How to guide:

Setup RMSSA for Security Manager

The intention of this guide is to give instructions on how to adjust the settings and configurations of RMS Security Patch Manager in order to use the RayManageSoft Security Analyzer (RMSSA) scan technology. RMSSA has to be used to deploy security patches to managed devices running Windows 8 or Windows Server 2012.

Please follow the step-by-step description to make sure all parts of the Security Manager environment are prepared correctly.

Prerequisite software

RMSSA is part of the Security Patch Management extension to RayManageSoft 10.x. Therefore Security Patch Manager has to be installed on your RMS 10.x administration server to enable the usage of RMSSA.

Managed devices that are about to run RMSSA have to be equipped with the following software and configuration:

- .NET Framework 4.0 must be installed
- Windows Update Agent (WUA) must be installed
- Windows update service (`wuauserv.exe`) must be running

Download the Security Analyzer package into the software library

RMSSA for Managed Devices is wrapped into a software package Raynet provides free of charge. You can download it from the RayManageSoft Third Party Prerequisite servers.

To do so:

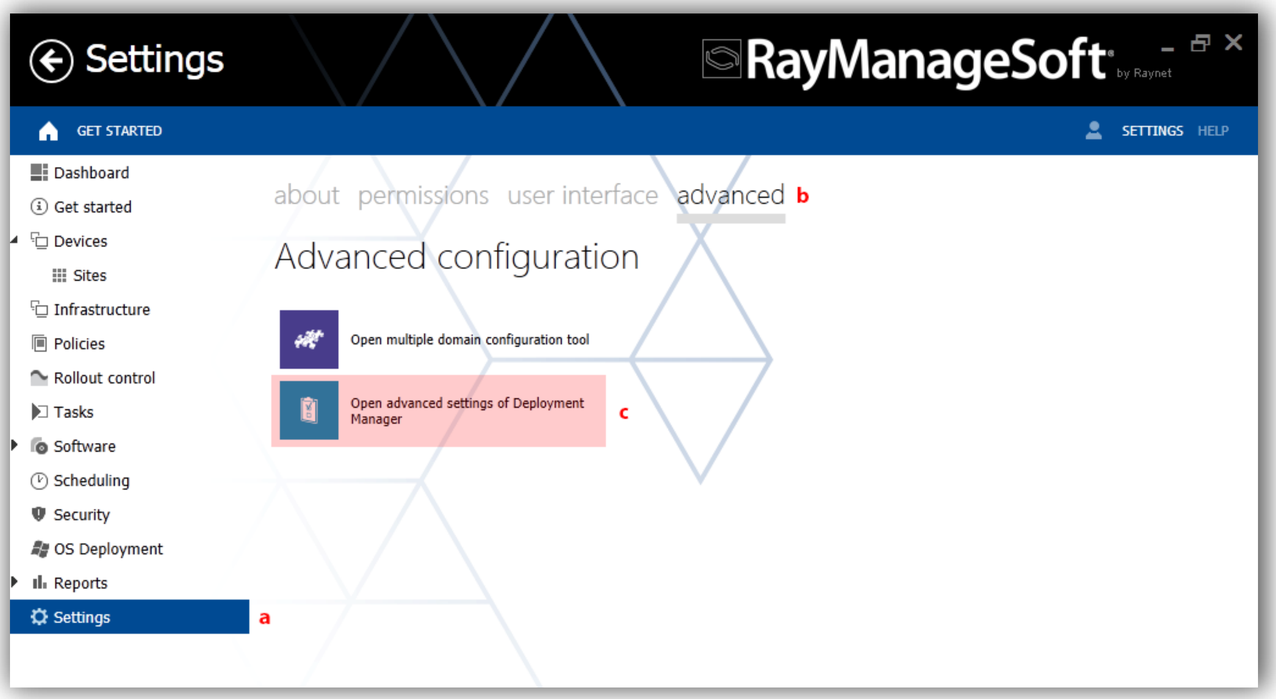
1) Launch your **Deployment Manager Administration Console**.

2) Open the **Deployment Manager Configuration**:

   a. Select the **Settings** node from the console tree

b. Call the **advanced** tab

c. Use the **Open advanced settings of Deployment Manager** button



The **Deployment Manager Configuration Console** launches.

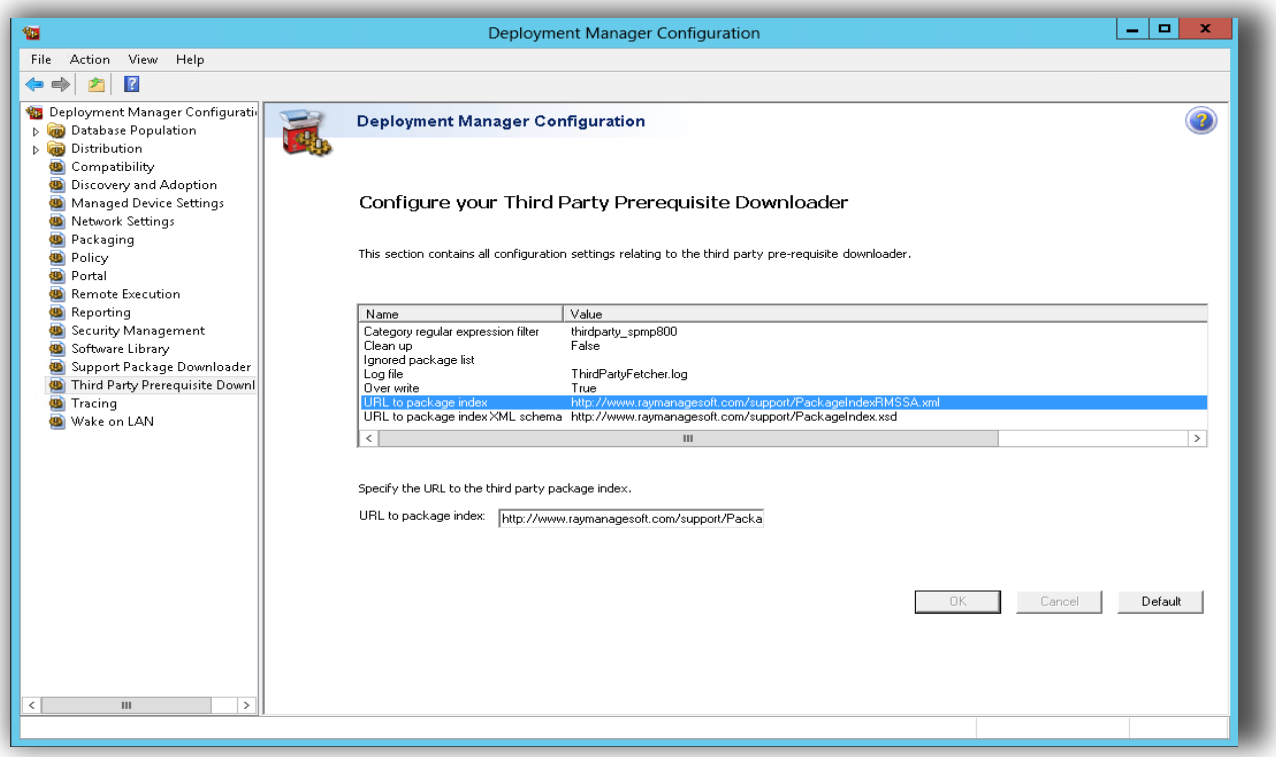
3) Select **Third Party Prerequisite Downloader** from the console tree.

4) From the details pane on the right-hand side, select **URL to package index.**

5) Set following as its value (as shown in the image below):
`http://raymanagesoft.com/support/PackageIndexRMSSA.xml`

6) Click **OK** to save the new URL.

7) You can close the **Deployment Manager Configuration Console** now.



Configure your Third Party Prerequisite Downloader

This section contains all configuration settings relating to the third party pre-requisite downloader.

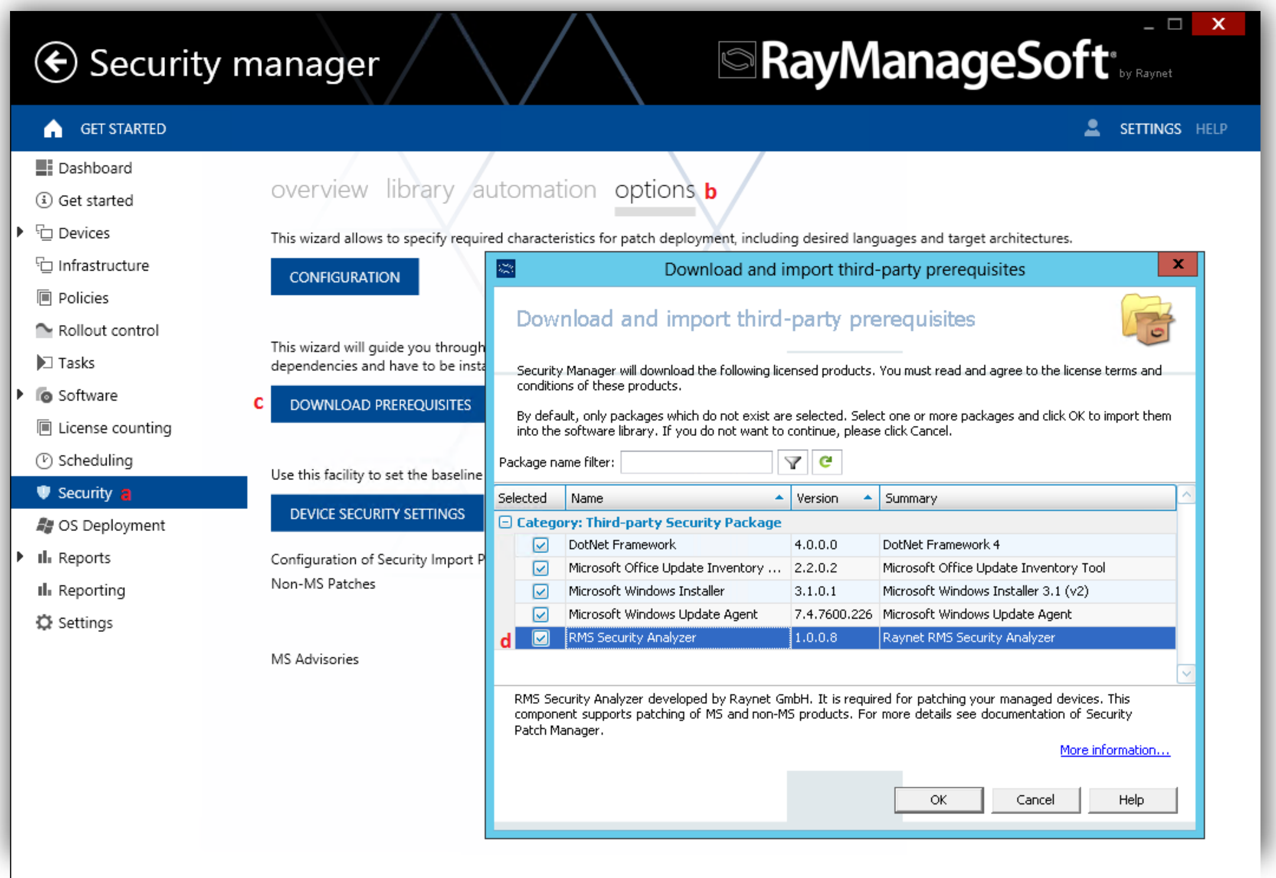
Name	Value
Category regular expression filter	thirdparty_spmp800
Clean up	False
Ignored package list	
Log file	ThirdPartyFetcher.log
Over write	True
URL to package index	http://www.raymanagesoft.com/support/PackageIndexRMSSA.xml
URL to package index XML schema	http://www.raymanagesoft.com/support/PackageIndex.xsd

Specify the URL to the third party package index.

URL to package index: http://www.raymanagesoft.com/support/Packa

8) Return to the Deployment Manager Administration Console to download the RMSSA package

a. Select the **Security** node
b. Call the **options** tab
c. Use the **DOWNLOAD PREREQUISITES** button
d. Within the Download and import third-party prerequisites window, RMS Security Analyzer along with the other prerequisite packages are available.
e. Activate the checkbox left of the package name
f. Click **OK** to save your changes.



This wizard allows to specify required characteristics for patch deployment, including desired languages and target architectures.

This wizard will guide you through dependencies and have to be insta

Use this facility to set the baseline

Configuration of Security Import P

Download and import third-party prerequisites

Download and import third-party prerequisites

Security Manager will download the following licensed products. You must read and agree to the license terms and conditions of these products.

By default, only packages which do not exist are selected. Select one or more packages and click OK to import them into the software library. If you do not want to continue, please click Cancel.

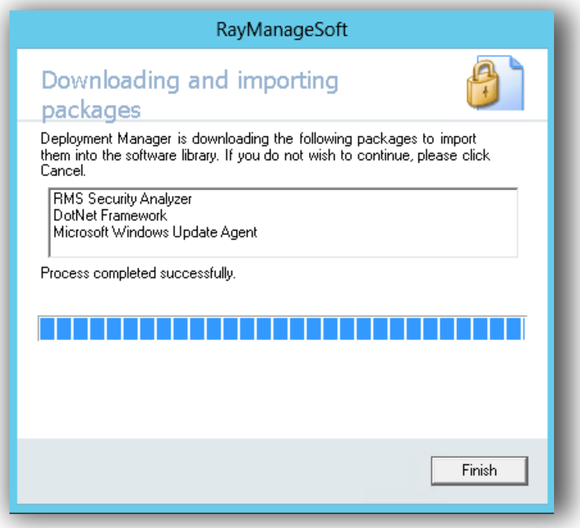
Package name filter:

Selected	Name	Version	Summary
⊟ Category: Third-party Security Package			
☑	DotNet Framework	4.0.0.0	DotNet Framework 4
☑	Microsoft Office Update Inventory ...	2.2.0.2	Microsoft Office Update Inventory Tool
☑	Microsoft Windows Installer	3.1.0.1	Microsoft Windows Installer 3.1 (v2)
☑	Microsoft Windows Update Agent	7.4.7600.226	Microsoft Windows Update Agent
d ☑	RMS Security Analyzer	1.0.0.8	Raynet RMS Security Analyzer

RMS Security Analyzer developed by Raynet GmbH. It is required for patching your managed devices. This component supports patching of MS and non-MS products. For more details see documentation of Security Patch Manager.

More information...

9) Deployment Manager immediately starts to download and import the package.



RayManageSoft

Downloading and importing packages

Deployment Manager is downloading the following packages to import them into the software library. If you do not wish to continue, please click Cancel.

RMS Security Analyzer
DotNet Framework
Microsoft Windows Update Agent

Process completed successfully.

10) Once the download and import packages wizard is completed, click **Finish**.

The RMS Security Analyzer package is available within the software library.

Distribute RMS Security Analyzer to managed devices

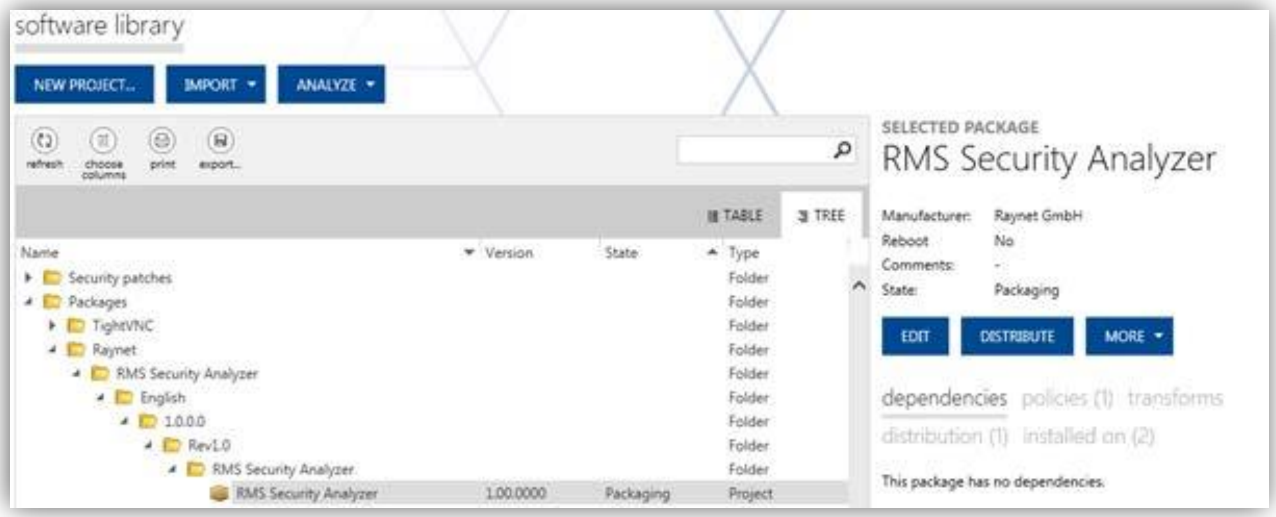
RMS Security Analyzer is executed on managed devices. You can deploy the package using the Deployment Manager distribution hierarchy.

To do so:

1. Select the **Software** node from the Deployment Manager Administration Console.

2. Within the **software library**, navigate through the package tree as shown in the screenshot below.

3. Select the **Security Analyzer** project.



Name	Version	State	Type
Security patches			Folder
Packages			Folder
TightVNC			Folder
Raynet			Folder
RMS Security Analyzer			Folder
English			Folder
1.0.0.0			Folder
Rev1.0			Folder
RMS Security Analyzer			Folder
RMS Security Analyzer	1.00.0000	Packaging	Project

SELECTED PACKAGE
RMS Security Analyzer

Manufacturer: Raynet GmbH
Reboot: No
Comments: -
State: Packaging

This package has no dependencies.

4. Use the **MORE** button within the side-bar on the right, and select **Pack** from the options menu to pack the project files.

5. Use the **DISTRIBUTE** button within the side-bar on the right.

The **Package Distribution Wizard** is displayed.

Follow the steps of the wizard and target all distribution locations and groups that host managed devices you want to run RMSSA on.

6. Once the Package Distribution Wizard is completed, use the **MORE** button within the side-bar on the right again, and select **Add to policy** from the options menu.

7. Follow the steps of the wizard.
   Add the RMS Security Analyzer to the schedule you use for security patch distribution. Make sure that it placed on the **first position** within all packages and security patches that have been added to the policy.

8. Return to the **software library**, and navigate through the Security patches branch to access the project files for **Security Patch Settings for Microsoft Windows**. This settings package is required to deploy the `Wsusscan.cab` to the managed devices.

   Repeat steps 4 – 7 to add the security settings package to policy.

   The settings package should be placed on the **second position** within the packages added to the security patch deployment policy.

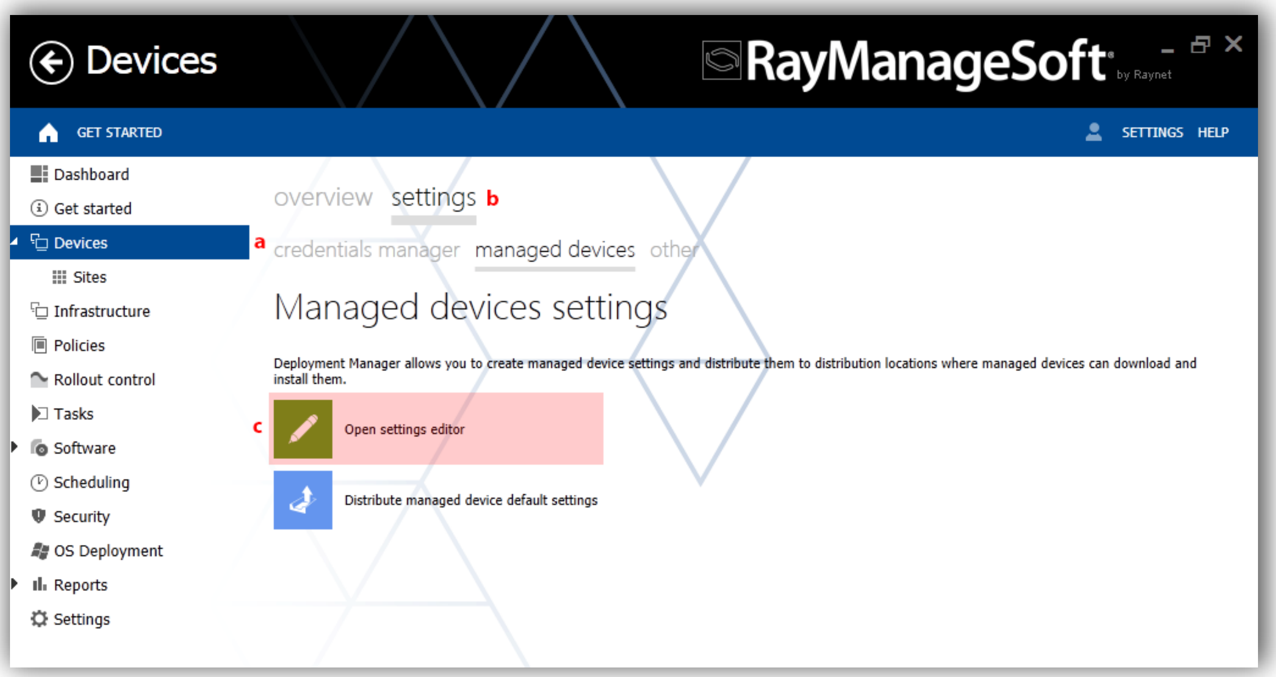
Update Managed Device settings

You have to advise managed devices to use RMSSA instead of the default MBSA scan tool. This is accomplished by updating the standard configuration Deployment Manager defines within managed device settings packages.

To do so:

1) Open the **Managed Device Settings Console**:

   a. Select the **Devices** node from the console tree
   b. Call the **settings** tab
   c. Use the **Open settings editor** button



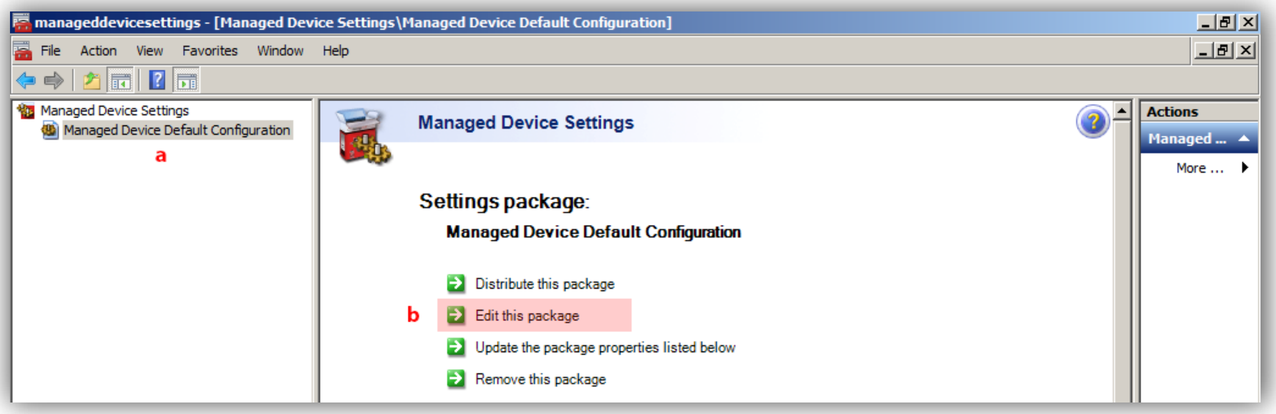
Managed devices settings

Deployment Manager allows you to create managed device settings and distribute them to distribution locations where managed devices can download and install them.

The **Managed Device Settings Console** is displayed.

2) You have to edit the default settings package:

   a. From the console tree on the left, select **Managed Device Default Configuration**
   b. Within the details pane, click **Edit this package**

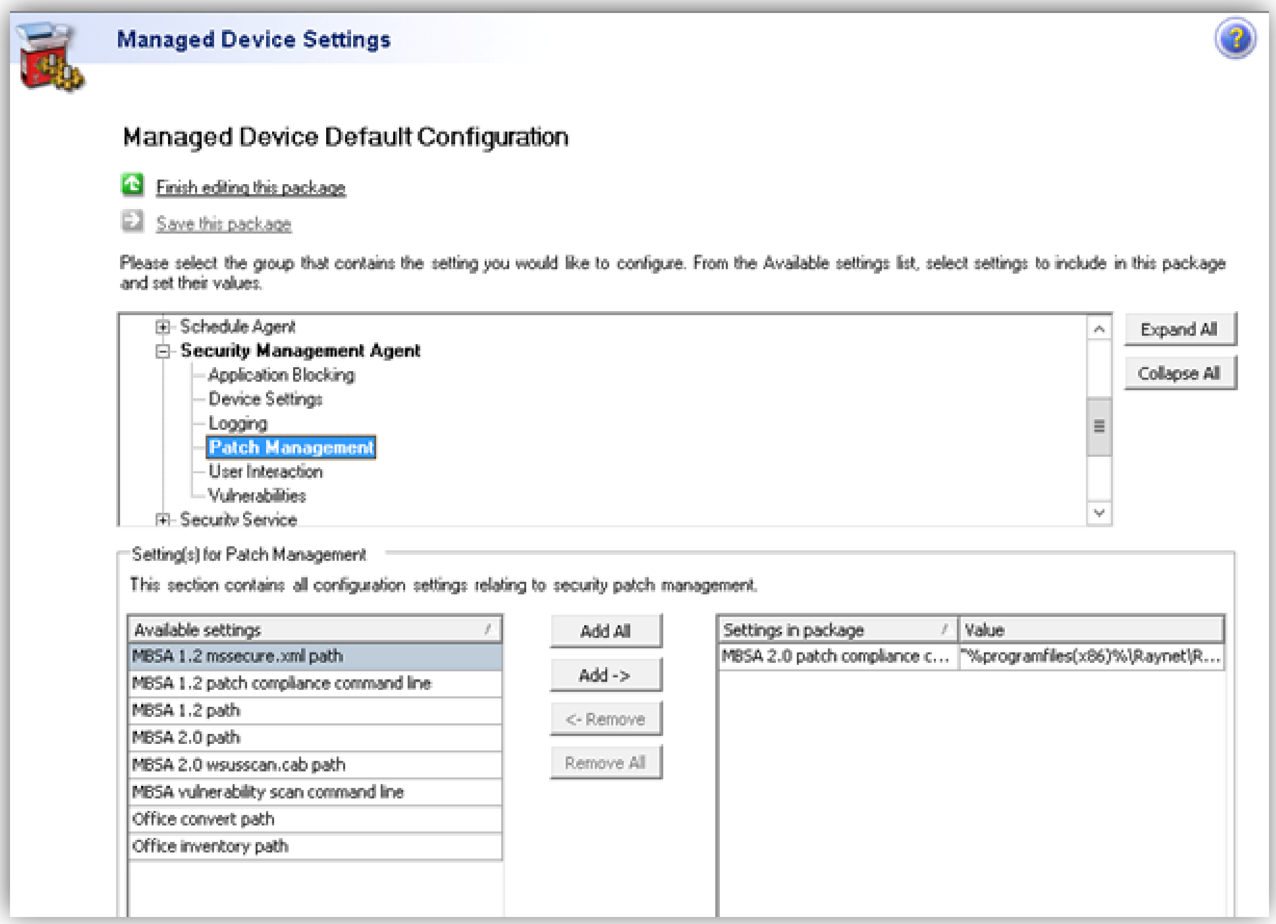


Settings package:
Managed Device Default Configuration

The list of available settings is displayed within the details pane.

3) Scroll down until you reach the **Security Management Agent** node, and expand the it.

4) Click on the **Patch Management** item.



Managed Device Default Configuration

Please select the group that contains the setting you would like to configure. From the Available settings list, select settings to include in this package and set their values.

- Schedule Agent
- Security Management Agent
  - Application Blocking
  - Device Settings
  - Logging
  - Patch Management
  - User Interaction
  - Vulnerabilities
- Security Service

Setting(s) for Patch Management

This section contains all configuration settings relating to security patch management.

Available settings
MBSA 1.2 mssecure.xml path
MBSA 1.2 patch compliance command line
MBSA 1.2 path
MBSA 2.0 path
MBSA 2.0 wsusscan.cab path
MBSA vulnerability scan command line
Office convert path
Office inventory path

Settings in package	Value
MBSA 2.0 patch compliance c...	"%programfiles(x86)%\Raynet\R...

5) Within the settings list below the tree structure:

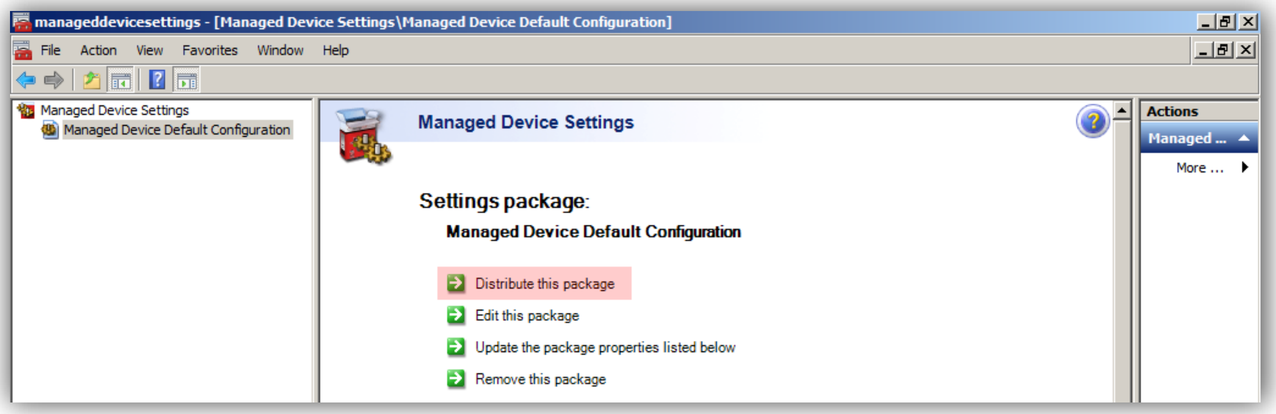
   a. Select **MBSA 2.0. path compliance command line**
   b. Click **Add ->** to make its value editable within the window on the right-hand side.
   c. Click on the current content of **MBSA 2.0. path compliance command line** within the value column
   d. Replace it with

```
"$(Programfiles)\Raynet\RMS Security Analyzer\RMSSA.exe"
"$(SysDirectory)\config\systemprofile\Appdata\SecurityScans\mbsaresults
.xml.mbsa" "$(WSUSSCANPATH)""$(SecurityUpdatePath)"
```

Please make sure to copy the value inclusive of quotation marks and blanks between the three parts of the expression.

6) Save your changes by using the **Save this package** button above the settings tree structure within the details pane.

7) You have to distribute the changed settings package to the managed devices. To do so, use the **Distribute this package** button from the details pane as shown in the screenshot below.


manageddevicesettings - [Managed Device Settings\Managed Device Default Configuration]
File
Action
View
Favorites
Window
Help
Managed Device Settings
Managed Device Default Configuration
Actions
Managed ...
More ...

Managed Device Settings

Settings package:

Managed Device Default Configuration

Distribute this package

Edit this package

Update the package properties listed below

Remove this package

The **Managed Device Settings Distribution Wizard** is displayed.

8) Follow the steps of the wizard and target all distribution locations and groups that host managed devices you want to run RMSSA on.

9) Once the wizard is complete, you can close the Managed Device Settings Console.

Update and deploy the security patch management policy

You have already added the required software and security settings packages to the security management policy. Now you have to add the default managed device settings package to your ManageSoft Default Configuration Policy and distribute both policies to finish the RMSSA setup process.

Please note that this description is based on a Deployment Manager configuration that includes the **Enhanced Policy Editor**. If your license does not cover this feature, consult the RayManageSoft documentation, especially the *Deployment policies* chapter of the *Software Deployment Guide* for a detailed description of how to add items to policy.

To update and distribute the ManageSoft Default Configuration Policy:

1) Return to the Deployment Manager Administration Console.

2) Select the **Policies** node.

3) Within the list of policies displayed in the **policies overview** tab, select your **ManageSoft Default Configuration Policy**.

4) Use the **EDIT** button from the side-bar on the right.

   The **policy editor** is displayed.

5) From the **summary** page, click the **packages tile**.

6) Use the **ADD…** button above the list of packages and select **Managed Device Settings** from the options menu.

   The **Add To Policy wizard** is displayed.

7) On the Select Managed Device Settings page, activate the checkbox for the **Managed Device Default Configuration** package.

8) Click **NEXT** to proceed.

   A dialogue is displayed to make sure you want to overwrite the existing Managed Device Default Configuration package.

9) Click **OVERWRITE EXISTING** to proceed.

10) In turn, click **NEXT**, **PROCESS** and **FINISH** on the displayed pages to finish and exit the Add To Policy wizard.

11) Within the re-displayed policy editor dialogue for the ManageSoft Default Configuration Policy, click **CLOSE**.

    The policies overview is re-displayed.

12) Select the ManageSoft Default Configuration Policy and use the **DISTRIBUTE** button from the side-bar on the right.

    The **Policy Distribution Wizard** is displayed.

13) Follow the steps of the wizard to distribute the policy to managed devices.

To update and distribute the security patch management policy:

1) Return to the Deployment Manager Administration Console.

2) Select the **Policies** node.

3) Within the list of policies displayed in the **policies overview** tab, select your **security patch management policy**.
(The name of this policy depends on your individual Security Manager policy setup.)

4) Use the **DISTRIBUTE** button from the side-bar on the right.

   The **Policy Distribution wizard** is displayed.

5) Follow the steps of the wizard to distribute the policy to managed devices.

Your basic RMSSA setup is completed.

What's next?

According to your distribution settings, packages and policies are on their way through the distribution hierarchy to take effect on managed devices. You can monitor the results within the **Reports** node of the Deployment Manager Administration Console. Refer to the *Reporting* chapter of the *Software Deployment Guide* on how to call the corresponding reports.

Please make use of the other articles available from the *RayManageSoft knowledge base* and refer to the RayManageSoft product documentation, which was delivered along with your RayManageSoft installation resources.

Contact our support team via *support@raynet.de* if you encounter issues regarding this document or the setup process itself.