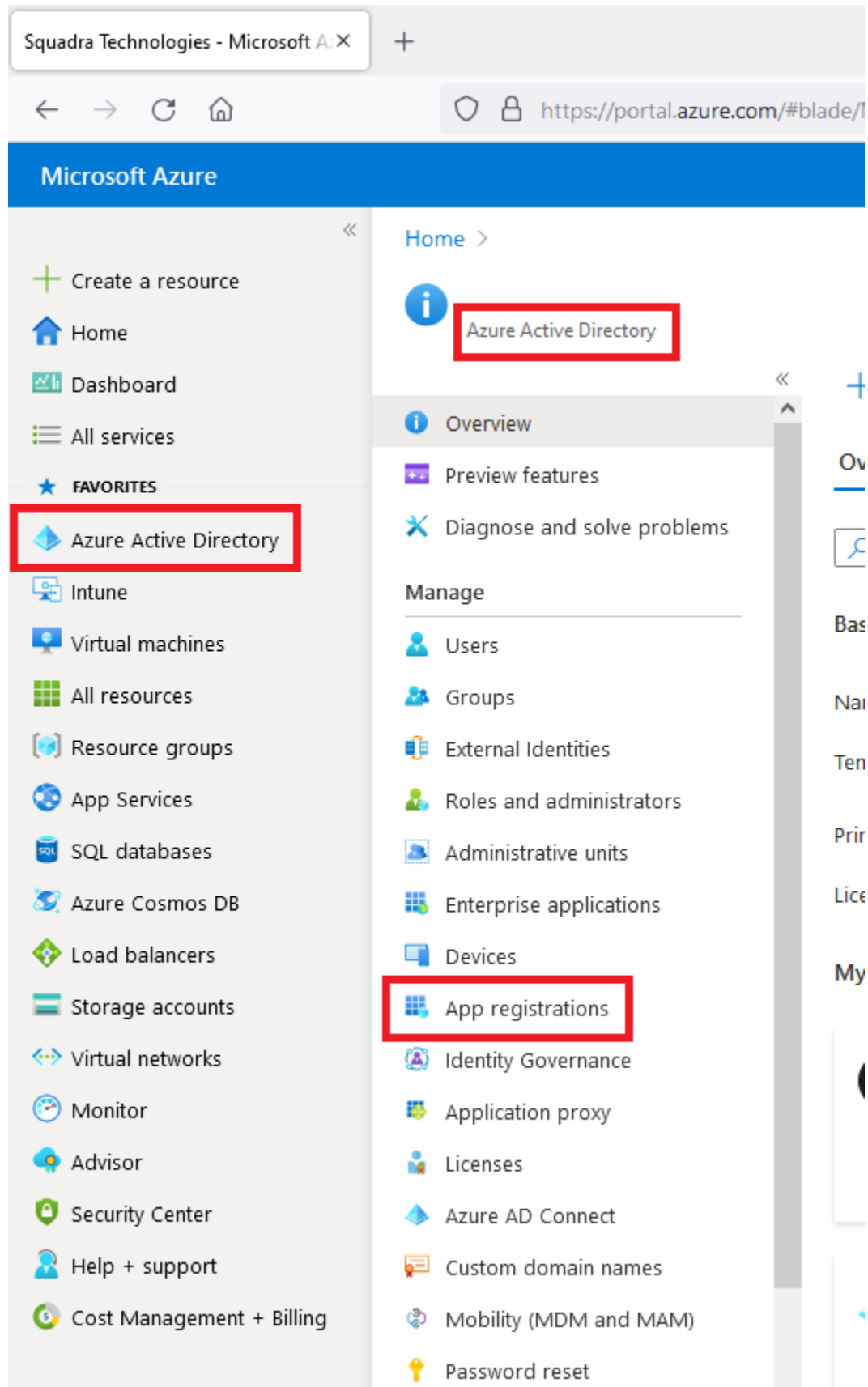
For the “secRMM Policy Configurator” to connect to “Azure Intune”/“Endpoint Manager”, you need to create an application in Azure Active Directory. Please follow the steps below to create the application in Azure Active Directory.

1. From within the Azure portal home page, select “Azure Active Directory” as shown in the screenshot below.



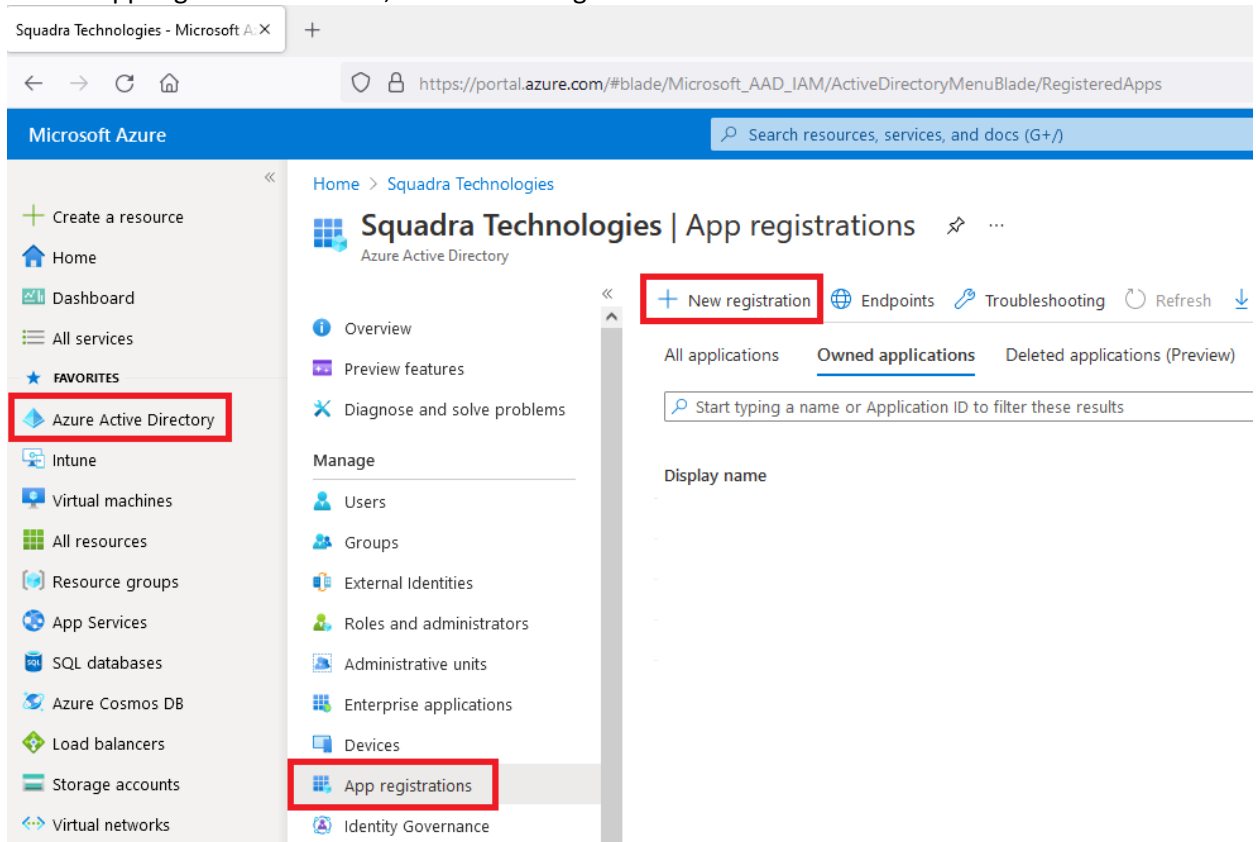
2. From within the “Azure Active Directory” blade, select “App registrations” as shown in the screenshot below.

secRMM Policy Configurator Administrator Guide



secRMM Policy Configurator Administrator Guide

3. In the “App registrations” blade, select “New registration” as shown in the screenshot below.



4. On the “Register an application” blade, fill out the form as shown in the screenshot below.

secRMM Policy Configurator Administrator Guide

Register an application - Microsoft

https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps

Microsoft Azure

Search resources, services, and docs (G+)

Home > Squadra Technologies >

Register an application

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

secRMM Policy Configurator

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

☒ Accounts in this organizational directory only (Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

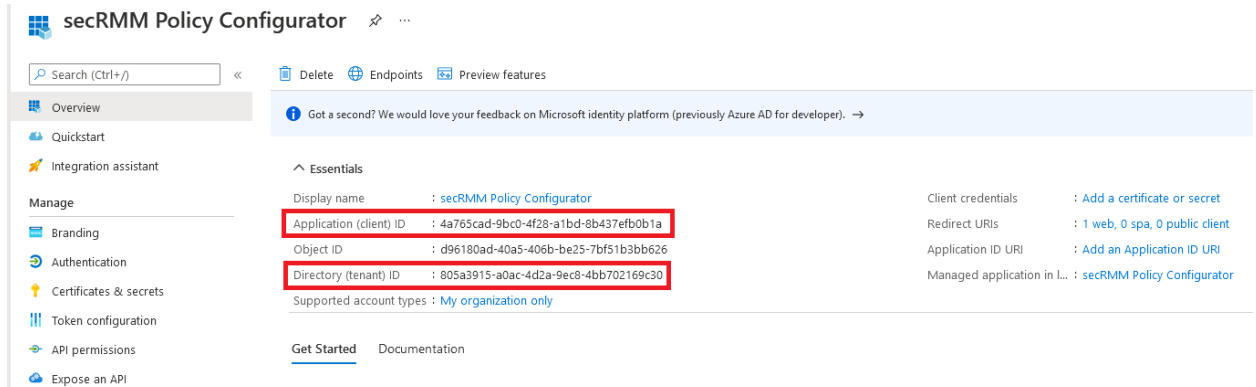
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise](#)

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

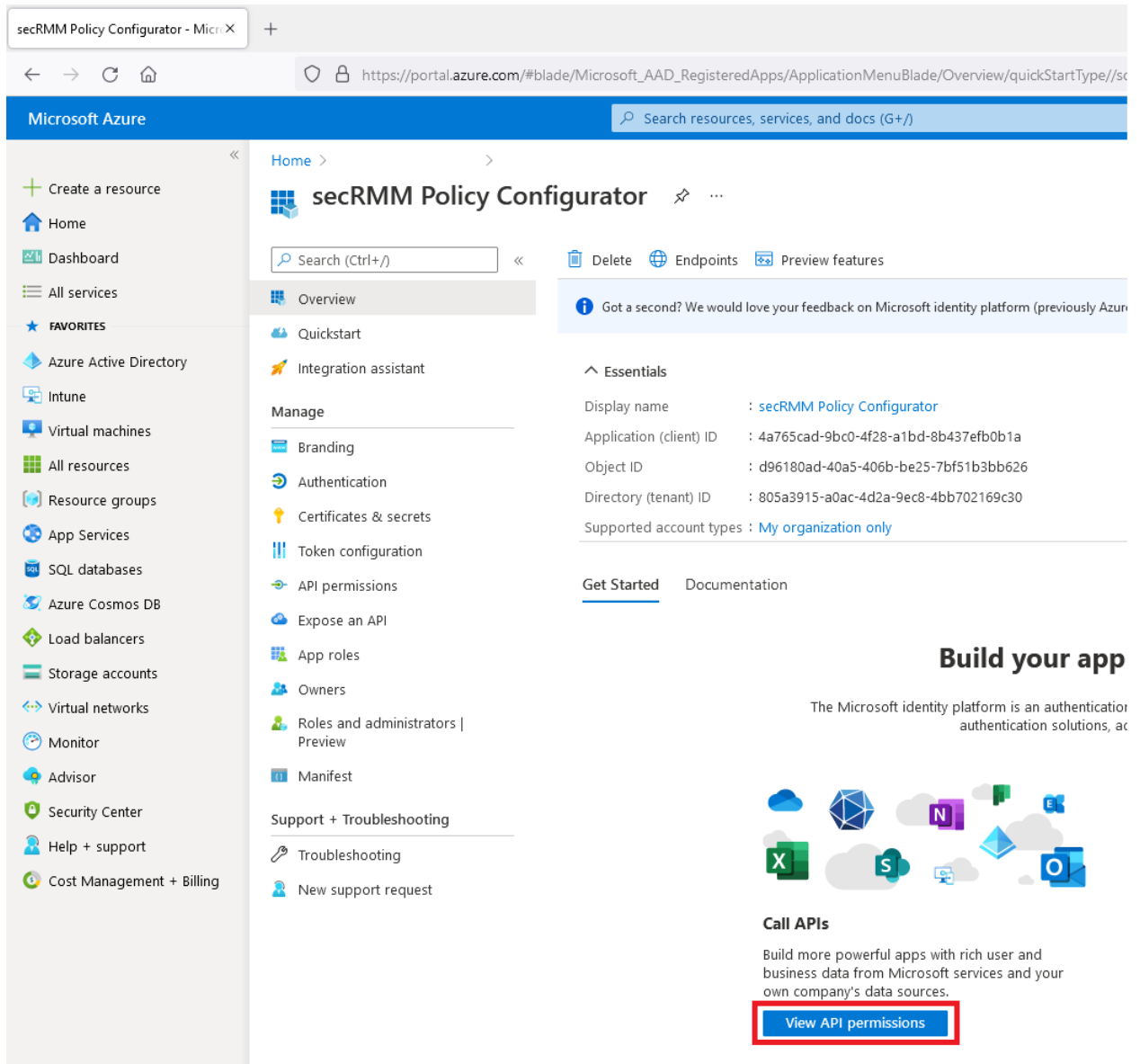
Register

5. The application will be created and within the Azure portal, you will be shown the “Essential” properties of the application as shown in the screenshot below. You will need 2 of the properties when you configure the “secRMM Policy Configurator” in a step below. The 2 properties are:
 - a. Directory (tenant) ID
 - b. Application (client) ID

secRMM Policy Configurator Administrator Guide



6. Now you need to give permissions to this application so the “secRMM Policy Configurator” can connect to Intune/”Endpoint Manager”. To do this, click the “View API permissions” as shown in the screenshot below.



secRMM Policy Configurator Administrator Guide

- On the “API permissions” blade, click the “Add a permission” button as shown in the screenshot below.

The screenshot shows the 'secRMM Policy Configurator | API permissions' page. The left sidebar contains a navigation menu with the following items: Overview, Quickstart, Integration assistant, Manage (with sub-items: Branding, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators | Preview, and Manifest), and API permissions (which is currently selected). The main content area is titled 'Configured permissions' and includes a search bar, a refresh button, and a 'Got feedback?' link. Below this, there is a table of configured permissions. The table has three columns: 'API / Permissions name', 'Type', and 'Description'. The table shows one permission: 'User.Read' under the 'Microsoft Graph (1)' group, with a 'Delegated' type and a description of 'Sign in and read user's basic information'. A red box highlights the '+ Add a permission' button located above the table. To the right of the button, there is a checkmark and the text 'Grant admin consent for Squadra Tec'.

Home > > secRMM Policy Configurator

secRMM Policy Configurator | API permissions

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

Overview

Quickstart

Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

Configured permissions

Applications are authorized to call APIs when they are granted permissions. [Learn more about permissions](#)

+ Add a permission ✓ Grant admin consent for Squadra Tec

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

To view and manage permissions and user consent, try [Enterprise](#)

- Click the “Microsoft Graph” button as shown in the screenshot below.

Request API permissions

Select an API

Microsoft APIs

APIs my organization uses

My APIs

Commonly used Microsoft APIs



Microsoft Graph

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



Azure DevOps

Integrate with Azure DevOps and Azure DevOps server



Azure Rights Management Services

Allow validated users to read and write protected content




Azure Service Management

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

9. We need to add 8 “API/Permissions” as shown in the screenshots below. Each time you click the “Add permissions” (as shown in the screenshots below), the browser will go back to the previous page. On that previous page, click the “Add a permission” button and the “Graph API” button again (as shown in the 2 screenshots above) until you have added all 8 “API/Permissions”.

Request API permissions

[← All APIs](#)

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

What type of permissions does your application require?

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

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

Select permissions [expand all](#)

2.


Permission	Admin consent required
✓ DeviceManagementApps (1)	
<input type="checkbox"/> DeviceManagementApps.Read.All ⓘ Read Microsoft Intune apps	Yes
<input checked="" type="checkbox"/> 3. DeviceManagementApps.ReadWrite.All ⓘ Read and write Microsoft Intune apps	Yes

4.

secRMM Policy Configurator Administrator Guide

Request API permissions

[← All APIs](#)

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

What type of permissions does your application require?

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

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

Select permissions [expand all](#)

devicemanagementconfiguration

PermissionAdmin consent required

DeviceManagementConfiguration (1)

☐ DeviceManagementConfiguration.Read.All ⓘ
Read Microsoft Intune device configuration and policiesYes

☒ DeviceManagementConfiguration.ReadWrite.All ⓘ
Read and write Microsoft Intune device configuration and policiesYes

Add permissions

Discard

Request API permissions



[← All APIs](#)



Microsoft Graph

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

What type of permissions does your application require?

Delegated permissions

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

1.

Application permissions

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

Select permissions

[expand all](#)

2.



Permission

Admin consent required

✓ DeviceManagementManagedDevices (1)



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

Yes



DeviceManagementManagedDevices.Read.All ⓘ
Read Microsoft Intune devices

Yes



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

Yes

4.

Add permissions

Discard

Request API permissions



[← All APIs](#)



Microsoft Graph

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

What type of permissions does your application require?

Delegated permissions

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

1.

Application permissions

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

Select permissions

[expand all](#)

2. ×

Permission

Admin consent required

▼ DeviceManagementManagedDevices (2)

<input checked="" type="checkbox"/>	DeviceManagementManagedDevices.PrivilegedOperations.All ⓘ Perform user-impacting remote actions on Microsoft Intune devices	Yes
<input type="checkbox"/>	DeviceManagementManagedDevices.Read.All ⓘ Read Microsoft Intune devices	Yes
<input checked="" type="checkbox"/> 3.	DeviceManagementManagedDevices.ReadWrite.All ⓘ Read and write Microsoft Intune devices	Yes

4.

Add permissions

Discard

secRMM Policy Configurator Administrator Guide

Request API permissions



[← All APIs](#)



Microsoft Graph

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

What type of permissions does your application require?

Delegated permissions

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

1.

Application permissions

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

Select permissions

[expand all](#)

2.



Permission

Admin consent required

✓ DeviceManagementRBAC (1)



DeviceManagementRBAC.Read.All ⓘ
Read Microsoft Intune RBAC settings

Yes



3.

DeviceManagementRBAC.ReadWrite.All ⓘ
Read and write Microsoft Intune RBAC settings

Yes

4.

Add permissions

Discard

Request API permissions



[← All APIs](#)



Microsoft Graph

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

What type of permissions does your application require?

Delegated permissions

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

1.

Application permissions

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

Select permissions

[expand all](#)



devicemanagementserviceconfig

2.



Permission

Admin consent required



DeviceManagementServiceConfig (1)



DeviceManagementServiceConfig.Read.All ⓘ
Read Microsoft Intune configuration

Yes



3.

DeviceManagementServiceConfig.ReadWrite.All ⓘ
Read and write Microsoft Intune configuration

Yes

4.

Add permissions

Discard

Request API permissions



[← All APIs](#)



Microsoft Graph

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

What type of permissions does your application require?

Delegated permissions

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

1.

Application permissions

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

Select permissions

[expand all](#)

2.

Permission

Admin consent required

▼ Directory (1)



3. Directory.Read.All ⓘ

Read directory data

Yes



Directory.ReadWrite.All ⓘ

Read and write directory data

Yes

> RoleManagement

4.


Add permissions

Discard

secRMM Policy Configurator Administrator Guide

Request API permissions

[All APIs](#)



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

What type of permissions does your application require?

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

1.

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

Select permissions

expand all

2.

group

Permission	Admin consent required
> Calls	
✓ Group (1)	
<input type="checkbox"/> Group.Create ⓘ Create groups	Yes
<input type="checkbox"/> Group.Read.All ⓘ Read all groups	Yes
<input checked="" type="checkbox"/> 3. Group.ReadWrite.All ⓘ Read and write all groups	Yes
> GroupMember	
> PrivilegedAccess	

4.

Add permissions

Discard

10. Now you need to grant admin consent so that the “secRMM Policy Configurator” can use the APIs you just added above. This is done by clicking the “Grant admin consent for X” as shown in the screenshot below. Note that X will be the name of YOUR company, not “Squadra Technologies”. The screenshot shows “Squadra Technologies” because you are working within the Squadra Technologies Azure tenant/directory whereas you will be working within your companies Azure tenant/directory.

secRMM Policy Configurator Administrator Guide

Home > Squadra Technologies > secRMM Policy Configurator

secRMM Policy Configurator | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

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

Configured permissions

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

+ Add a permission ✓ Grant admin consent for Squadra Technologies

API / Permissions name	Type	Description	Admi...	Status
▼ Microsoft Graph (9)				
DeviceManagementApps.ReadWrite.All	Application	Read and write Microso...	Yes	⚠ Not granted for Squadra Technologies
DeviceManagementConfiguration.ReadWrite.All	Application	Read and write Microso...	Yes	⚠ Not granted for Squadra Technologies
DeviceManagementManagedDevices.PrivilegedOperations.All	Application	Perform user-impacting...	Yes	⚠ Not granted for Squadra Technologies
DeviceManagementManagedDevices.ReadWrite.All	Application	Read and write Microso...	Yes	⚠ Not granted for Squadra Technologies
DeviceManagementRBAC.ReadWrite.All	Application	Read and write Microso...	Yes	⚠ Not granted for Squadra Technologies
DeviceManagementServiceConfig.ReadWrite.All	Application	Read and write Microso...	Yes	⚠ Not granted for Squadra Technologies
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for Squadra Technologies
Group.ReadWrite.All	Application	Read and write all grou...	Yes	⚠ Not granted for Squadra Technologies
User.Read	Delegated	Sign in and read user p...	No	

11. A confirmation dialog will appear. Click the “Yes” button as shown in the screenshot below.

Grant admin consent confirmation.

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

Yes No

include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Squadra Technologies

API / Permissions name	Type	Description	Admi...	Status
▼ Microsoft Graph (9)				
DeviceManagementApps.ReadWrite.All	Application	Read and write Microso...	Yes	⚠ Not granted for Squadra Technologies
DeviceManagementConfiguration.ReadWrite.All	Application	Read and write Microso...	Yes	⚠ Not granted for Squadra Technologies
DeviceManagementManagedDevices.PrivilegedOperations.All	Application	Perform user-impacting...	Yes	⚠ Not granted for Squadra Technologies
DeviceManagementManagedDevices.ReadWrite.All	Application	Read and write Microso...	Yes	⚠ Not granted for Squadra Technologies
DeviceManagementRBAC.ReadWrite.All	Application	Read and write Microso...	Yes	⚠ Not granted for Squadra Technologies
DeviceManagementServiceConfig.ReadWrite.All	Application	Read and write Microso...	Yes	⚠ Not granted for Squadra Technologies
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for Squadra Technologies
Group.ReadWrite.All	Application	Read and write all grou...	Yes	⚠ Not granted for Squadra Technologies
User.Read	Delegated	Sign in and read user p...	No	

12. You should see successful messages as shown in the screenshot below.

secRMM Policy Configurator Administrator Guide

Successfully granted admin consent for the requested permissions.

Configured permissions

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

+ Add a permission ✓ Grant admin consent for Squadra Technologies

API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (9)				
DeviceManagementApps.ReadWrite	Application	Read and write Microsoft Intune apps	Yes	✓ Granted for Squadra Tec...
DeviceManagementConfiguration.ReadWrite	Application	Read and write Microsoft Intune device configuration and...	Yes	✓ Granted for Squadra Tec...
DeviceManagementManagedDevices.Actions	Application	Perform user-impacting remote actions on Microsoft Intu...	Yes	✓ Granted for Squadra Tec...
DeviceManagementManagedDevices.ReadWrite	Application	Read and write Microsoft Intune devices	Yes	✓ Granted for Squadra Tec...
DeviceManagementRBAC.ReadWrite	Application	Read and write Microsoft Intune RBAC settings	Yes	✓ Granted for Squadra Tec...
DeviceManagementServiceConfiguration.ReadWrite	Application	Read and write Microsoft Intune configuration	Yes	✓ Granted for Squadra Tec...
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for Squadra Tec...
Group.ReadWrite.All	Application	Read and write all groups	Yes	✓ Granted for Squadra Tec...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Squadra Tec...

13. Now you need to generate a “client secret” which acts like a password for the “secRMM Policy Configurator”. In the applications “Manage” blade, click the “Certificates & secrets” as shown in the screenshot below.

Home > >

secRMM Policy Configurator ⚙ ...

Search (Ctrl+/) « Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Got a second? We would love your feedback on Microsoft identity platform (f

Essentials

Display name : secRMM Policy Configurator

Application (client) ID : 4a765cad-9bc0-4f28-a1bd-8b437efb0b1a

Object ID : d96180ad-40a5-406b-be25-7bf51b3bb626

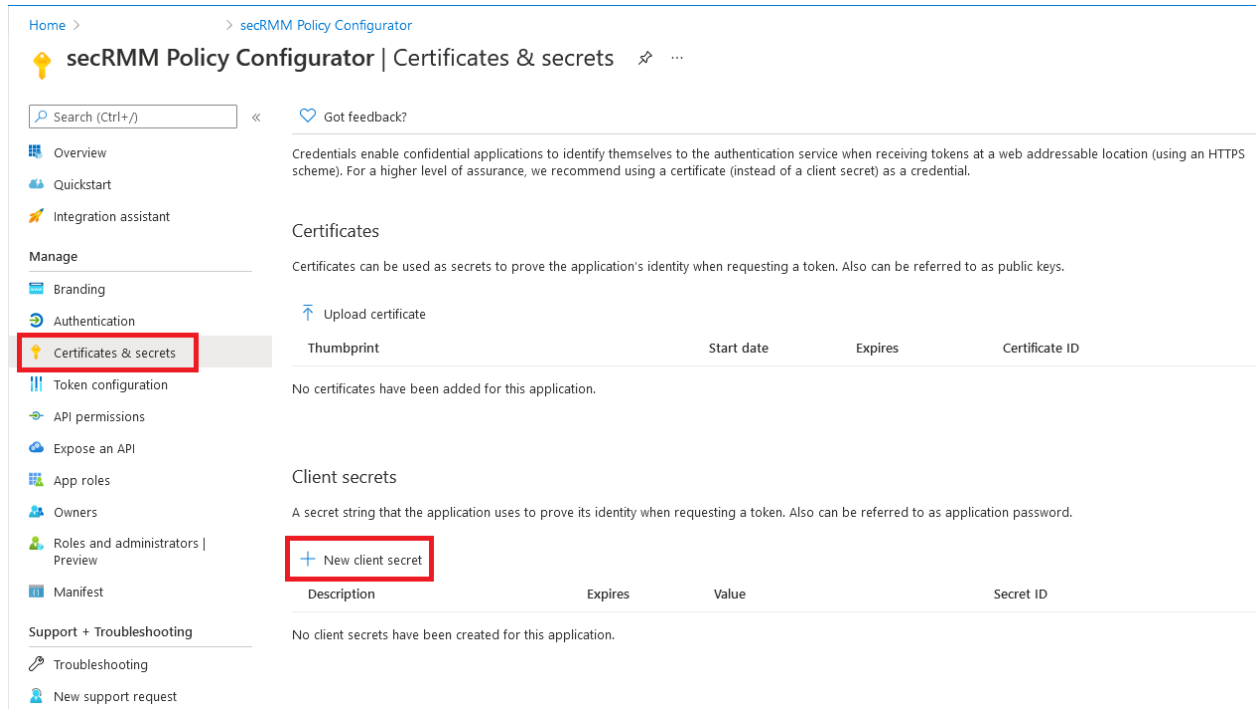
Directory (tenant) ID : 805a3915-a0ac-4d2a-9ec8-4bb702169c30

Supported account types : My organization only

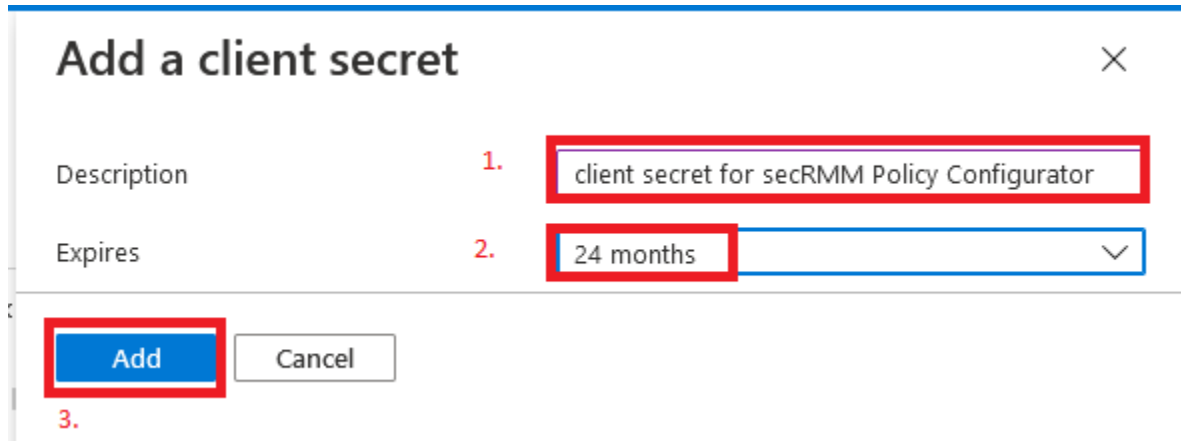
Get Started Documentation

secRMM Policy Configurator Administrator Guide

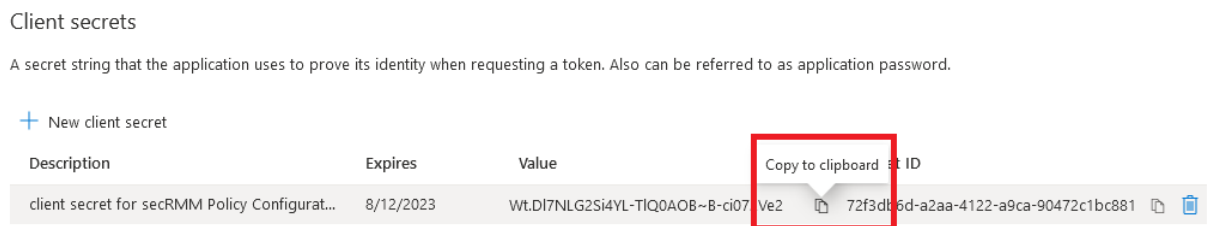
14. Click the “New client secret” as shown in the screenshot below.



15. Add a client secret as shown in the screenshot below.



16. Copy the client secret value to the clipboard as shown in the screenshot below.



17. Open notepad and paste the client secret from the step above into notepad as shown in the screenshot below. Note that the value you will have will be different from the value shown in

secRMM Policy Configurator Administrator Guide

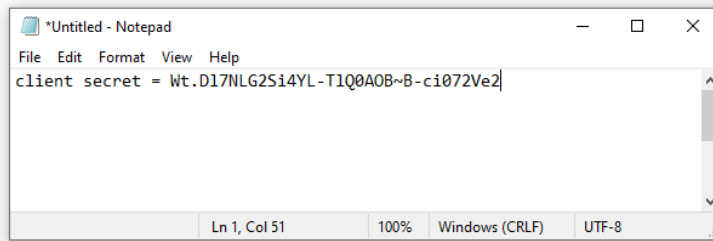
the screenshot below. This value is equivalent to a password. You will need this client secret in a step below to put into the “secRMM Policy Configurator”.

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	Secret ID
client secret for secRMM Policy Configurat...	8/12/2023	Wt.D17NLG2Si4YL-TIQ0A0B~B-ci072Ve2	72f3db6d-a2aa-4122-a9ca-90472c1bc881



In the applications “Manage” blade, click the “Authentication” button. Now, click the 2 checkboxes and then click the Save button at the top of the screen as shown in the screenshot below.

Home > Squadra Technologies > secRMM Policy Configurator

secRMM Policy Configurator | Authentication

Search (Ctrl+/) << **Save** Discard Got feedback?

Got a second to give us some feedback? →

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web

Quickstart Docs

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

http://localhost

[Add URI](#)

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. <https://example.com/logout>

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens](#).

Select the tokens you would like to be issued by the authorization endpoint:

- ☒ Access tokens (used for implicit flows)
- ☒ ID tokens (used for implicit and hybrid flows)

- In the applications “Manage” blade, click the “Manifest” button. Scroll down until you see the line that reads “oauth2AllowIdTokenImplicitFlow”. Change the word false to true. Now click the “Save” button at the top of the screen as shown in the screenshot below.

secRMM Policy Configurator Administrator Guide

secRMM Policy Configurator | Manifest

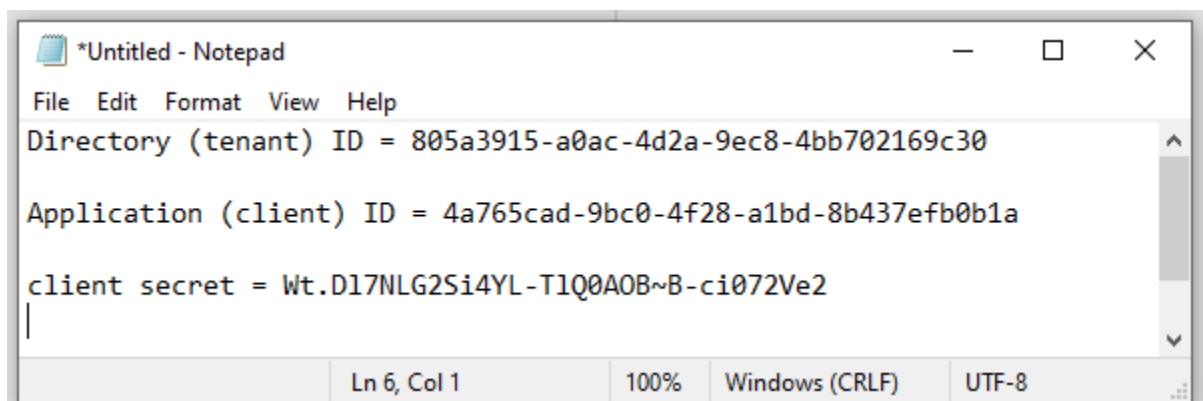
Search (Ctrl+/) Save Discard Upload Download Got feedback?

Successfully updated application.

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

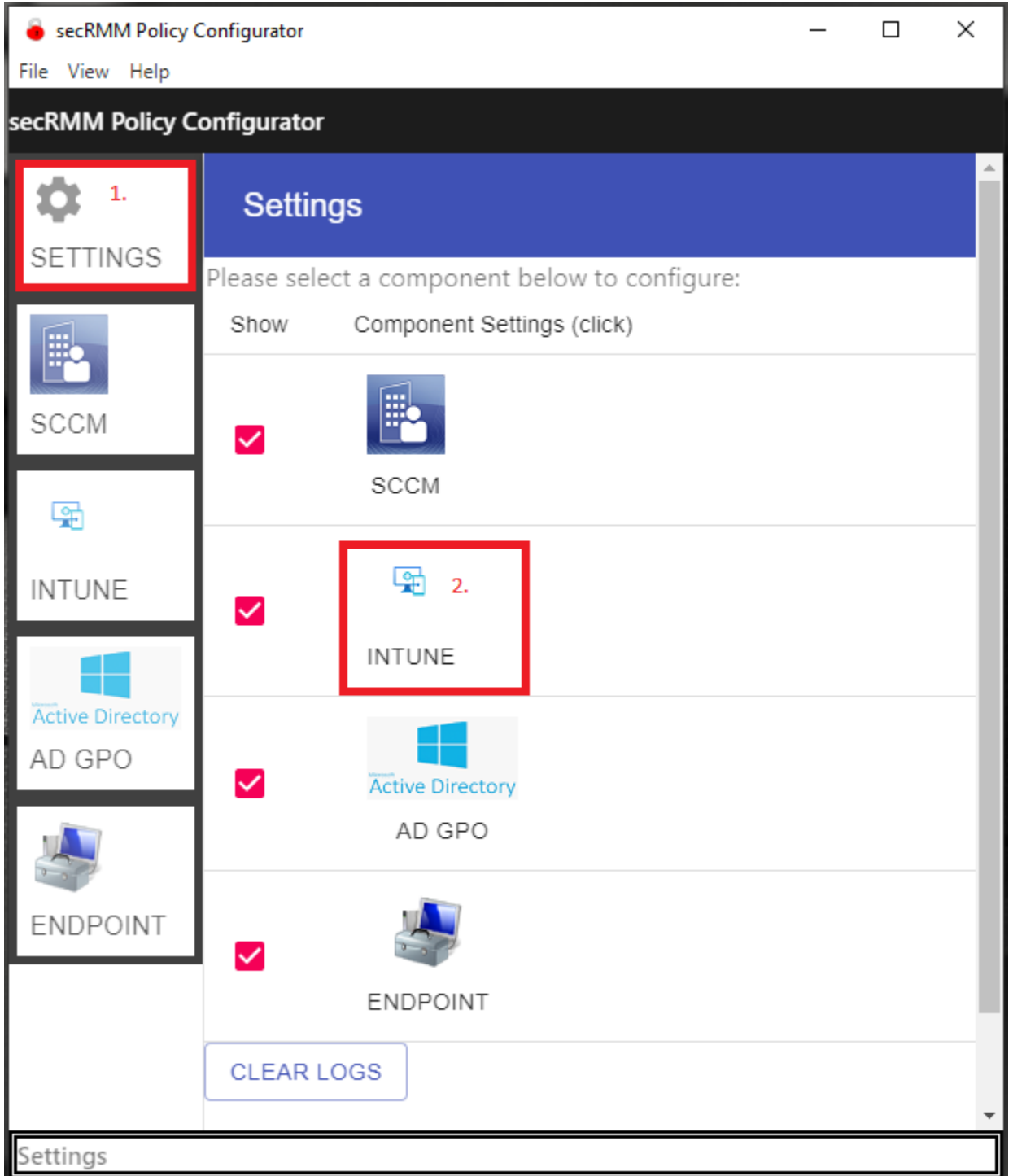
```
12     "groupmembershipclaims": null,
13     "identifieruris": [],
14     "informationalurls": {
15       "termsOfService": null,
16       "support": null,
17       "privacy": null,
18       "marketing": null
19     },
20     "keyCredentials": [],
21     "knownClientApplications": [],
22     "logoUrl": null,
23     "logoutUrl": null,
24     "name": "secRMM Policy Configurator",
25     "oauth2AllowIdTokenImplicitFlow": true,
26     "oauth2AllowImplicitFlow": true,
27     "oauth2Permissions": [],
28     "oauth2RequirePostResponse": false,
29     "optionalClaims": null,
30     "orgRestrictions": [],
31     "parentalControlSettings": {
32       "countriesBlockedForMinors": [],
33       "legalAgeGroupRule": "Allow"
34     },
35     "passwordCredentials": [
36       {
37         "customKeyIdentifier": null,
```

19. Now the Azure application setup is complete. You need the 2 values from step 5 above and the 1 value from step 17 (which you have in notepad). You can just take the 2 values from step 5 and put them in the same notepad as the value from step 17 as shown in the screenshot below.



secRMM Policy Configurator Administrator Guide

20. The 3 values you have in notepad are the values you will put into the “secRMM Policy Configurator”. Open the “secRMM Policy Configurator” and click the “Settings” button. Now click the “Intune” button as shown in the screenshot below.



secRMM Policy Configurator Administrator Guide

Settings for Intune

Azure Tenant Id (Directory) *

Azure Client Id (Application) *

Azure Application Secret

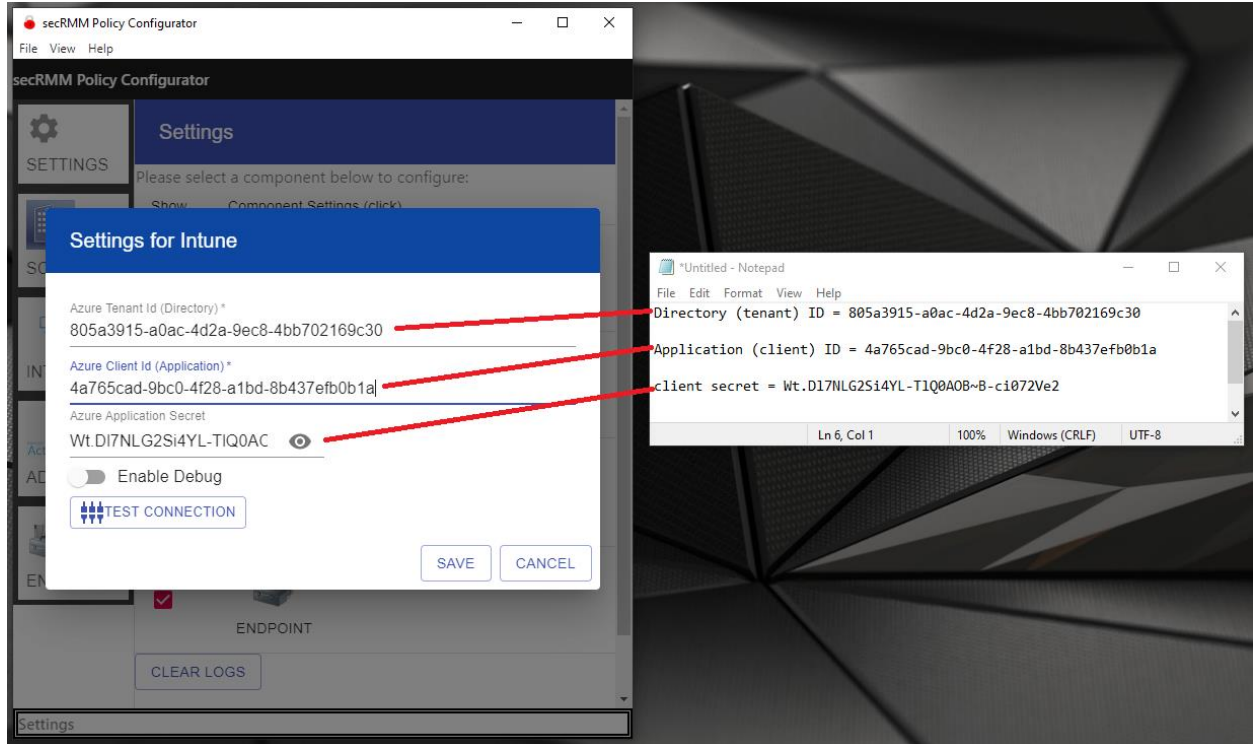
Please enter a value.

☐ Enable Debug

TEST CONNECTION

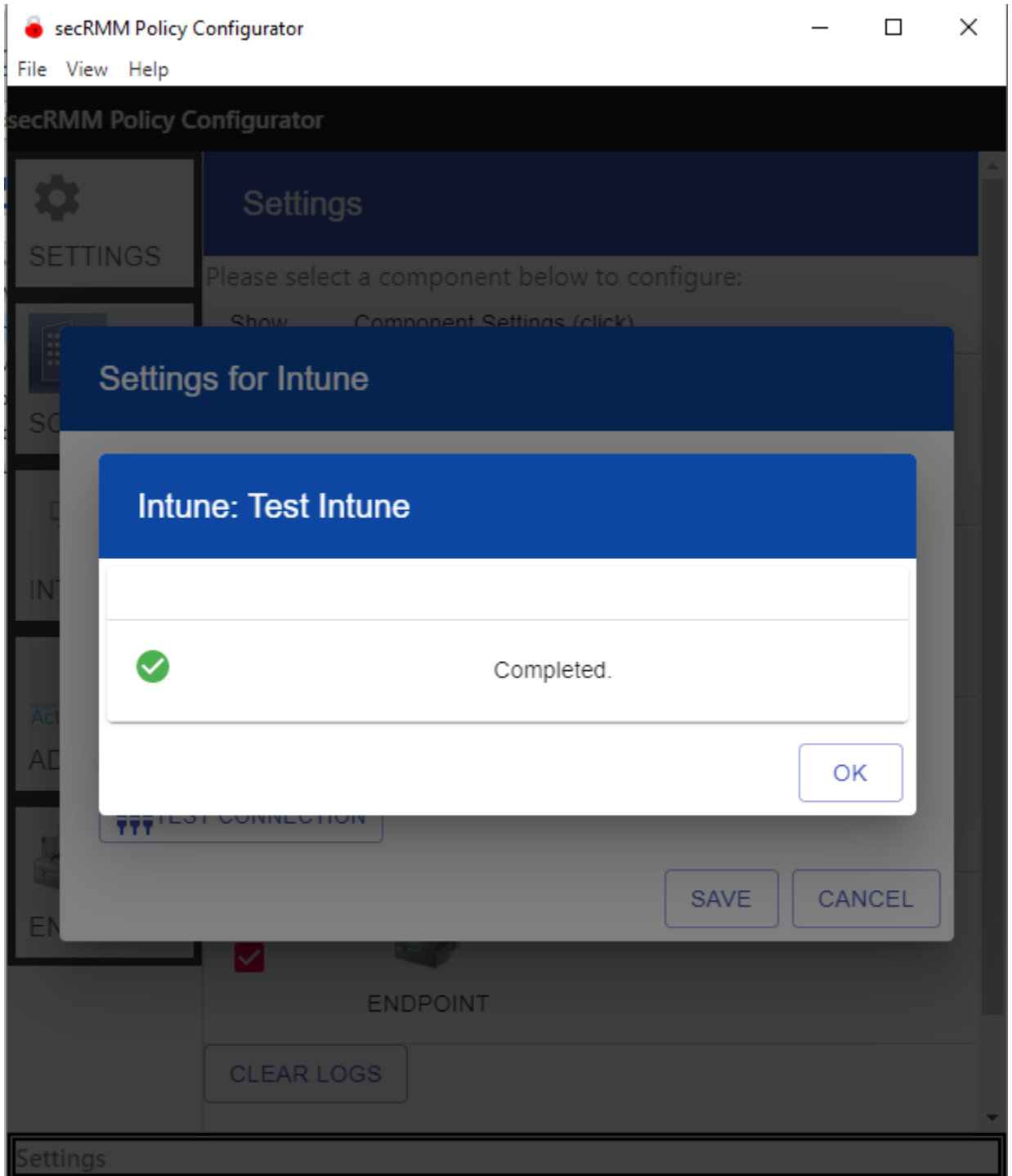
SAVE CANCEL

21. Put the values from notepad into the “secRMM Policy Configurator” text fields as shown in the screenshot below.



secRMM Policy Configurator Administrator Guide

22. Now click the “test connection” button and ensure it says “Completed” as shown in the screenshot below.



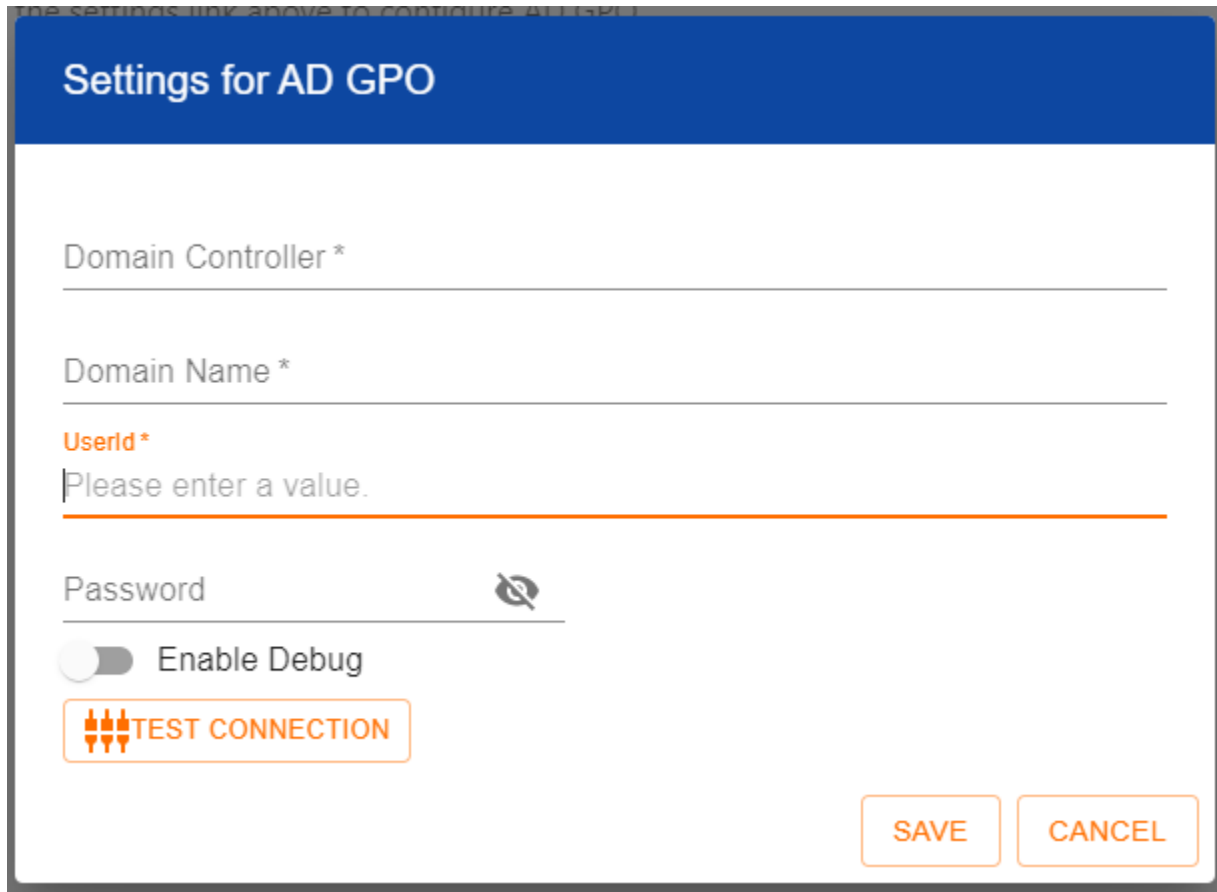
23. You are now ready to use the “secRMM Policy Configurator” with Intune.

Active Directory Group Policy Objects

secRMM Policy Configurator Administrator Guide

For the “secRMM Policy Configurator” to connect to Active Directory Group Policy Objects, you only need to supply:

1. Your Domain Controller Server Name (the NetBios name is sufficient).
2. The domain name (ex: contoso.com).
3. A domain administrator userid/password.



Settings for AD GPO

Domain Controller *

Domain Name *

UserId *

Please enter a value.

Password

Enable Debug

TEST CONNECTION

SAVE CANCEL

Endpoint

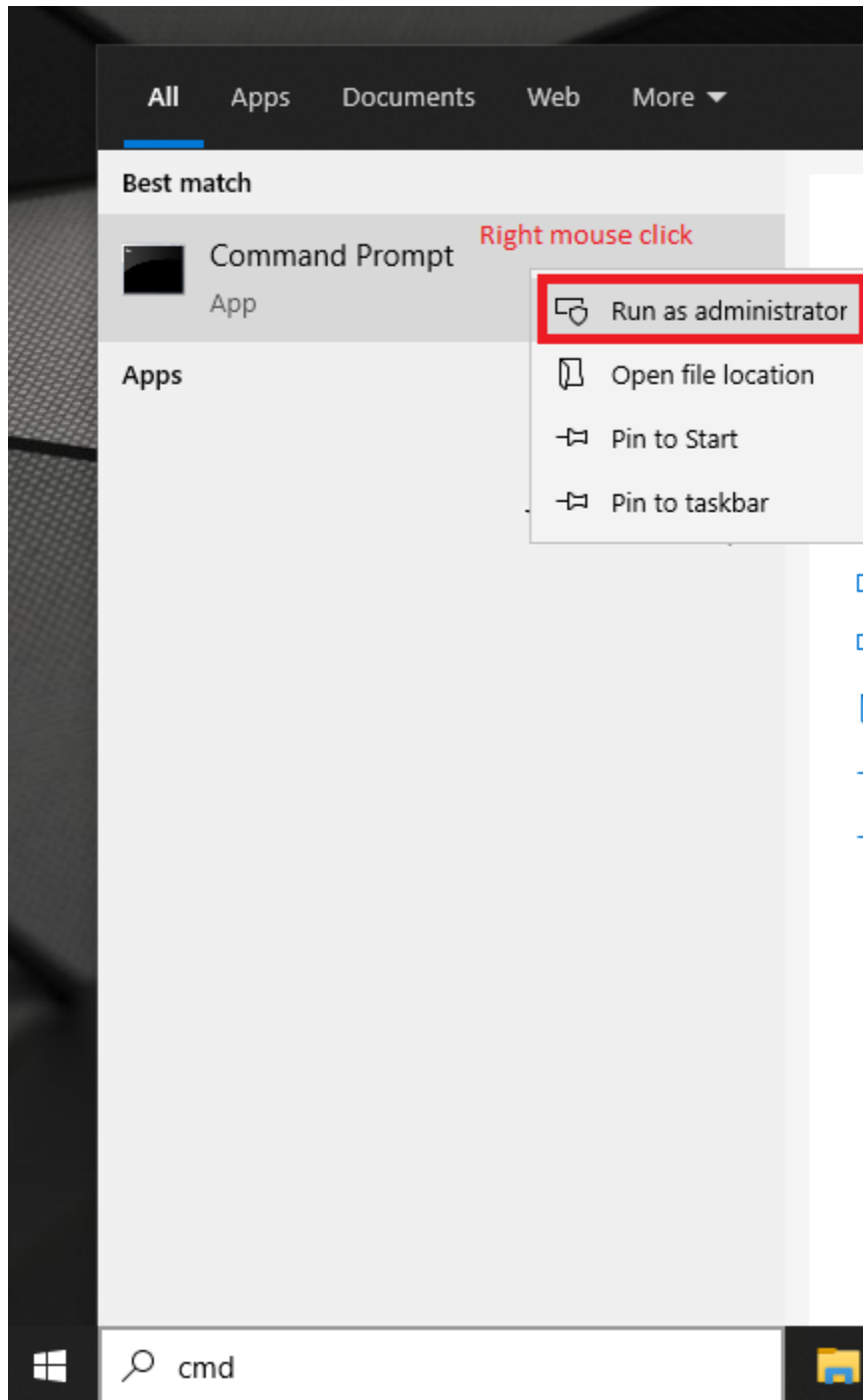
For the “secRMM Policy Configurator” to connect to other Windows computers (i.e. Endpoints), you need to setup WinRM on the Windows computers (if it is not already enabled) and configure WinRM on the Windows computer that is running the “secRMM Policy Configurator”. Please follow the steps below to configure WinRM as stated above.

Configuring the Endpoint Computers

Enabling WinRM

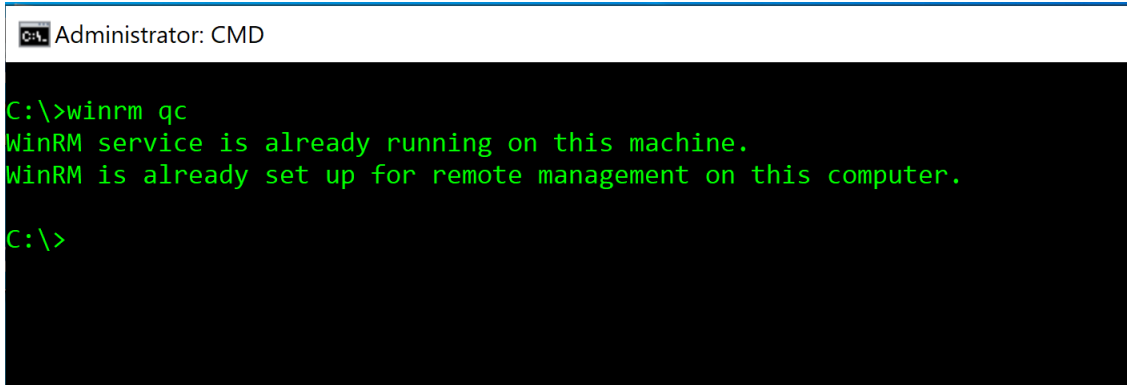
Please follow the steps below to enable WinRM:

1. Open Windows CMD using “Run As Administrator as shown in the screenshot below.



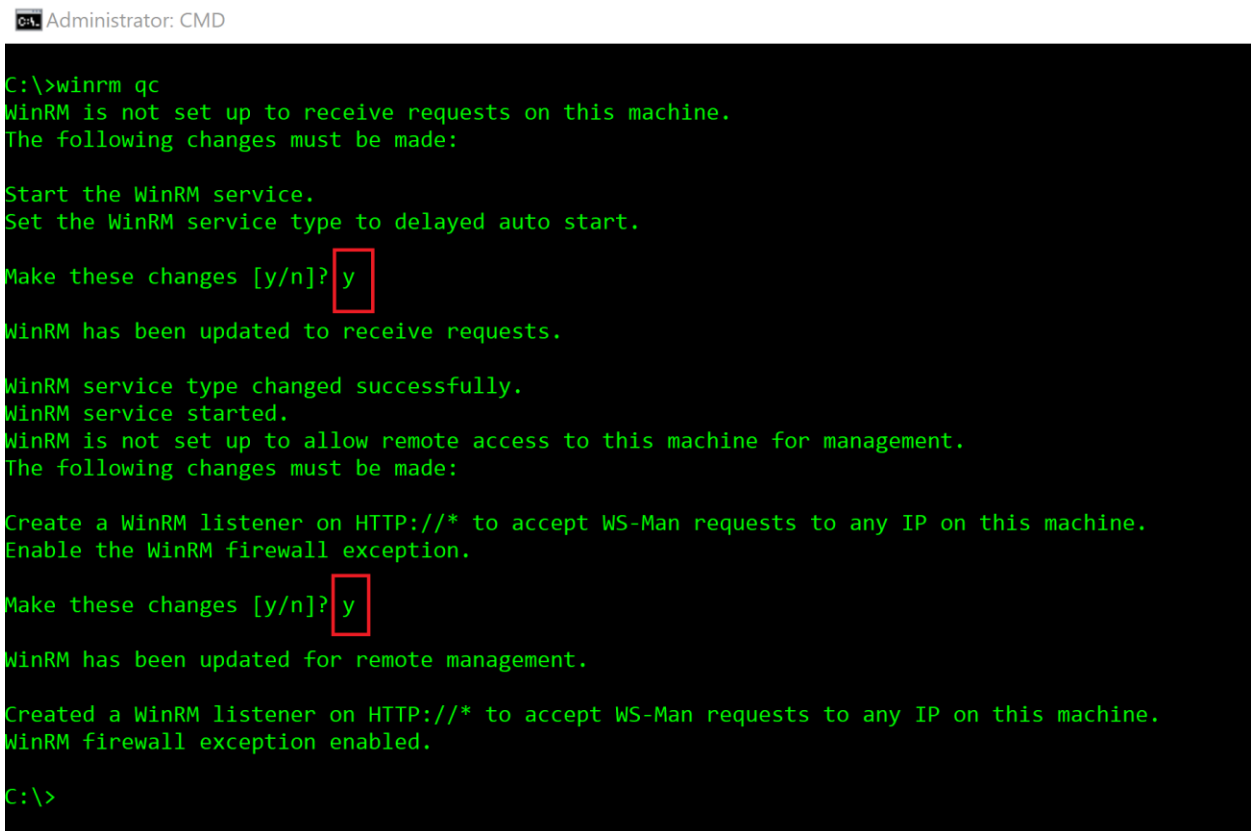
2. In the CMD Window, type “winrm qc” as shown in the screenshot below. Note that in the first screenshot, WinRM has already been enabled on the Windows computer. This may be a likely scenario for your environment. If it is not already enabled, go to step 3 below for instructions.

secRMM Policy Configurator Administrator Guide



A screenshot of a Windows Command Prompt window titled "Administrator: CMD". The text inside shows the command `C:\>winrm qc` being executed. The output is: `WinRM service is already running on this machine.` and `WinRM is already set up for remote management on this computer.` The prompt `C:\>` is shown again at the bottom.

3. If WinRM is not already enabled as shown in the screenshot above, it will then look like the screenshot below. Note that you will need to respond to 2 questions by typing the y character as shown in the screenshot below.



A screenshot of a Windows Command Prompt window titled "Administrator: CMD". The text inside shows the command `C:\>winrm qc` being executed. The output is: `WinRM is not set up to receive requests on this machine.` and `The following changes must be made:`
`Start the WinRM service.`
`Set the WinRM service type to delayed auto start.`
`Make these changes [y/n]? y` (The 'y' is highlighted with a red box)
`WinRM has been updated to receive requests.`
`WinRM service type changed successfully.`
`WinRM service started.`
`WinRM is not set up to allow remote access to this machine for management.`
`The following changes must be made:`
`Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.`
`Enable the WinRM firewall exception.`
`Make these changes [y/n]? y` (The 'y' is highlighted with a red box)
`WinRM has been updated for remote management.`
`Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.`
`WinRM firewall exception enabled.`
The prompt `C:\>` is shown at the bottom.

4. The computer is now enabled to receive WinRM commands from the “secRMM Policy Configurator”.

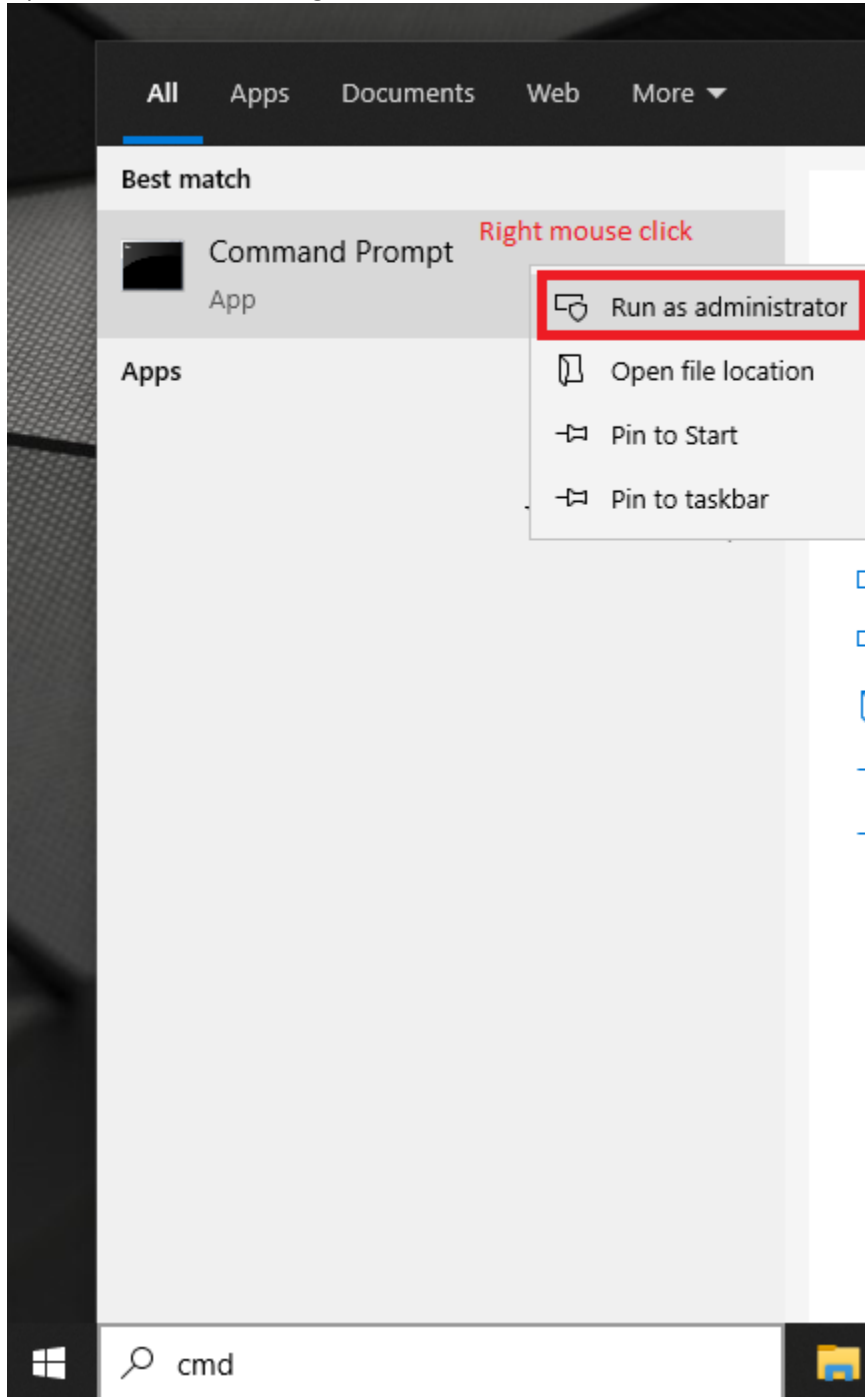
Disabling WinRM

For completeness, we will document how to undo the “winrm qc” command that was documented above.

secRMM Policy Configurator Administrator Guide

Please follow the steps below to disable WinRM:

1. Open Windows CMD using "Run As Administrator as shown in the screenshot below.



2. In the CMD Window, disable the WinRM firewall rules by typing:
`netsh advfirewall firewall set rule name="Windows Remote Management (HTTP-In)" new enable=no`
3. In the CMD Windows, delete the WinRM listener by typing:

secRMM Policy Configurator Administrator Guide

```
winrm delete winrm/config/Listener?Address=*&Transport=HTTP
```

4. In the CMD Windows, stop the WinRM service by typing:

```
sc stop winrm
```
5. In the CMD Windows, disable the WinRM service by typing (please note that, you MUST have a space after the equal (=) sign):

```
sc config winrm start= disabled
```

Configuring the “secRMM Policy Configurator” Computer

The computer that will run the “secRMM Policy Configurator” program also needs to have WinRM enabled so please follow the section above titled “Enabling WinRM” before following the steps below.

For each Windows computer that you want to deploy secRMM policy(s) to, you will need to add that computer to the “WinRM TrustedHosts list” on the Windows computer that is running the “secRMM Policy Configurator” program. To accomplish this task, you will use 2 Powershell commands. In the text below (as an example), the computer you want to add to the “WinRM TrustedHosts list” is named W10EnterpriseVM.

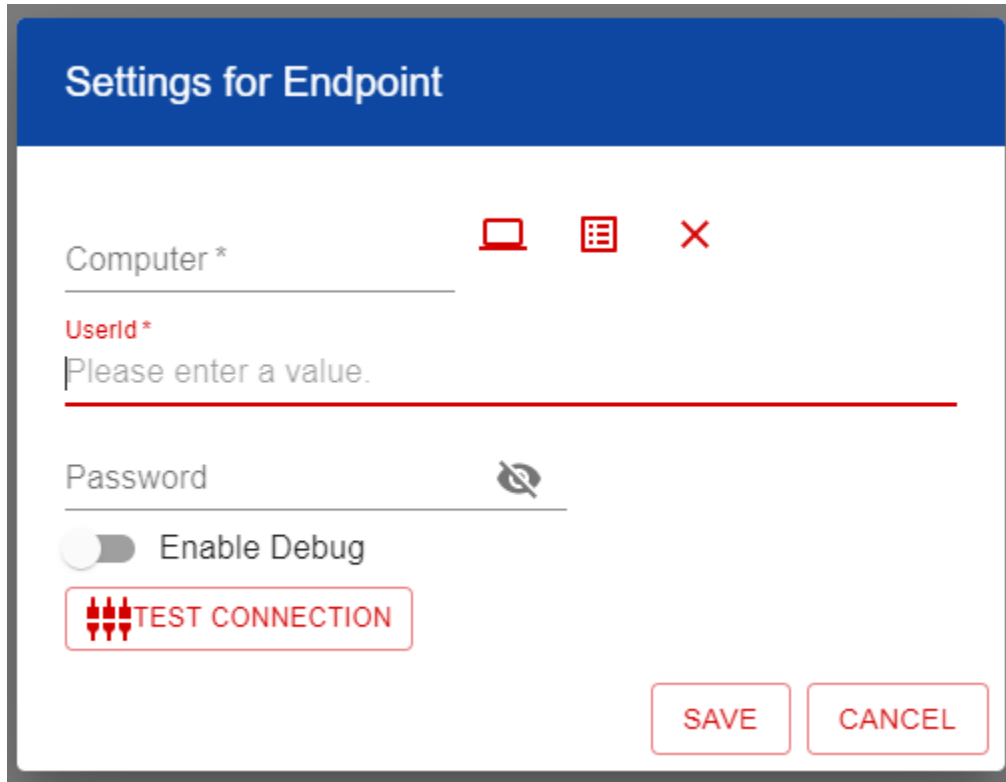
```
$List = (Get-Item WSMan:\localhost\Client\TrustedHosts).value  
Set-Item WSMan:\localhost\Client\TrustedHosts -Value "$List, W10EnterpriseVM"
```

There are lots of examples on the Internet about other ways to accomplish this task if you search for “WinRM TrustedHosts”. Of course your best bet (if you need help with this task) is to contact Squadra Technologies technical support and we will do this step for you and educate you on your options within your environment.

Specifying the WinRM credentials

You are now ready to specify the computer(s) and credentials in the “secRMM Policy Configurator” program. The list of computers is a semicolon separated list of computers. For the userid/password, if you are in a domain, then specify a domain administrator account. If you are in a workgroup, specify a local administrator account that is defined on every computer in the computer list.

Note that in the list of computers, one of the computers will be used as the “master computer”. The “master computer” will be the first computer in the list unless the computer running the “secRMM Policy Configurator” is also in the list of computers. If the “secRMM Policy Configurator” computer is in the list of computers, then it will be the “master computer”. The job of the “master computer” is to be the computer where the secRMM policy(s) are pulled from.



Settings for Endpoint

Computer *

Userid *

Please enter a value.

Password

Enable Debug

TEST CONNECTION

SAVE CANCEL

Microsoft documentation for WinRM

<https://docs.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-windows-remote-management>.

Technical Details

This section covers some important technical details about the “secRMM Policy Configurator” program.

The computer running “secRMM Policy Configurator” program should have PowerShell version 5 or greater installed.

All of the Microsoft technologies that are covered in the sections above are implemented in Powershell. This means that you are free to modify how the technologies work within your environment by modifying the Powershell scripts within the “secRMM Policy Configurator”. The scripts are located in the subdirectory of the “secRMM Policy Configurator” at “C:\Program Files\secRMMPolicyConfigurator\dist\scripts” as shown in the screenshot below.

secRMM Policy Configurator Administrator Guide

This PC > OS (C:) > Program Files > secRMMPolicyConfigurator > dist > scripts				
Name	Date modified	Type	Size	
ActiveDirectory	8/12/2021 10:24 AM	File folder		
Common	8/12/2021 1:20 PM	File folder		
Endpoint	8/12/2021 10:24 AM	File folder		
Intune	8/12/2021 1:36 PM	File folder		
PropertyTests	8/12/2021 10:24 AM	File folder		
SCCM	8/12/2021 10:24 AM	File folder		
secRMMPolicyConfiguratorConfig.xml	8/12/2021 1:38 PM	XML Document	3 KB	

Please contact Squadra Technologies support if you would like to make changes and we would be happy to help.

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, w10, etc.
3. The version of the “secRMM Policy Configurator” you have installed.
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/