Security Removable Media Manager

Prerequisites
Installation Guide

Version 9.9.13.0
(May 2019)

Protect your valuable data
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
Contents

INTRODUCTION .......................................................................................................................... 4

CHECKING FOR THE MICROSOFT PREREQUISITE SOFTWARE .................................................. 4

PREPARE THE SERVER ........................................................................................................... 5

DOWNLOAD THE SOFTWARE .................................................................................................. 7
  GET THE DEPLOYMENT SCRIPT .................................................................................... 10
  GET MICROSOFT INSTALLATION FILES ....................................................................... 11

DEPLOY USING SCCM ........................................................................................................... 12
  CREATE SCCM APPLICATION ....................................................................................... 12
  DISTRIBUTE THE secRMM MICROSOFT PREREQUISITE SOFTWARE CONTENT TO SCCM DISTRIBUTION POINTS .................................................................................. 37
  DEPLOY THE secRMM MICROSOFT PREREQUISITE SOFTWARE TO SCCM ENDPOINTS ................................................................. 42

DEPLOY USING AD GPO ......................................................................................................... 52
  CREATE AD GPO ........................................................................................................... 52
  LINK AD GPO ............................................................................................................... 60

VERIFY THE DEPLOYMENT .................................................................................................... 63

CONTACTING SQUADRA TECHNOLOGIES SUPPORT .......................................................... 63

ABOUT SQUADRA TECHNOLOGIES, LLC ........................................................................... 63
Introduction

NOTE: This document is 95% screenshots so don’t get discouraged with the number of pages! Hopefully you will find that a picture is really worth 1000 words.

Security Removable Media Manager (secRMM) relies on the Microsoft Visual C++ Redistributable dlls. secRMM is using the most current version of the Microsoft Visual C++ Redistributable dlls called “Microsoft Visual C++ 2015 Redistributable Update 3”. If you are keeping current with Microsoft updates, this should already be installed on your systems. If your systems do not already have “Microsoft Visual C++ 2015 Redistributable Update 3” installed, this installation guide will show you how to deploy it to your systems. To check if your systems already have this software, see the section below titled “Checking for the Microsoft Prerequisite software”. If this software is already on your systems, you do not need to perform the steps in this document.

You have the option of deploying the “Microsoft Visual C++ 2015 Redistributable Update 3” software using either System Center Configuration Manager (SCCM) or Active Directory Group Policy Objects (AD GPO). Both of these options are described in this installation guide. Since two out of the four steps are the same, we combined the instructions for deploying using SCCM or GPO into one document.

If you try to install secRMM without “Microsoft Visual C++ 2015 Redistributable Update 3” installed, you will receive an error as shown in the screenshot below.

Checking for the Microsoft Prerequisite software

To see if the “Microsoft Visual C++ 2015 Redistributable Update 3” dlls are already on your systems, you can check in the Windows\system32 directory for a dll named vcruntime140.dll.
If the “Microsoft Visual C++ 2015 Redistributable Update 3” dlls are not on your systems and you install secRMM anyways, secRMM will generate an error (“Provider load failure”) and will not be able to function properly.

**Prepare the server**

To deploy the “Microsoft Visual C++ 2015 Redistributable Update 3” software, we will create a network share on a server in your domain that all the computers in your domain can access.

If you started out by following the secRMM installation documentation for SCCM or GPO, you will probably have already done much of this section.

*Please be sure though that you allow Read and Write access to the subdirectory named secRMMPrerequisite.* This is because the script will write log files back into the secRMMPrerequisite subdirectory so you are able to analyze the deployment from a central location.
As you can see from the screenshot above, we used a server (named sccmr2) and created a secRMM directory under the directory named _SCCMAppDeployments. We will share the directory C:\_SCCMAppDeployments\secRMM\secRMMPrerequisite so the client computers in your domain can read and write to it. In the screenshot below, you can see we create the share on the SCCMR2 server for C:\_SCCMAppDeployments\secRMM\secRMMPrerequisite. The share is named secRMMPrerequisite so other computers can access this share at \SCCMR2\secRMMPrerequisite.

Note the share permission below. We allow the “Domain Computers” read and write access to this share.
Download the software

Now that the directory structure has been created, we will download the files that need to go into the secRMMPrerequisite subdirectory.

Deploying the “Microsoft Visual C++ 2015 Redistributable Update 3” software is performed using a Windows CMD script named InstallMSVSRuntime.cmd. You will download this script from the Squadra Technologies web site.

Go to http://www.squadratechnologies.com and follow the screen shot below to get to the secRMM download page.
Please specify your information to download secRMM.

Once you click the submit button below, you will be redirected to the download page.

First Name: Bill
Last Name: Gates
E-mail: Bill@microsoft.com
Company:
Phone:
Country:

Submit
On the “Additional optional downloads” page, when you click the “secRMMDeployment.zip” link, it will download the secRMMDeployment.zip file to your local computer.
Get the deployment script

Extract (unzip) the secRMMDeployment.zip that you just downloaded in the section above. Copy the InstallMSVSRuntime.cmd file that is in the “Prerequisites” subdirectory from the extracted zip file into the secRMMPrerequisite share (in our example, this is on the sccmr2 server under the directory named C:\_SCCMAppDeployments\secRMM\secRMMPrerequisite).
Get Microsoft installation files

Go to the Microsoft download center at: https://www.microsoft.com/en-us/download/details.aspx?id=53587

Click the download button.

Select to download both the vc_redist.x64.exe and vc_redist.x86.exe files

The downloaded files will be copied to your local drive.
Copy both of these files (vc_redist.x64.exe and vc_redist.x86.exe) into the secRMMPrerequisite share (in our example, this is on the sccmr2 server under the directory named C:\_SCCMAppDeployments\secRMM\secRMMPrerequisite).

At this point, the server has the 3 files (InstallMSVSRuntime.cmd, vc_redist.x64.exe and vc_redist.x86.exe) we need to deploy the “Microsoft Visual C++ 2015 Redistributable Update 3” software to the computers in your environment.

**Deploy using SCCM**

**Create SCCM Application**

Create a SCCM Application to deploy the Microsoft Prerequisite software to the computers in your environment. Press the “Create Application” button on the SCCM Console ribbon bar when you have the Software Library->Application Management->Applications->secRMM clicked.

The “Create Application Wizard” will display. Select the “Manually specify the application installation” and click the Next button.
There are no items to show in this view.
Create Deployment Type Wizard

Specify settings for this deployment type

Deployment types include information about the installation method and source files for this application.

Type: 

- Script Installer

- Automatically identify information about the deployment type from installation files

- Manually specify the deployment type information

Location: 

Example: \Server\Share\File

< Previous  Next >  Summary  Cancel
Specify information about the content to be delivered to target devices

Specify the location of the deployment type’s content and other settings that control how content is delivered to target devices. All the contents in the path specified will be delivered.

- **Content location:** \\sccm2\SecRMMPrerequisite
- **Persist content in the client cache:**
- **Allow clients to share content with other clients on the same subnet:**

This option allows clients that use Windows BranchCache to download content from on-premises distribution points. Content downloads from cloud-based distribution points can always be shared by clients that use Windows BranchCache.

- **Specify the command used to install this content:**
  - **Installation program:** InstallMSYSRuntime.cmd
  - **Installation start in:**

Configuration Manager can remove installations of this content if an uninstall program is specified below.

- **Uninstall program:**
- **Uninstall start in:**

- **Run installation and uninstall program as 32-bit process on 64-bit clients:**
The “Detection Rule” dialog (screenshot directly below) tells SCCM how it should know that this SCCM Application has been run on the SCCM client computer. Notice we have clicked the radio button with the associated text of “The file system setting must satisfy the following rule to indicate the presence of this application”. We need to get the “Value” to specify. To do this, we will use the Microsoft files we downloaded from the Microsoft site. It does not matter whether you use vc_redist.x64.exe or vc_redist.x86.exe since they will contain the same value. Right mouse click on vc_redist.x64.exe or vc_redist.x86.exe and on the menu, select Properties. On the Properties dialog, click the Details tab. The value we want to use in the SCCM “Detection Rule” dialog is the “File version” value.
Right click on the files and select Open. From there, you can choose to Run as administrator, Troubleshoot compatibility, Pin to Start, 7-Zip, Scan with Windows Defender, or Share. You can also give access to, pin to taskbar, or restore previous versions. If you need to send to, cut, copy, create shortcut, delete, or rename, you can do so. However, if you want to modify the properties of the file, you will need to go to Properties.
### vc_redist.x64.exe Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Microsoft Visual C++ 2015 Redistributable (x64) Application</td>
</tr>
<tr>
<td>File description</td>
<td>Microsoft Visual C++ 2015 Redistributable (x64) Application</td>
</tr>
<tr>
<td>Type</td>
<td>Application</td>
</tr>
<tr>
<td>File version</td>
<td>14.0.24212.0</td>
</tr>
<tr>
<td>Product name</td>
<td>Microsoft Visual C++ 2015 Redistributable (x64) Application</td>
</tr>
<tr>
<td>Product version</td>
<td>14.0.24212.0</td>
</tr>
<tr>
<td>Copyright</td>
<td>Copyright (c) Microsoft Corporation. All rights reserved</td>
</tr>
<tr>
<td>Size</td>
<td>14.5 MB</td>
</tr>
<tr>
<td>Date modified</td>
<td>1/15/2018 11:00 AM</td>
</tr>
<tr>
<td>Language</td>
<td>English (United States)</td>
</tr>
<tr>
<td>Original filename</td>
<td>VC_redist.x64.exe</td>
</tr>
</tbody>
</table>

Remove Properties and Personal Information
Detection Rule

Create a rule that indicates the presence of this application.

Setting Type: File System

Specify the file or folder to detect this application.

Type: File
Path: %WINDIR%\System32
File or folder name: vcruntime140.dll

- Uncheck 2.

The file system setting must satisfy the following rule to indicate the presence of this application

- Property: Version
- Operator: Greater than or equal to
- Value: 14.0.24212.0

- OK

4. Cancel
There are no items to show in this view.
Create Deployment Type Wizard

Confirm the settings for this deployment type

Details:
- General Information:
  - Name: seCRM Microsoft prerequisite software
  - Technology: Script Installer
  - Administrator comments:
  - Language:
- Content:
  - Content location: \access\20secRMMPrerequisite
  - Persist in client cache: No
  - Enabled peer-to-peer content distribution: Yes
  - Installation program: "InstallMSVSRuntime.cmd"
  - Installation start-in:
- Detection Method:
- User Experience:
  - Installation behavior: Install for system
  - Login requirement: Whether or not a user is logged on
  - Installation priority: Normal
  - Allow users to interact with this program: No
  - Maximum allowed run time (minutes): 120
  - Estimated install time (minutes): 5
- Requirements:
- Dependencies:

To change these settings, click Previous. To apply the settings, click Next.
The Create Deployment Type Wizard completed successfully

Details:

- **Success: General Information**:
  - Name: secRMM Microsoft prerequisite software
  - Technology: Script Installer
  - Administrator comments:
  - Languages:

- **Success: Content**:
  - Content location: \Install\prerequisites\secRMM Prerequisite
  - Persist in client cache: No
  - Enabled peer-to-peer content distribution: Yes
  - Installation program: "InstallMSVSRuntime.cmd"
  - Installation start in:

- **Success: Detection Method**:

- **Success: User Experience**:
  - Installation behavior: Install for system
  - Login requirement: Whether or not a user is logged on
  - Installation priority: Normal
  - Allow users to interact with this program: No
  - Minimum allowed run time (minutes): 120
  - Estimated install time (minutes): 5

- **Success: Requirements**:

To exit the wizard, click Close.
Create Application Wizard

Deployment Types

Configure deployment types and the priority in which they will be applied for this application.

Deployment types include information about the installation method and the source files for this application.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Name</th>
<th>Type</th>
<th>Languages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>secRMM Microsoft prerequisite software</td>
<td>Script</td>
<td></td>
</tr>
</tbody>
</table>

Add ..  Edit ..  Copy  Delete

Next >  Previous  Summary  Cancel
Distribute the secRMM Microsoft prerequisite software content to SCCM Distribution Points

Distribute the content to your SCCM Distribution Points. The data in the screenshots below will be much different than your environment but the screenshots will give you a general idea of how to distribute the secRMM Microsoft prerequisite software.
The image shows a screen from the Distribute Content Wizard with a summary of the settings. The wizard displays the following details:

- **Content (1):** secRMM Microsoft prerequisite software
- **Dependencies (1):** secRMM Microsoft prerequisite software
- **Collections (0):**
- **Distribution point groups (3):**
- **Distribution points (1):** SCCMF2.CONTOSO.COM

The summary states: "To change these settings, click Previous. To apply the settings, click Next."
Deploy the secRMM Microsoft prerequisite software to SCCM endpoints

We can now deploy the secRMM Microsoft prerequisite software using SCCM to all SCCM endpoint computers.
Specify user experience setting for the deployment.

User notifications: [Hide in Software Center and all notifications]

When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:

- Software installation
- System restart (if required to complete the installation)

Write filter handling for Windows Embedded devices:

- Commit changes at deadline or during a maintenance window (requires restarts)

If this option is not selected, content will be applied on the overlay and committed later.
Deploy Software Wizard

Summary

Confirm the settings for this new deployment

Details:

General
- Software: secRMM Microsoft prerequisite software
- Collection: All Systems (Member Count: 15)
- Use default distribution point groups associated to this collection: Enabled
- Automatically distribute content for dependencies: Enabled

Deployment Settings
- Action: Install
- Purpose: Required
- Pre-deploy software to the user's primary device: Disabled
- Send wake-up packets: Enabled
- Allow clients to use a metered Internet connection to download content: Disabled

Application Settings (retrieved from application in software library)
- Application Name: secRMM Microsoft prerequisite software
- Application Version:
- Application Deployment Types: Script Installer

Scheduling
- Time based on: UTC
- Available Time: As soon as possible
- Deadline Time: Disabled
- Delayed enforcement on deployment: Disabled

User Experience
- User notifications: Hide in Software Center and all notifications
- Ignore Maintenance Windows: Enabled
- System restart (if required to complete the installation): Enabled
- Correct changes at deadline or during a maintenance window (requires restart): Enabled

To change these settings, click Previous. To apply the settings, click Next.
Deploy using AD GPO

Create AD GPO

We will use a Windows computer startup script from AD GPO to run the deployment script.
Right click `secRMM Microsoft prerequisite software` and select `Edit...`
Browse

Organize
Name
Type
Size

InstallMSVSRuntime
Windows Command Script
6 KB

vc_redist.x64
Application
14,925 KB

vc_redist.x86
Application
14,120 KB

File name: InstallMSVSRuntime

Add a Script

Script Name:
\secrm\secRMMPrerequisite\InstallMSVSRuntime. cr

Script Parameters:

OK
Link AD GPO

The final step is to link the GPO to an OU in your organization that contains the Windows computers you want to deploy the software to.
Right click on CONTOSO.com and select "Link an Existing GPO."
Select GPO

Look in this domain:
CONTOSO.com

Group Policy objects:
- secRMM Computer Rule 1
- secRMM Event Log Security Setting
- secRMM Installation v6.0.3.0
- secRMM Microsoft prerequisite software
- secRMM User Rule 1
- secRMMCentral_SCCM
- secRMMCentral_SCOM
- TurnOnLoopbackMerge
- User_secRMM_1
- User_secRMM_LoopbackMerge

OK

Group Policy Management

Group Policy Management
- Forest CONTOSO.com
  - Domains
    - CONTOSO.com
      - BitLockedDefaultFolderForRecoveryPassword
      - Default Domain Policy
      - RunAsDifferentUserOnStartMenu
      - secRMM Microsoft prerequisite software
      - secRMMCentral_SCCM
      - User_secRMM_1
  - Domain Controllers
  - TestComputerBranch
  - TestUserBranch
  - Group Policy Objects
  - WMI Filters
  - Starter GPOs
- Sites
  - Group Policy Modeling
  - Group Policy Results

secRMM Microsoft prerequisite software

Links
- Display links in this location: CONTOSO.com
- The following sites, domains, and GPOs are linked to this GPO:
  - Location: CONTOSO.com
  - Enforced: No
  - Link Enabled: Yes
  - Path: CONTOSO.com

Security Filtering
- The settings in this GPO can only apply to the following groups, users, and computers:
  - Name: Authenticated Users
Verify the deployment

Whether you used SCCM or AD GPO, you will see an event id of 11707 in the Application event log as shown below.

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. The version of SCCM you have installed.
4. Whether the Windows Operating System is 32bit or 64bit.
5. 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