



Security Removable Media Manager
(secRMM)

Microsoft Entra Verified ID Setup Guide

Version 9.11.27.0

(April 2024)

Protect your valuable data



secRMM Entra Verified ID Setup Guide

© 2011 Squadra Technologies, LLC. ALL RIGHTS RESERVED.

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

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

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

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

TRADEMARKS

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

Disclaimer

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

Squadra Technologies Administrator Guide
Created - March 2011

Contents

INTRODUCTION	4
PREREQUISITES.....	4
SETUP OVERVIEW.....	4
SETUP DETAILS	5
CREATE THE CUSTOM AZURE VC CREDENTIAL IN YOUR AZURE TENANT	5
SEND YOUR DID TO SQUADRA TECHNOLOGIES	9
POPULATE SECRMM WITH THE AZURE VC VALUES FROM YOUR TENANT.....	10
<i>TenantID</i>	11
<i>ApplicationID/Application Secret</i>	12
<i>DID</i>	13
<i>Manifest URL</i>	13
ISSUING AND TESTING AZURE VC	14
ISSUING A CERTIFICATE TO AN END-USER	15
TESTING A CERTIFICATE.....	22
WHEN A REMOVABLE STORAGE DEVICE MOUNTS	26
CONTACTING SQUADRA TECHNOLOGIES SUPPORT	30
ABOUT SQUADRA TECHNOLOGIES, LLC.	30

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.

secRMM allows the system/security administrator to have end-users who want to use removable media devices authenticate themselves when they mount the device to the Windows computer. One way to accomplish this is to use Microsoft Entra Verified ID. Microsoft Entra Verified ID is the Microsoft implementation of an Internet standard called 'Decentralized Identity'. Microsoft Entra Verified ID is a service running in your Azure tenant that works in conjunction with the Microsoft Authenticator phone app. The system/security administrator issues a credential to the end-users Authenticator app on their phone. When the end-user mounts a removable media device, they must first scan a QrCode using their Microsoft Authenticator app before they will be allowed to access the removable media device.

If the functionality in the paragraph above is a desirable feature for your environment, this document will help you setup this secRMM feature (RequireAzureVC property).

Note: the secRMM terminology calls 'Microsoft Entra Verified ID' as 'Azure Verifiable Credentials' (i.e. Azure VC). When the secRMM code was developed, it was called Azure VC and since then, Microsoft has renamed it to 'Microsoft Entra Verified ID'.

Prerequisites

You will need to have an Azure tenant. By default, this also means you will have an "Azure Active Directory" (AAD) instance. 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 setup the secRMM connection to your Azure tenant.

1. Follow the Microsoft documentation to create a Microsoft Entra Verified ID in your Azure tenant. The link is: <https://docs.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant>.

Once you have followed these steps from Microsoft, you will have created an Azure Key Vault and you will have registered an application in Azure Active Directory. Both the Azure Key Vault and the registered application are used by Azure VC.

2. Instead of using the default Microsoft verifiable credential however, you will use a **custom verifiable credential for secRMM**. This is shown in the 'Setup details' section below.
3. Send your DID to Squadra Technologies so that we can add it to the list of trusted DIDs.
4. Populate the secRMM 'RequireAzureVC' property using the values from your Azure tenant.

Setup details

Create the custom Azure VC credential in your Azure tenant

In your Azure tenant, under 'Verified ID', click the 'Add a credential' as shown in the screenshot below.

The screenshot shows the 'Verified ID | Credentials' page in the Azure Active Directory portal. At the top, there is a breadcrumb navigation 'Home > Verified ID'. Below the title, there is a sub-header 'Azure Active Directory'. On the right side of the header, there are three buttons: a back arrow ('<<'), a red-bordered 'Add a credential' button with a plus sign, and a 'Refresh' button with a circular arrow icon. On the left, there is a vertical sidebar with four options: 'Overview' (selected), 'Credentials' (highlighted with a grey background), 'Organization settings', and 'Registration'. The main content area has a table with columns 'Name' and 'Type'. There are no rows currently listed.

Click the 'Custom credential' and then click the Next button at the bottom of the page. This is shown in the screenshot below.

secRMM Entra Verified ID Setup Guide

Home > Verified ID | Credentials >

Create credential

...

Once the credential is created it will be a part of the Entra Verified ID network. Information including your company and domain name will be published so other organizations will be able to verify in their own tenant & application(s).

[Learn more](#)

Organization details

Organization i

SquadraTechnologies

Linked domain i

<https://www.squadratechnologies.com/>

 Verified domain

Select a credential type

Verified employee

Verified employee credential

Custom credential

Design your own credential from scratch.

Verified student (Coming soon)

A credential that contains the claims:
name, first name, last name, email, photo,
role, and school.

Next

Cancel

secRMM Entra Verified ID Setup Guide

In the 'Credential name', name your credential. It can be any value you want. In the screenshot below, we used secRMM.

In the 'Display definition', replace the text with:

```
{  
  "locale": "en-US",  
  "card": {  
    "backgroundColor": "#ffffff",  
    "description": "Use your verified credential to access removable media.",  
    "issuedBy": "Squadra Technologies",  
    "textColor": "#000000",  
    "title": "Verified Credential SecRMM",  
    "logo": {  
      "description": "Verified Credential secRMM Logo",  
      "uri": "https://www.squadratechnologies.com/Products/secRMM/Vendors/Microsoft/VerifiedCredentialSecRMM\_icon.png"  
    }  
  },  
  "consent": {  
    "instructions": "Sign in with your account to get your card.",  
    "title": "Do you want to get your Verified Credential?"  
  },  
  "claims": [  
    {  
      "claim": "vc.credentialSubject.givenName",  
      "label": "Name",  
      "type": "String"  
    },  
    {  
      "claim": "vc.credentialSubject.familyName",  
      "label": "Surname",  
      "type": "String"  
    }  
  ]  
}
```

In the 'Rules definition', replace the text with:

```
{  
  "attestations": {  
    "idTokenHints": [  
      {  
        "mapping": [  
          {  
            "outputClaim": "givenName",  
            "required": false,  
            "inputClaim": "given_name",  
            "indexed": false  
          },  
          {  
            "outputClaim": "familyName",  
            "required": false,  
            "inputClaim": "family_name",  
            "indexed": false  
          }  
        ],  
        "name": "idTokenHint",  
        "value": "true"  
      }  
    ]  
  }  
}
```

secRMM Entra Verified ID Setup Guide

```
        "required": false,
        "trustedIssuers": []
    }
],
"validityInterval": 2592000,
"vc": {
    "type": [
        "VerifiedCredentialSecRMM"
    ]
}
}
```

Click the 'Create' button as shown in the screenshot below.

[Home](#) > [Verified ID | Credentials](#) > [Create credential](#) >

Create a new credential ...



Display definition * ⓘ

The display definition describes the claims contained in the credential as well as the branding.

```
1  {
2      "locale": "en-US",
3      "card": {
4          "backgroundColor": "#ffffff",
5          "description": "Use your verified credential to access removable media.",
6          "issuedBy": "Squadra Technologies",
7          "textColor": "#000000",
8          "title": "Verified Credential SecRMM",
9          "logo": {
10              "description": "Verified Credential secRMM Logo",
11              ...
12          }
13      }
14  }
```

[Learn how to create the display definition](#) ⓘ

Rules definition * ⓘ

The rules definition determines what the user needs to do to get the credentials. Include an index claim if you want to be able to search for the credential later.

```
20  {
21      "trustIssuers": []
22  },
23  "validityInterval": 2592000,
24  "vc": {
25      "type": [
26          "VerifiedCredentialSecRMM"
27      ]
28  }
29 }
30 }
```

[Learn how to create the rules definition](#) ⓘ

Create

Send your DID to Squadra Technologies

In your Azure portal, under 'Verified ID'->'Overview', click your 'Domain' URL as shown in the screenshot below.

The screenshot shows the 'Verified ID | Overview' page in the Azure Active Directory portal. The 'Overview' tab is selected and highlighted with a red box. On the left, there's a 'Manage' sidebar with 'Credentials', 'Organization settings', and 'Registration' options. The main area is titled 'Basic information' and shows 'Organization name' as 'SquadraTechnologies'. Below it, the 'Domain' field contains 'https://www.squadratechnologies.com/' with a green checkmark icon and the text 'Verified domain' next to it. A red box highlights this entire row.

Now click the 'Verify' link as shown in the screenshot below.

The screenshot shows the 'Domain' overview page. The 'Domain' field contains 'https://www.squadratechnologies.com/'. Below it, there are two sections: 'DID registration' (status: 'Registered Review') and 'Domain ownership verification' (status: 'Domain has been verified'). The 'Verify' link in the 'Domain ownership verification' section is highlighted with a red box.

Copy the lines shown in the next page and send them to Squadra Technologies (support@squadratechnologies.com) so that your DID can be added to the list of approved DIDs.

How to verify this domain's ownership

X

Verifying your domain is important to build trust with your users and other organizations.

[Learn more on verification](#)

1. Copy or download the manifest

```
1  {
2    "@context": "https://identity.foundation/.well-known/conte
3    "linked_dids": [
4      "eyJhbGciOiJFUzI1NksilCJraWQiOijkaWQ6d2Vi0nd3dy5zcXVhZH
5    ]
6  }
```

Populate secRMM with the Azure VC values from your tenant

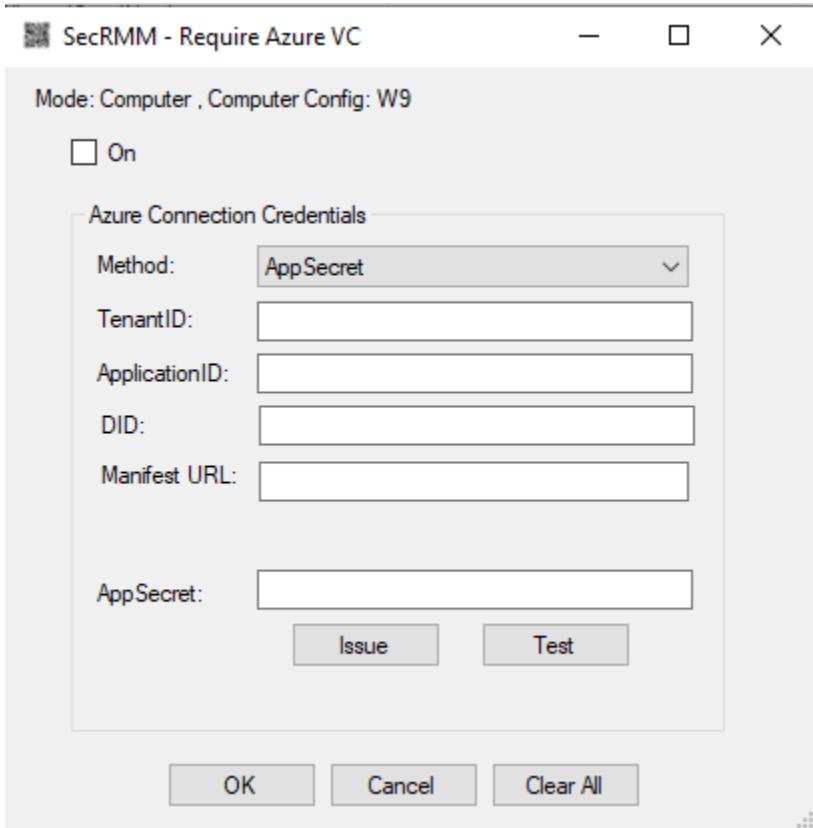
The values needed to populate secRMM so that it can use Azure VC are:

1. Set the checkbox to On
2. Set the Method to 'AppSecret'
3. Specify your Azure TenantID
4. Specify the Azure ApplicationID associated with your Azure VC service
5. Specify the Azure VC DID
6. Specify the Azure VC Manifest URL
7. Specify the Azure Application Secret associated with your Azure VC service

You can see these values in the screenshot below.

The section below shows you where you get these values in your Azure tenant.

secRMM Entra Verified ID Setup Guide



TenantID

You can get your Azure tenantID by clicking 'Organization settings' under the 'Verified ID' azure blaze as shown in the screenshot below. There are other methods and azure web pages that expose the Azure tenantID as well so if you are comfortable with other methods, they will work as well.

The screenshot shows the 'Verified ID | Organization settings' page in the Azure Active Directory portal. The 'Organization settings' tab is selected. On the left, there are navigation links for 'Overview', 'Manage', 'Credentials', and 'Registration'. The main area displays several configuration settings: 'Organization name' (SquadraTechnologies), 'Tenant identifier' (805a3915-a0ac-4d2a-9ec8-4bb702169c30, highlighted with a red box), 'Decentralized identifier (DID)' (did:web:www.squadratechnologies.com), 'Key vault' (https://azurercvcsecrmm.vault.azure.net/), and 'Signing key identifier' (https://azurercvcsecrmm.vault.azure.net/keys/vcSigningKey-1227f612-ff...). At the bottom, there are buttons for 'Reset your organization' and 'Delete all credentials and reset service'.

ApplicationID/Application Secret

You can get the ApplicationID and 'Application Secret' by going into Azure Active Directory, clicking on 'App registrations' as shown in the screenshot below

The screenshot shows the Microsoft Azure portal interface. On the left, there is a navigation sidebar with various service icons and links. A red box highlights the 'Azure Active Directory' link under the 'All services' section. On the right, the main content area shows the 'Azure Active Directory' blade with its own navigation menu. A second red box highlights the 'App registrations' link under the 'Manage' section.

- + Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- Intune
- Verified ID
- Log Analytics workspaces
- Microsoft Sentinel
- Microsoft Defender for Cloud
- Azure Active Directory
- Virtual machines
- All resources
- Resource groups
- Storage accounts
- Virtual networks

Home < Azure Active Directory

- Overview
- Preview features
- Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance

Click the app that you created in

secRMM Entra Verified ID Setup Guide

DID

You can get the DID by clicking 'Organization settings' under the 'Verified ID' azure blaze as shown in the screenshot below.

The screenshot shows the 'Verified ID | Organization settings' page in the Azure Active Directory portal. The left sidebar has 'Overview', 'Manage', 'Credentials', and 'Organization settings' (which is selected and highlighted with a red box). The main area shows fields for 'Organization name' (SquadraTechnologies), 'Tenant identifier' (805a3915-a0ac-4d2a-9ec8-4bb702169c30), 'Decentralized identifier (DID)' (did:web:www.squadratechnologies.com, also highlighted with a red box), 'Key vault' (https://azurvcsecrmm.vault.azure.net/), and 'Signing key identifier' (https://azurvcsecrmm.vault.azure.net/keys/vcSigningKey-1227f612-ff...). At the bottom are 'Reset your organization' and 'Delete all credentials and reset service' buttons.

Manifest URL

To get the 'Manifest URL', in your Azure portal, go to 'Verified ID', click 'Credentials', click the secRMM credential named 'VerifiedCredentialSecRMM' as shown in the screenshot below.

The screenshot shows the 'Verified ID | Credentials' page in the Azure Active Directory portal. The left sidebar has 'Overview', 'Manage', 'Credentials' (selected and highlighted with a red box), and 'Organization settings'. The main area shows a table with one row for 'VerifiedCredentialSecRMM' (Name column) and 'Custom type' (Type column). There are 'Add a credential' and 'Refresh' buttons at the top right. The 'Manage' section of the sidebar is also highlighted with a red box.

secRMM Entra Verified ID Setup Guide

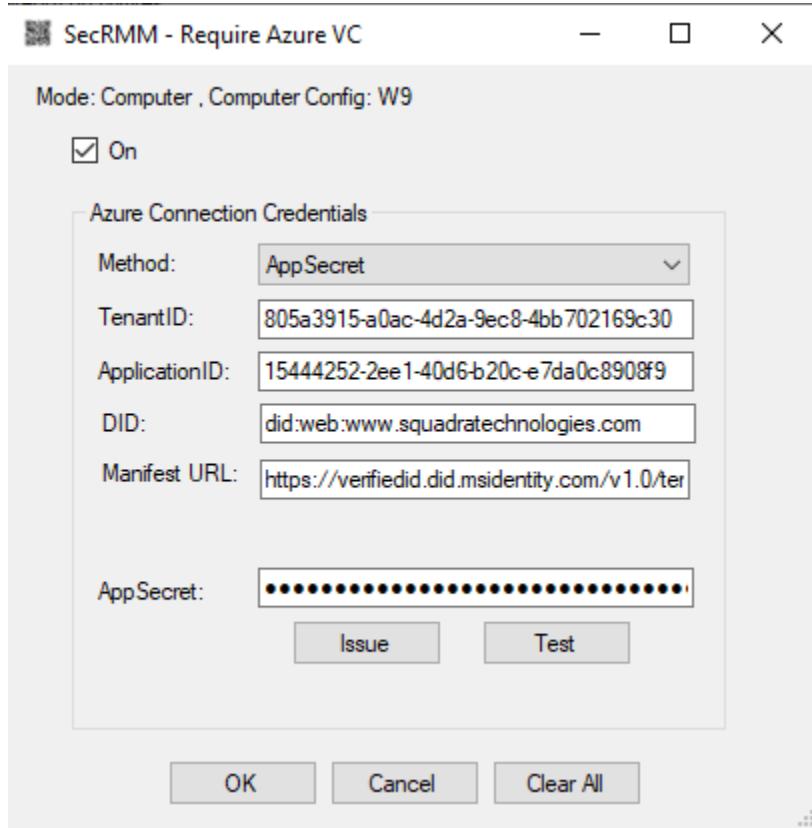
At the bottom of the page, you will see the 'Manifest URL' as shown in the screenshot below. Right click on the 'Manifest URL' and then select 'Copy Link'.

The screenshot shows the 'Verified Credential SecRMM' page in the Microsoft Entra Verified ID section. The 'Details' tab is selected. In the 'Organization details' section, the organization is listed as 'SquadraTechnologies' and the linked domain is 'https://www.squadratechnologies.com/' with a green checkmark indicating it's a 'Verified domain'. Below this, there's a 'Credential preview' section showing a card for 'Verified Credential SecRMM' from 'Squadra Technologies'. The 'Manifest URL' field contains the URL 'https://verifiedid.did.msidentity.co/ODA1YTM5MTUTBhyy00ZDJhLTlIYzgtNGJiNzAyMTY5YzMwdmVyaWZpZWJcmVkZW50aWFsc2Vjcm1t/manifest'. A context menu is open over this URL, with the 'Copy Link' option highlighted by a red box and the number '2.' next to it. Other options in the menu include 'Open Link in New Tab', 'Open Link in New Window', 'Open Link in New Private Window', 'Bookmark Link', 'Save Link As...', 'Save Link to Pocket', 'Search Brave for "https://verifie...', 'Inspect Accessibility Properties', and 'Inspect (Q)'.

Issuing and testing Azure VC

Now that your Azure VC environment is configured for secRMM, as the system administrator, you can issue certificates to your end-users and you can test that the workflow is working properly. This can be done on a computer with secRMM installed and that has the 'RequireAzureVC' property populated as shown in the screenshot below.

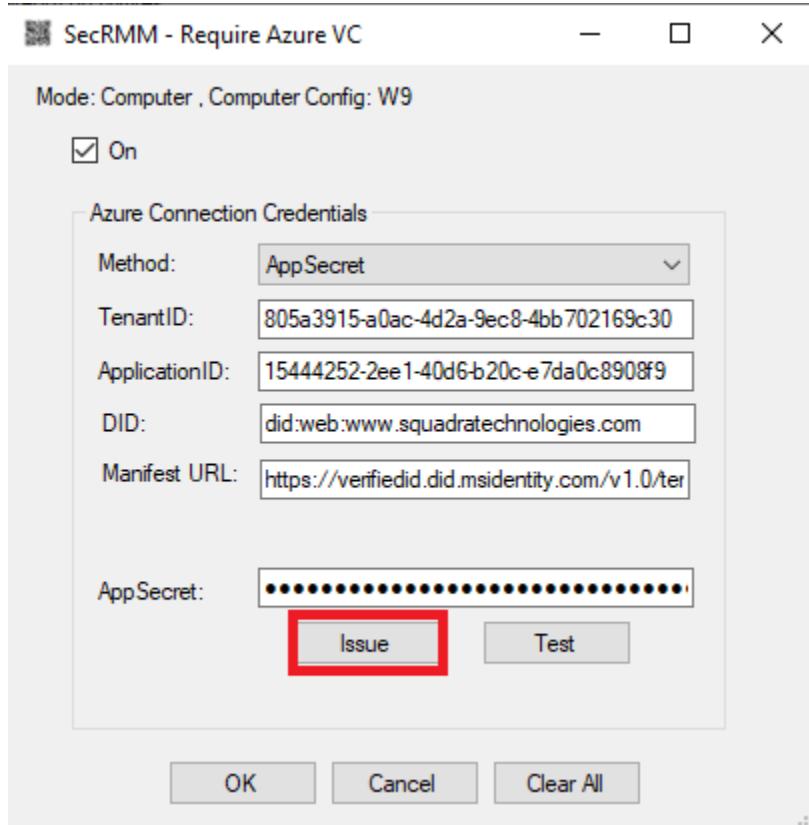
secRMM Entra Verified ID Setup Guide



Issuing a certificate to an end-user

To issue a certificate to an end-user, click the 'Issue' button as shown in the screenshot below.

secRMM Entra Verified ID Setup Guide



Have your end-user scan the QRCode on the screen using their personal phone using the Microsoft Authenticator app as shown in the screenshots below.

Cancel



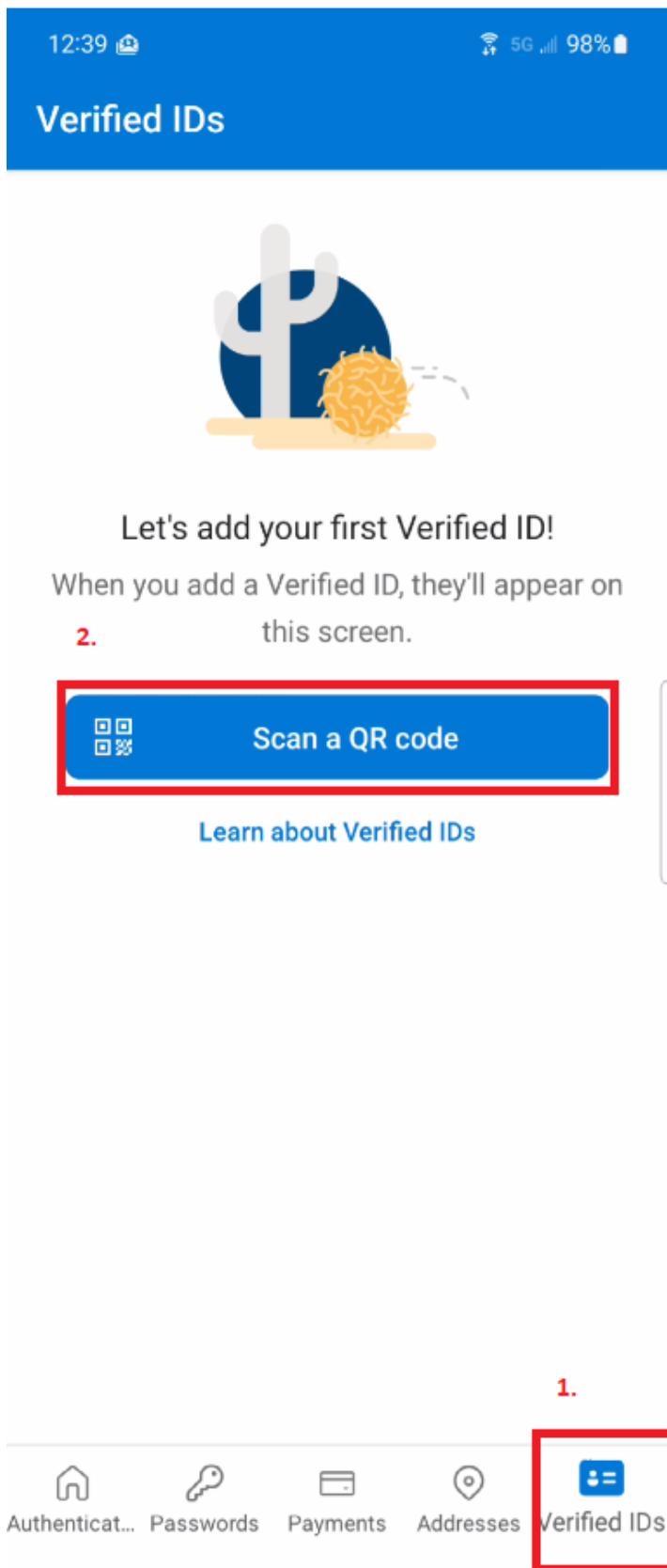
PIN: 5934

Please scan this QrCode using the Microsoft Authenticator App on your phone.



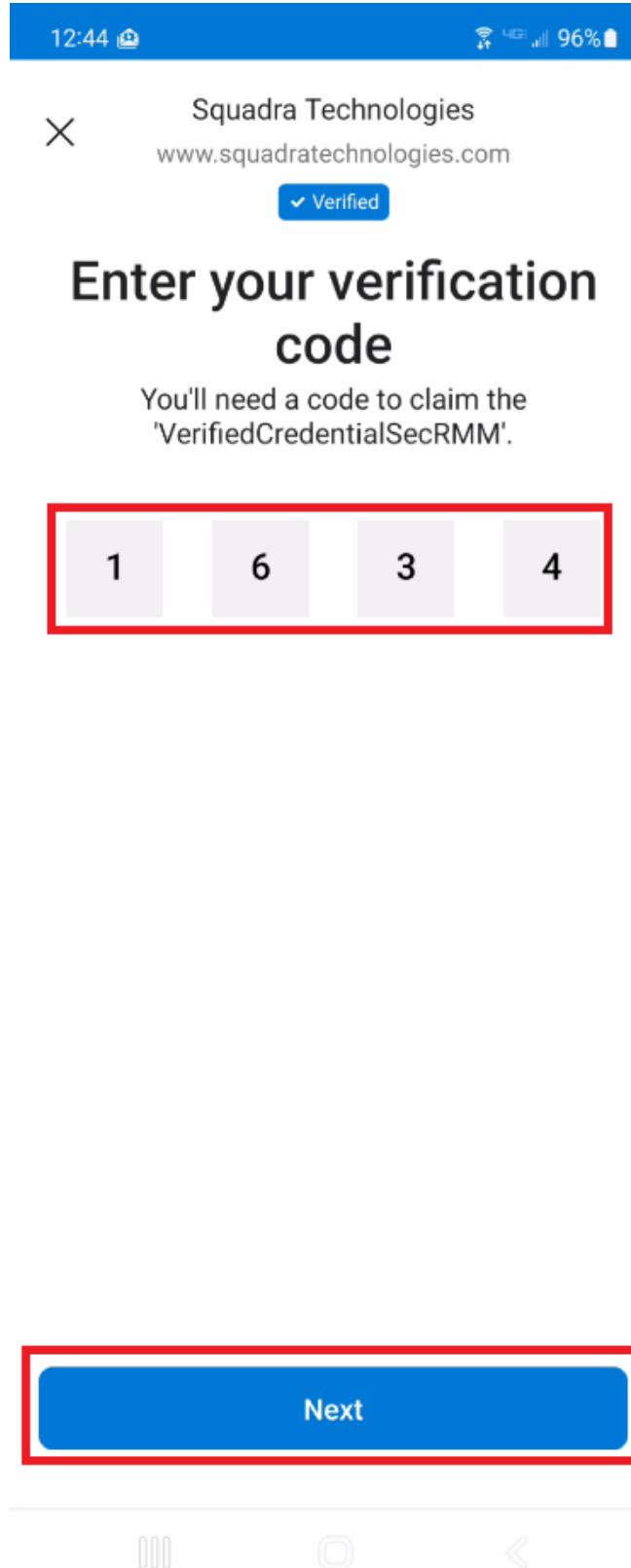
Now on the end-users phone, running Microsoft Authenticator, click the 'Verified IDs' at the bottom of the screen and then the 'Scan a QR code' as shown in the screenshot below.

secRMM Entra Verified ID Setup Guide



secRMM Entra Verified ID Setup Guide

Now enter the verification code and click the 'Next' button as shown in the screenshot below.



secRMM Entra Verified ID Setup Guide

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

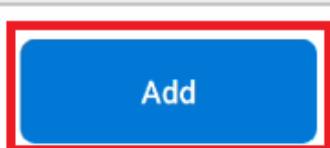


Squadra Technologies
[www.squadradechnologies.com](http://www.squadratechnologies.com)

✓ Verified

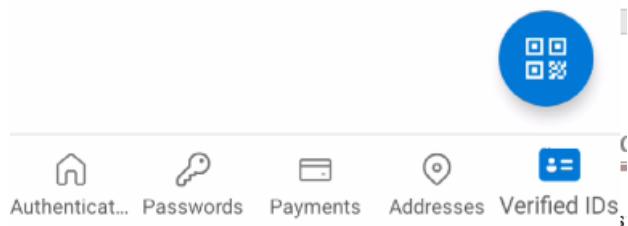
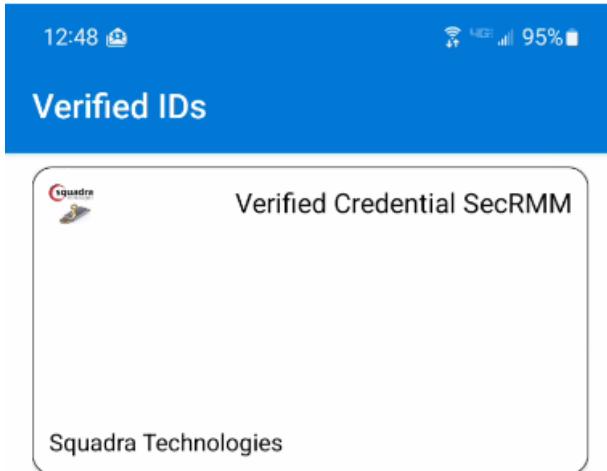
Add a Verified ID

Sign in with your account to get your card.



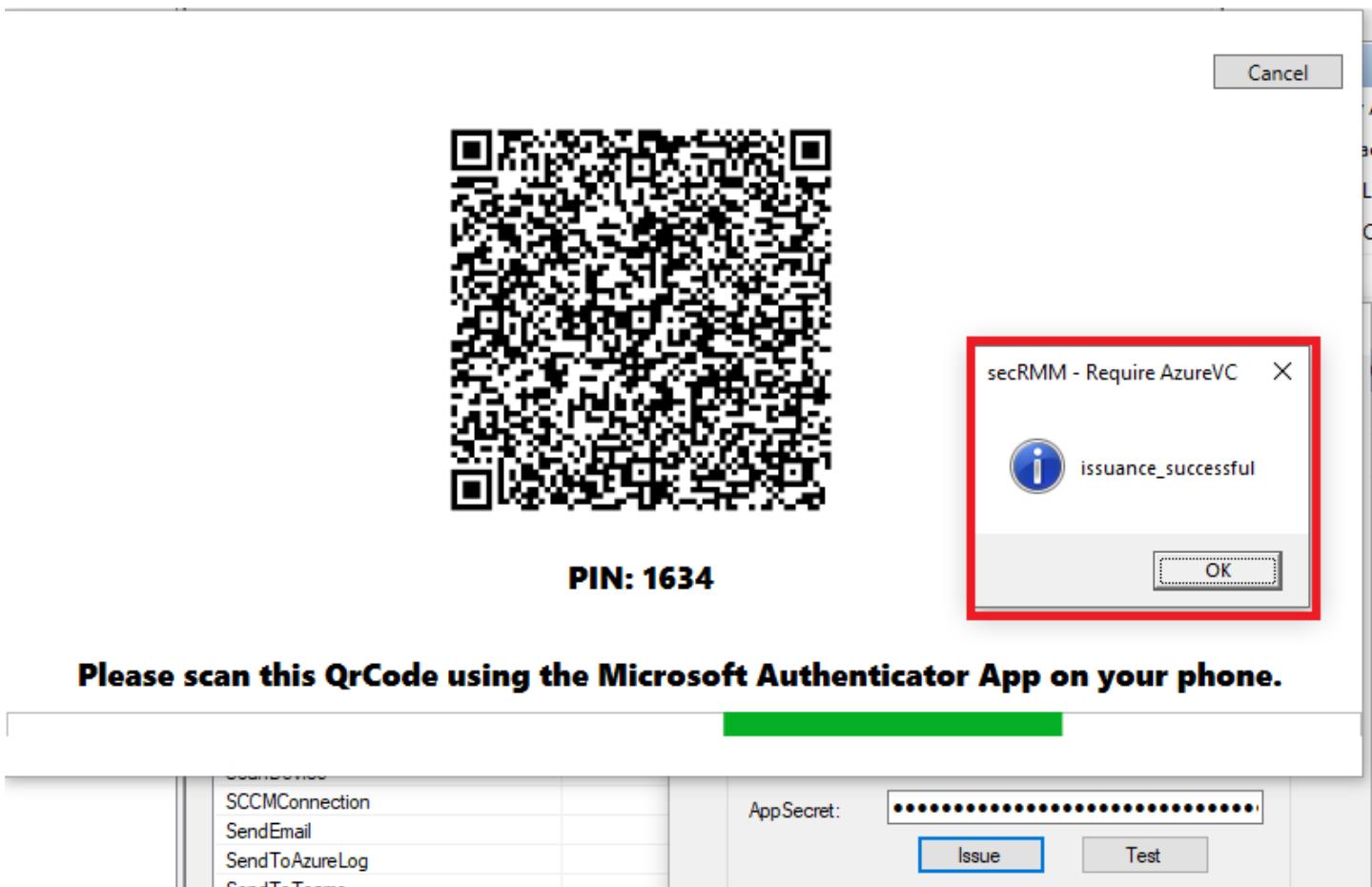
secRMM Entra Verified ID Setup Guide

The credential will now be listed in the list of 'Verified IDs' as shown in the screenshot below.



Back on the Windows computer where you started the issuance of the credential, there will be a message window indicating that the credential has been issued to Microsoft Authenticator as shown in the screenshot below.

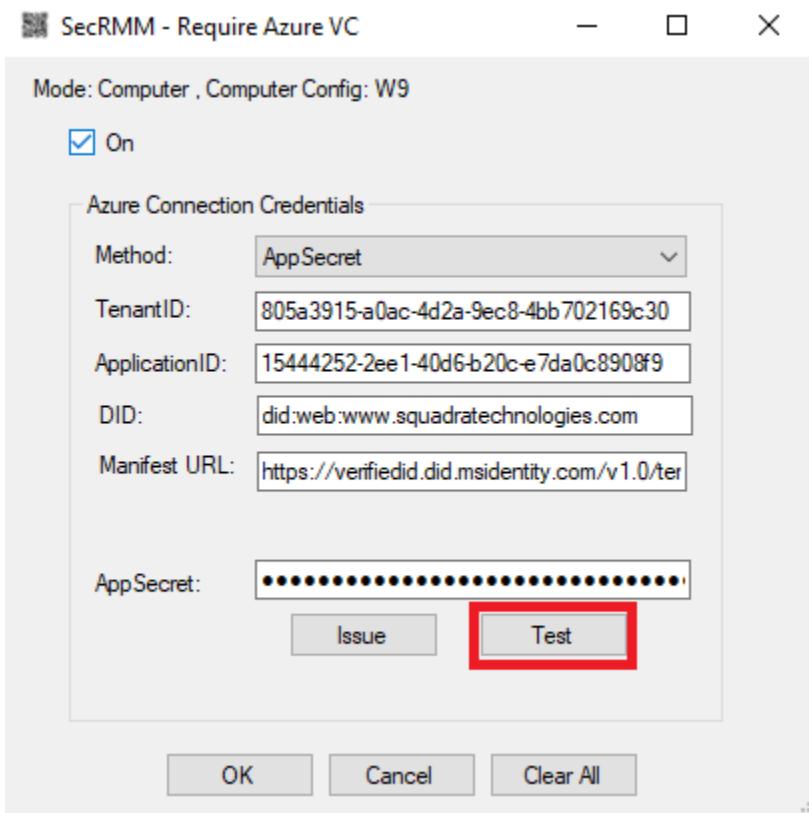
secRMM Entra Verified ID Setup Guide



Testing a certificate

Once you have issued a certificate to Microsoft Authenticator, you can test that the certificate is valid to your Azure VC service in your Azure tenant. To start the test, click the 'Test' button as shown in the screenshot below.

secRMM Entra Verified ID Setup Guide

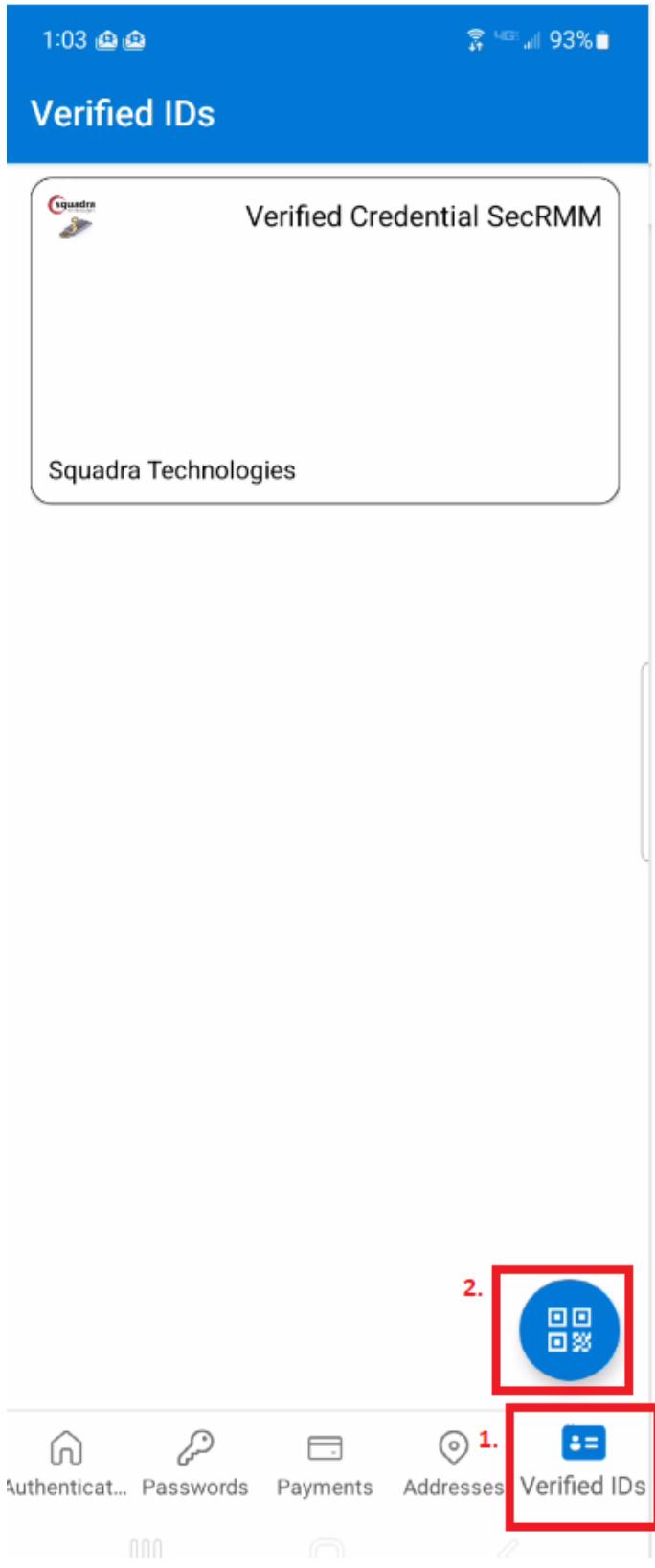


A QRCode will be displayed as shown in the screenshot below.



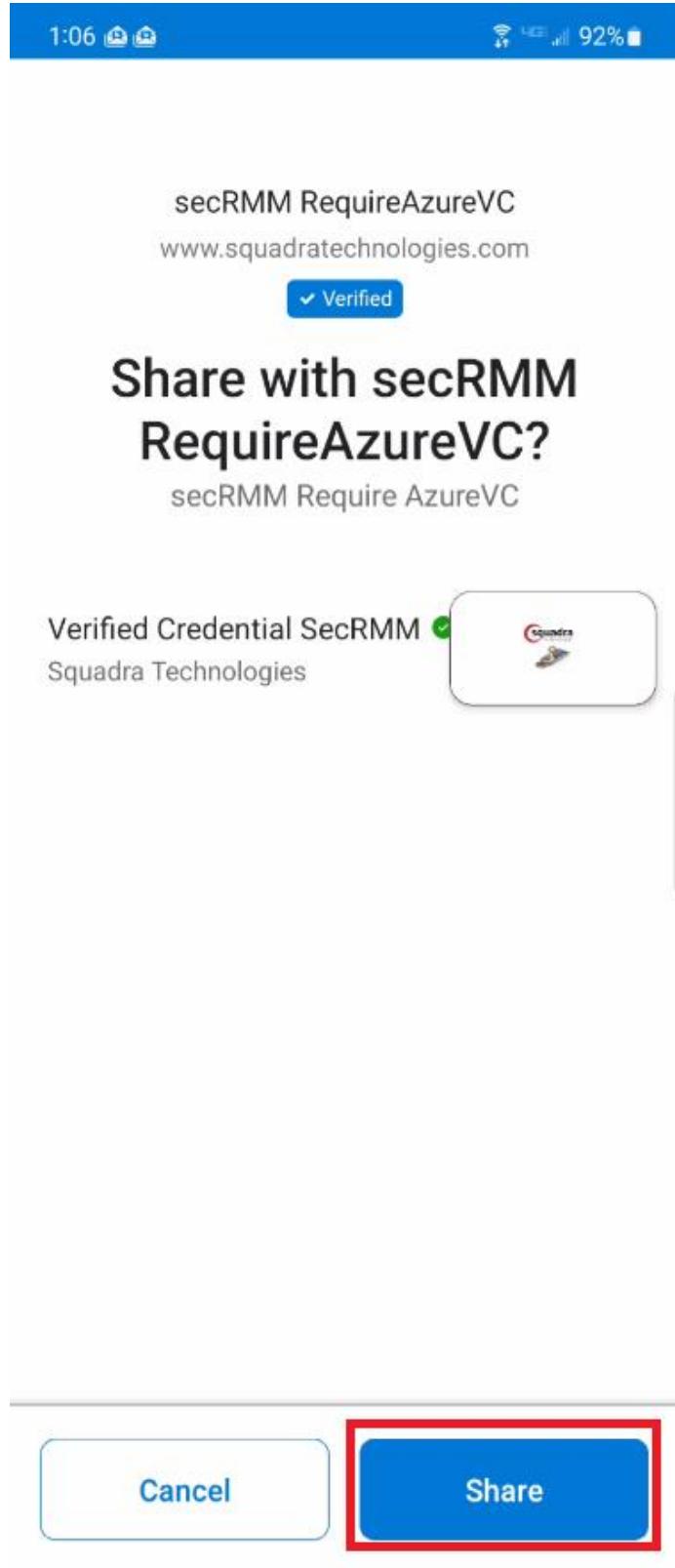
From Microsoft Authenticator on a mobile phone that has the secRMM credential issued, click the 'Verified IDs' button on the bottom of the app and then click the blue circle with the QRCode symbol as shown in the screenshot below.

secRMM Entra Verified ID Setup Guide



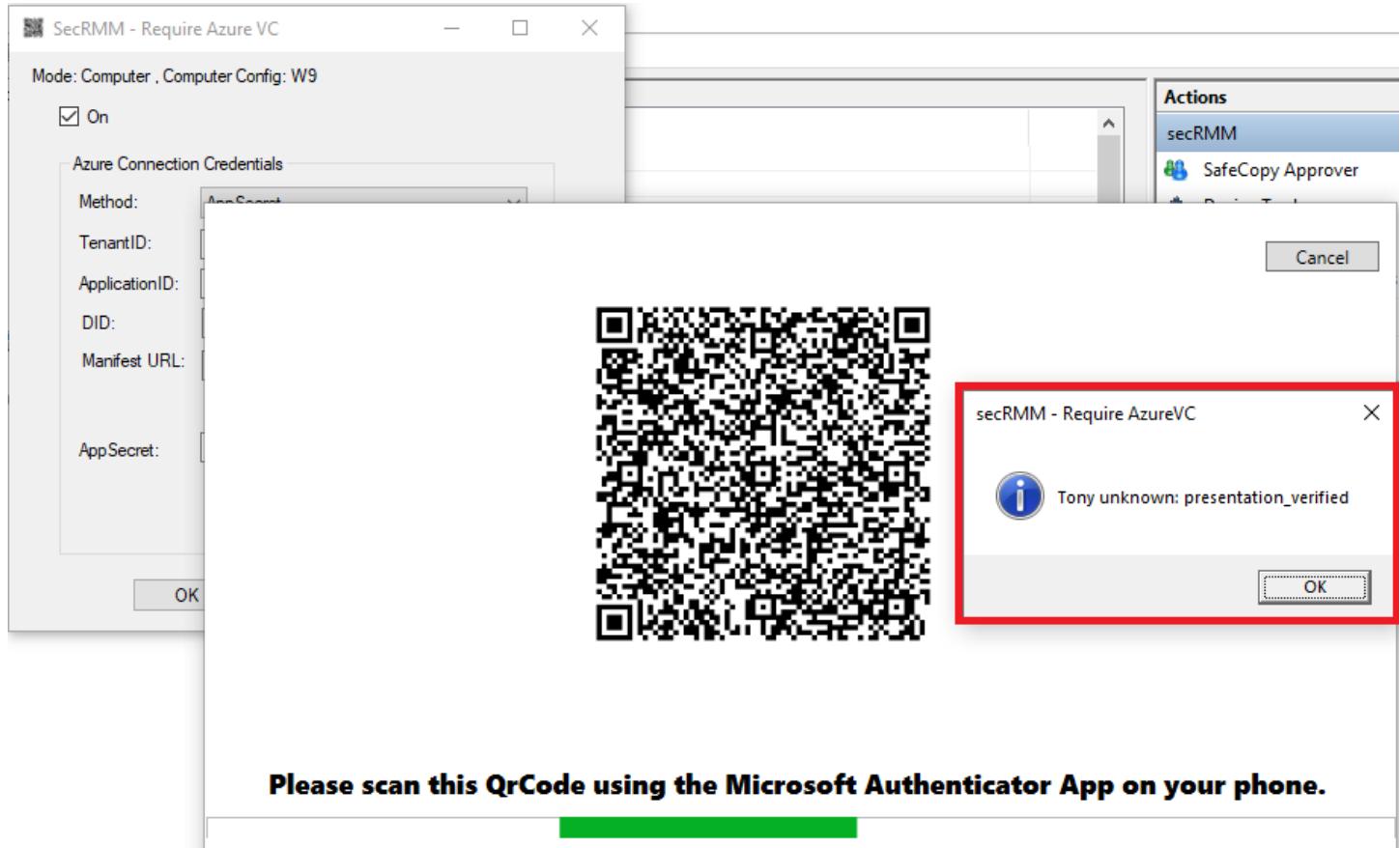
secRMM Entra Verified ID Setup Guide

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



secRMM Entra Verified ID Setup Guide

Back on the Windows computer where you started the test, there will be a message window indicating that the credential in Microsoft Authenticator is valid as shown in the screenshot below.



When a removable storage device mounts

This section shows what the end-user will experience when you configure the secRMM RequireAzureVC property.

When the end-user plugs in a removable storage device to the Windows computer running secRMM and with the RequireAzureVC property configured, they will see Windows Explorer pop-up briefly as it usually does when a new removable storage device mounts to the Windows operating system. Then, Windows Explorer will disappear and they will see the dialog in the screenshot below. This dialog gives them the option to continue (Yes) or cancel (No). In either case, a secRMM event is generated letting the security administrators know what choice they made.

secRMM Entra Verified ID Setup Guide

AzureVC Prompt - secRMM - using the Microsoft Authenticator App on your phone

AzureVC Prompt (E:)

A removable storage device has been detected.

The security policy for:

W9\Tony

requires that you scan a AzureVC within 3 minutes after clicking the Yes button.



To scan a AzureVC, please click '**Yes**'.

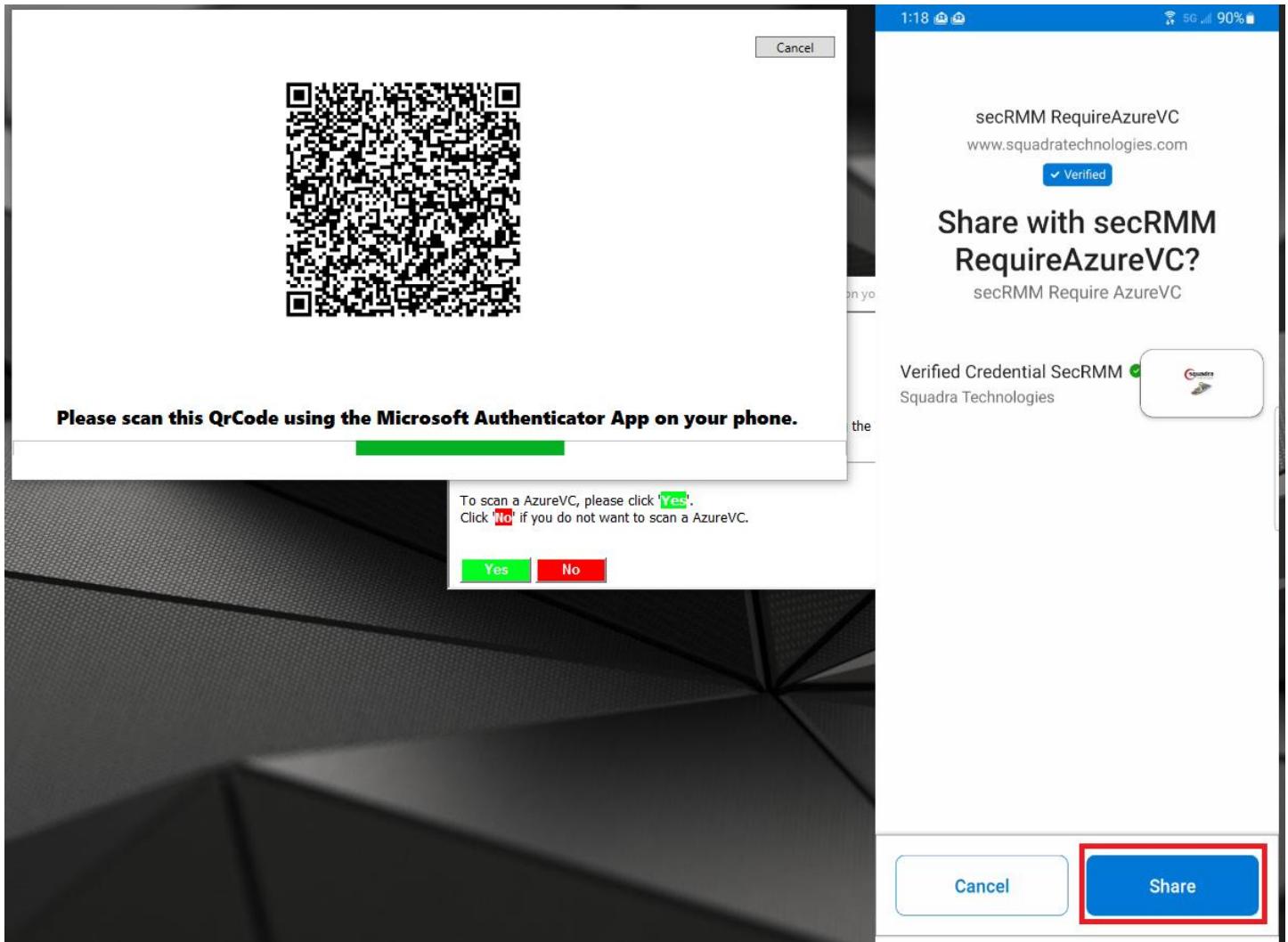
Click '**No**' if you do not want to scan a AzureVC.

Yes

No

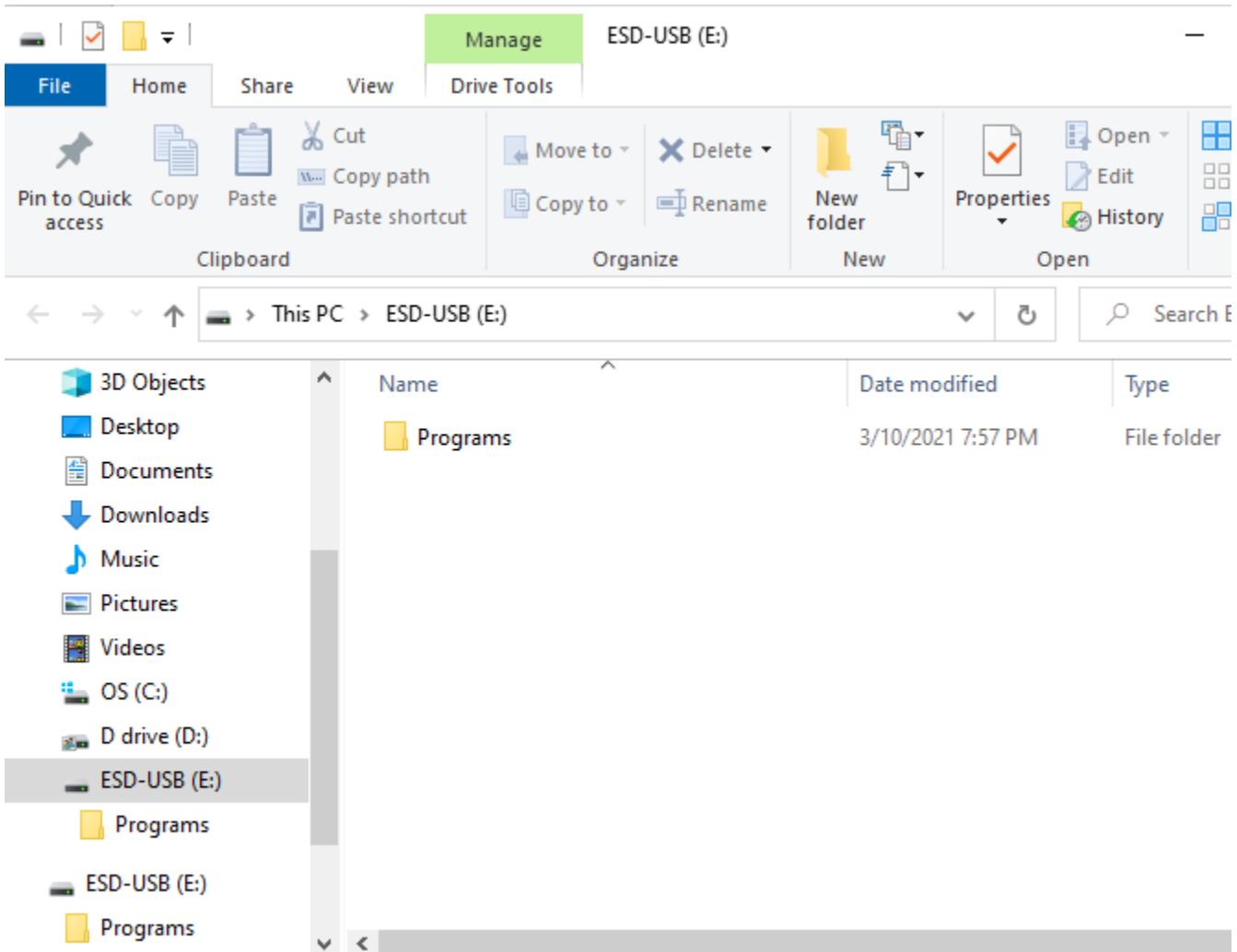
Once the end-user clicks the 'Yes' button, they are presented with a QrCode on the Windows screen that they will scan using the Microsoft Authenticator app on their phone. The Microsoft Authenticator app must already have the Azure VC secRMM credential loaded for them to continue. The screenshot below shows what they will see and that they need to click the 'Share' button on their phone.

secRMM Entra Verified ID Setup Guide



When this step happens, Windows Explorer will then appear on their Windows computer screen so they can use the removable storage device as shown in the screenshot below.

secRMM Entra Verified ID Setup Guide



In the Windows event log (the secRMM event log), the security administrators can view the fact that the end-user authenticated using Azure VC before they were able to access the removable storage device as shown in the screenshot below.

The screenshot shows the Windows Event Viewer. The left pane shows categories: Event Viewer (Local), Custom Views, Windows Logs, Applications and Services Logs. Under Applications and Services Logs, there are sub-categories: Dell, Hardware Events, Intel, IntelAudioServiceLog, Internet Explorer, Key Management Service, Microsoft, Microsoft Office Alerts, OneApp_IGCC, OpenSSH, PowerShellCore, and secRMM. The secRMM category is highlighted with a red box. The right pane shows a log entry for the secRMM application. The log details two information events: one at 9/5/2022 1:18:36 PM with Event ID 400 (AUDIT) and Task Category AUDIT, and another at 9/5/2022 1:17:27 PM with Event ID 300 (EXTERNAL) and Task Category EXTERNAL. Below the log table, a "General" tab is selected, showing the event details. The details pane contains the following text:
Removable Media Security Audit:
Drive: E:, Volume: \Device\HarddiskVolume17, Desc: Removable Disk Removable Media Win32_LogicalDisk USB2.0 HighSpeed Port#3Hub#1,
SerialNumber: 4C530001060623106322, Model: SanDisk Cruzer Glide USB Device, InternalID: USBSTOR
\DISK&VEN_SANDISK&PROD_CRUZER_GLIDE&REV_1.00\4C530001060623106322&0
Status: ONLINE
User(s): W9\Tony
Additional Azure VC Info: Tony unknown: presentation_verified

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/