



// User Guide 3.0

RayManageSoft Unified Endpoint Manager



RAYMANAGESOFT® UNIFIED ENDPOINT
MANAGER



**Copyright © Raynet GmbH (Germany, Paderborn HRB 3524). All rights reserved.
Complete or partial reproduction, adaptation, or translation without prior written permission
is prohibited.**

User Guide for release 3.0

Raynet and RayFlow are trademarks or registered trademarks of Raynet GmbH protected by patents in European Union, USA and Australia, other patents pending. Other company names and product names are trademarks of their respective owners and are used to their credit.

The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Raynet GmbH. Raynet GmbH assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. All names and data used in examples are fictitious unless otherwise noted.

Any type of software or data file can be packaged for software management using packaging tools from Raynet or those publicly purchasable in the market. The resulting package is referred to as a Raynet package. Copyright for any third party software and/or data described in a Raynet package remains the property of the relevant software vendor and/or developer. Raynet GmbH does not accept any liability arising from the distribution and/or use of third party software and/or data described in Raynet packages. Please refer to your Raynet license agreement for complete warranty and liability information.

Raynet GmbH Germany
See our website for locations.

www.raynet.de



Contents

Introduction	6
Getting Started	8
Dashboard	10
Home	12
Reports	13
Add a Report	14
Edit a Report	15
Endpoints	16
Computer Devices	16
Mobile Devices	44
Applications	46
List View	48
Folder View	48
Package Details	50
Add a Package	103
Edit a Package	117
Patch Management	125
Add a Rule	126
Edit a Rule	127
Endpoint Security	130
Update Management	130
Group Management	152
Groups	152
Administration	162
Tenant Settings	162
Device Settings	168
Device Schedules	263



Scheduled Tasks	286
Integrations	296
Site-Administration	309
All Users	309
Tenants	313
System Settings	325
Using Sorting, Filter, and Search Options	331
Sorting Options	331
Filtering Options	331
Search Options	336
Troubleshooting	337
Appendix I: Preference Settings for Managed Devices	338
Configuration, Fixing, and Evaluation	339
Managed Device Settings Packages	341
Preference Settings in the Registry	342
Preference Settings in Command Line Tools	343
Preference Settings in the Global Configuration File	359
Preference Setting Listing By Behavior	366
Alphabetical Listing of Preference Settings for Managed Devices	394
Appendix II: Logging on Managed Devices	578
Windows Agent	578
MacOS Agent	580
Appendix III: Update Policies for Windows Devices	581
Appendix IV: API Key Creation	594
Appendix V: Supported OS	596
Windows Desktop	596
Windows Server	596
MacOS	596



Appendix VI: Silent Installation for Managed Devices	597



Introduction

This guide is designed to assist IT staff to administrate and use RayManageSoft Unified Endpoint Manager 3.0.

The document will cover all information necessary to configure, administrate, and use RayManageSoft Unified Endpoint Manager.

Manual Conventions

The following typesetting conventions are used in this manual:

- Cross references to other manuals are shown in italics:
"This can be found in the *RayManageSoft Unified Endpoint Manager Release Notes*."
- Cross references and external links are shown in blue and are underlined:
"See [RayManageSoft Unified Endpoint Manager](#) for..."
- Quotations from the computer screen (titles, prompts, and so on) are shown in bold:
"Go to **Devices** screen."
- Code syntax, file samples, directory paths, entries that you may type on screen, and the like are shown in a monospaced font:
"Use `docker compose -up` to set your instance up"
- Large blocks of code are shown in a monospaced font with a grey background:

```
version: "3.7"  
services:
```
- Italics may also be used for emphasis: "This manual is *not* intended..."
- Bold may also be used for inline headings: "**Target**: Indicates a target frame..."

Two note formats are used in RayManageSoft Unified Endpoint Manager documentation

This is the basic format for giving additional information to the current topic.
It can come with four different headings:



Be aware:

This note format contains important information related to your current activity. You should not skip over this text.



Note:

This format is used for items of interest that relate to the current discussion.



Best practice:

If there is a best practice approach to the current topic you can decide if you want to follow it, or stick to your own plan.



Tip:

Tips are designed to help you find the easiest and quickest way to work with RayManageSoft Unified Endpoint Manager.

The second format is for very serious alerts.



WARNING

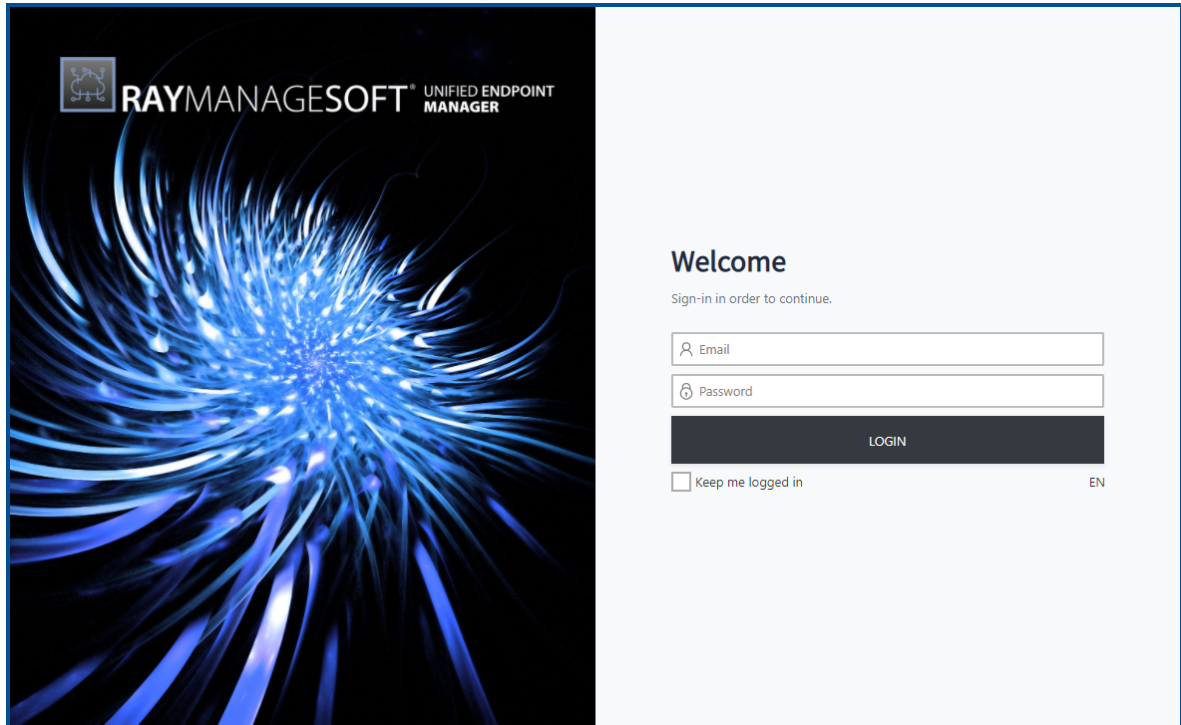
The information here may save you from data loss. Pay particular attention.

Documentation Requests

We welcome your suggestions and input on the various documentation resources available with RayManageSoft Unified Endpoint Manager and its components. Your comments and requests can be forwarded through your Raynet GmbH support representative.

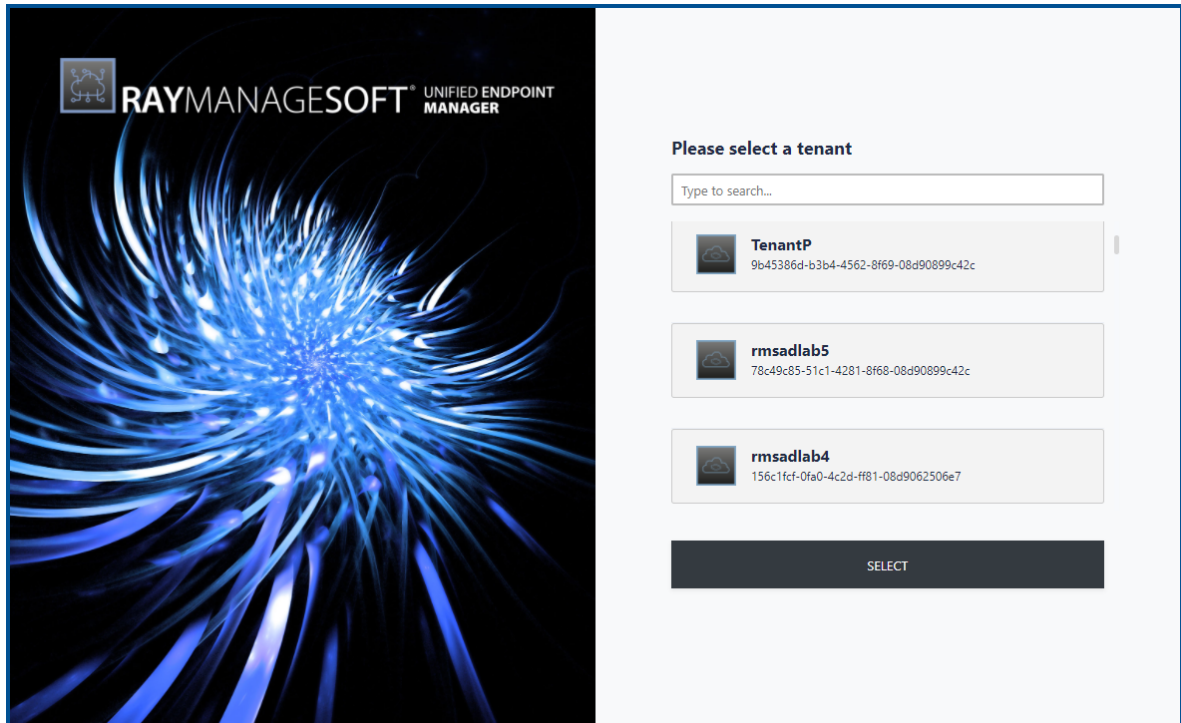


Getting Started



Enter the **E-mail** and the **Password** used for the account in order to log in. To avoid having to log in each time it is possible to check the **Keep me logged in** checkbox. If it has been checked, RayManageSoft Unified Endpoint Manager will remember the account that was last logged in from the currently used web browser until it has been logged out. It is also possible to change the language of the RayManageSoft Unified Endpoint Manager instance by simply clicking on the language code showing the currently selected language and selecting the target language. Currently the following languages are available for RayManageSoft Unified Endpoint Manager:

- English - EN
- German - DE



After logging in, it is necessary to choose which tenant to connect to. If the tenant is not directly shown in the list of tenants, either scroll down the list of tenants until the target tenant is shown or use the search field above the list to find the tenant. The tenant selection will only be shown if multiple tenants exist in the environment.

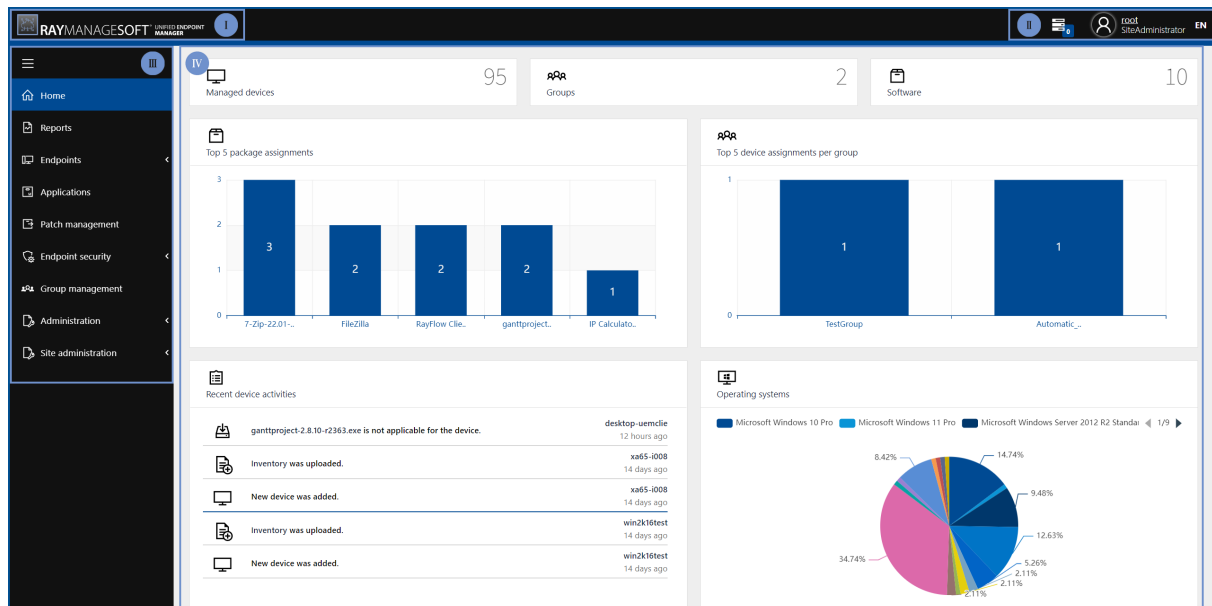
After connecting to the chosen tenant, the RayManageSoft Unified Endpoint Manager Dashboard will open.



Dashboard

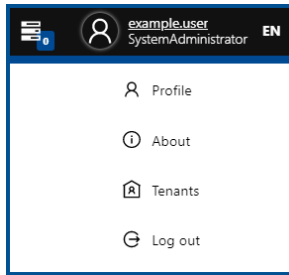
The RayManageSoft Unified Endpoint Manager **Dashboard** is divided into four different sections.

- **Section I** contains the branding which also functions as **Home** button. Clicking on this button will always load the **Home** screen.
- **Section II** contains the **Task List** icon which also includes the number of the currently active tasks, the **User** icon including the name of the currently logged in user and his role, and the **Language** button showing the currently selected language.
- **Section III** is the **Sidebar** with the vertical functional navigation. This section is used to select the content that will be shown in the content section.
- **Section IV** is the content section. This area shows the content selected in the **Sidebar**.



The Task List icon: The **Task List** icon located in **Section II** shows the number of currently active tasks in its right bottom corner. More information about the tasks that are currently running will be shown when clicking on the icon.

The User icon: The User icon also includes the name and the function of the currently logged in user account. When hovering about the icon a context menu will open.



The following options are available in the context menu:

- **Profile:** This option will open the **My Profile** page containing information regarding the logged in user. More information regarding RayManageSoft Unified Endpoint Manager users can be found in the [All Users](#) section of this guide.
- **About:** This option will open the **About** page. The page contains all relevant information about the installed version of RayManageSoft Unified Endpoint Manager including important information about the licensing, like the Hardware ID of the server on which RayManageSoft Unified Endpoint Manager is installed. For more information regarding the licensing refer to the *RayManageSoft Unified Endpoint Manager Installation Guide*.
- **Tenants:** This option can be used in order to switch from the current tenant to another tenant.
- **Log out:** Can be used to log out of RayManageSoft Unified Endpoint Manager. It will be necessary to log in again even if the **Keep me logged in** checkbox on the **Welcome** page was checked.

The Language button: The **Language** button can be used to change the language of RayManageSoft Unified Endpoint Manager. The language will be changed immediately. It is not necessary to relog.

The Collapse sidebar button: This button can be used in order to minimize the sidebar. Only the icons of the different sections will be shown when the sidebar has been minimized.



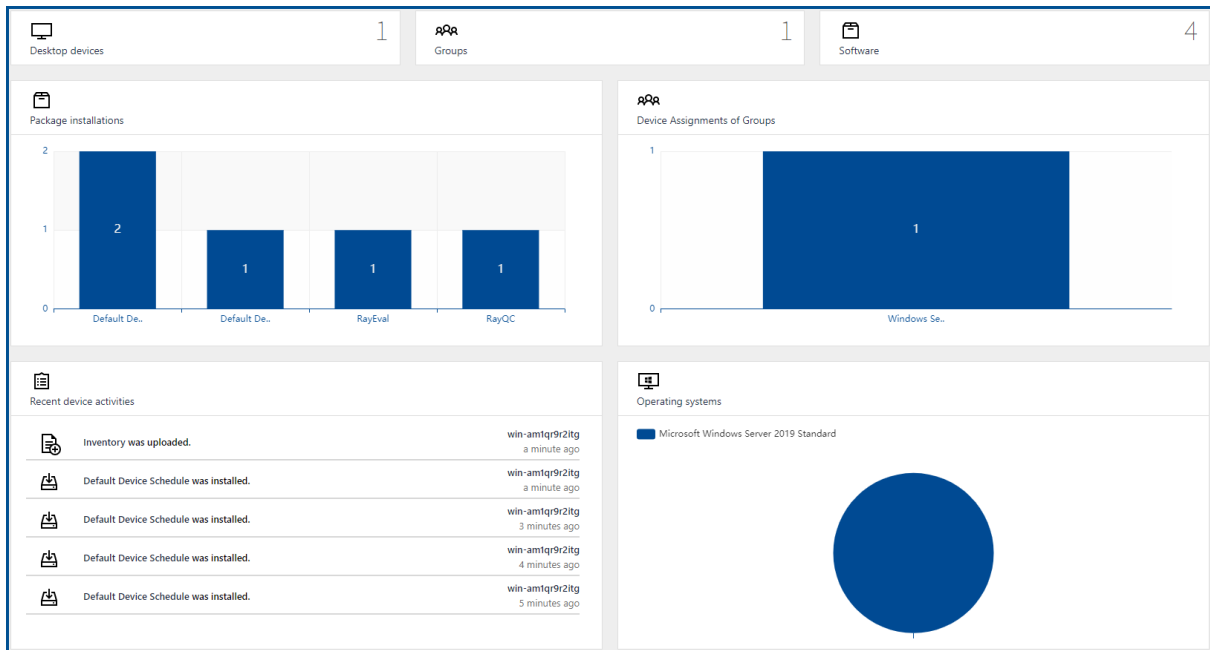
The following main categories are available in the sidebar:

- [Home](#)
- [Reports](#)
- [Endpoints](#)
- [Applications](#)
- [Patch management](#)
- [Endpoint security](#)
- [Group management](#)
- [Administration](#)
- [Site-Administration](#)



Home

The **Home** screen of RayManageSoft Unified Endpoint Manager shows an overview of the data from the tenant to which the logged in user is currently connected to.

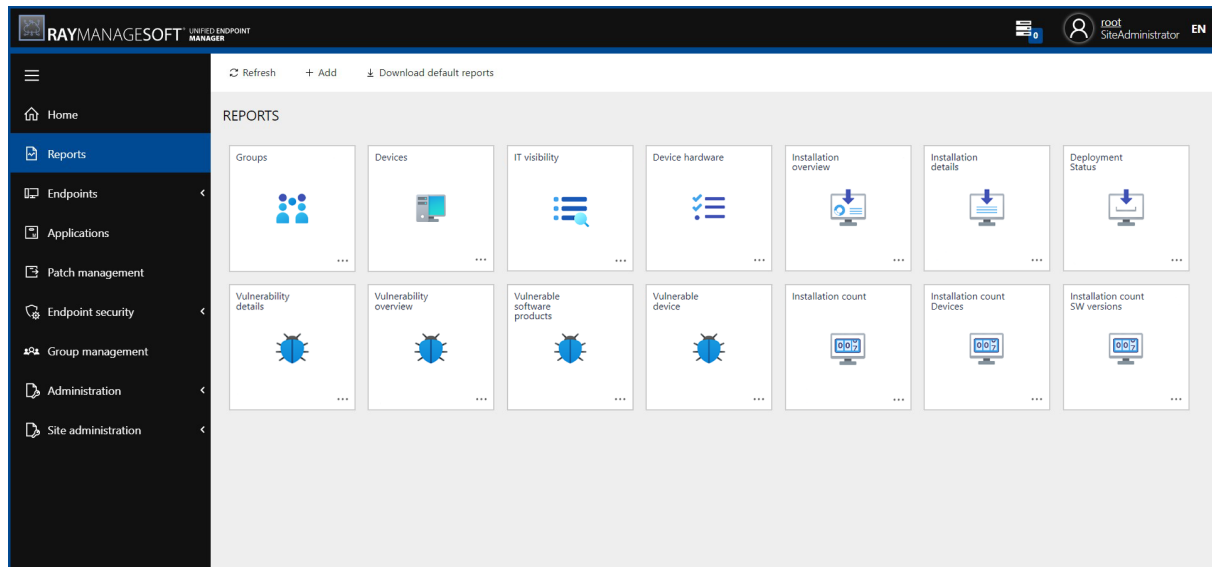


The information given in the **Home** screen includes the numbers for computers, groups, and software. Furthermore, there are charts for package installations, device assignments of groups, and operating systems, as well as a list of recent device activities. The **Home** screen is interactive. Which means that clicking on a group or activity will directly open the page containing the related information.



Reports

The **Reports** section of RayManageSoft Unified Endpoint Manager offers both, a place where to find the default reports in order to create a new report and the reports already made available. If a report is made available in RayManageSoft Unified Endpoint Manager, the report itself cannot be changed. Only the information about the data can be changed.



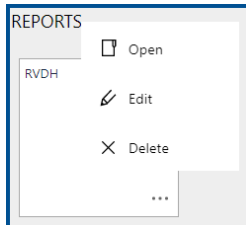
The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the screen can be used to refresh the view.
- **Add** - The **Add** button on the top left of the screen can be used to add a report. For more information see [Add a Report](#).
- **Download default reports** - This can be used to download the default reports. After downloading the reports, it is possible to import the reports into Data Hub. The ZIP file that will be downloaded contains the following reports:
 - o Deployment-Status.rpa
 - o Device-Hardware.rpa
 - o Devices.rpa
 - o Groups.rpa
 - o Installation-count.rpa
 - o Installation-overview.rpa
 - o IT-visibility.rpa
 - o Vulnerability details.rpa
 - o Vulnerability overview.rpa
 - o Vulnerability software products.rpa



Best practice:

It is recommended to import the default reports from RayManageSoft Unified Endpoint Manager into a separated RayVentory Data Hub tenant dedicated to RayManageSoft Unified Endpoint Manager to avoid any overlapping with the default RayVentory Data Hub reports!



The following actions are available when opening the context menu for a specific report that has been made available by clicking on the ... button at the bottom of the report.

- **Open** - The **Open** button can be used to open the report and gain access to the actual information contained in the report.
- **Edit** - The **Edit** button can be used to edit the information for this report (not the report itself). For more information see [Edit a Report](#).
- **Delete** - The **Delete** button can be used to delete this specific report.

Add a Report

The **Add shared report** dialog is used to add new reports to RayManageSoft Unified Endpoint Manager.

In order to add a report, first enter a name for the report in the **NAME** field of the dialog. Then enter the link where the report can be found into the **SHARED LINK** field of the **Add shared report** dialog. Information on how to create a shared link can be found in the RayVentory Data

Hub documentation.

Furthermore it is possible to add a custom image to the report by clicking on the image below the **SHARED LINK** field. A file browser will be opened. Browse for an image file to customize the image used for the report (the following file formats are supported: .gif, .jpg, .jpeg, and .png).

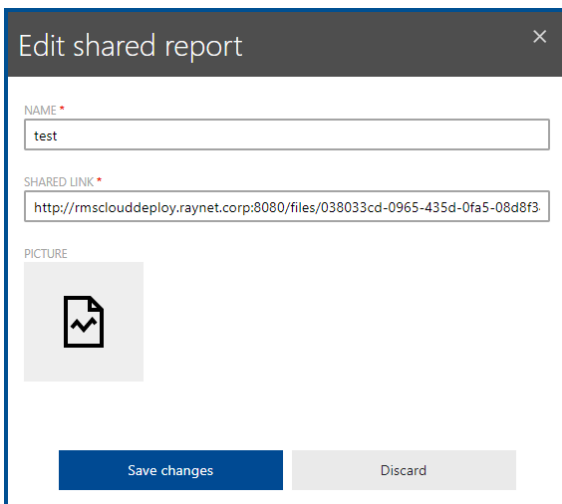
Edit a Report

The **Edit shared report** dialog is used in order to edit the information about a report.



Be aware:

All changes made by the **Edit shared report** dialog will NOT change the report itself. Only the information about the report, or in case of a change of the **SHARED LINK**, the report that will be displayed will be changed.



NAME *

test

SHARED LINK *

http://rmsclouddeploy.raynet.corp:8080/files/038033cd-0965-435d-0fa5-08d8f3.

PICTURE

Save changes Discard

It is possible to change the a name of the report in the **NAME** field of the dialog. It is also possible to change the link where the report can be found in the **SHARED LINK** field of the **Edit shared report** dialog.

Furthermore, it is possible to edit the image by clicking on the image below the **SHARED LINK** field. A file browser will be opened. Browse for an image to customize the image used for the report (the following file formats are supported: .gif, .jpg, .jpeg, and .png).



Endpoints

The **Endpoints** category of the sidebar contains the following subcategories.

- [Computer devices](#)
- [Mobile devices](#)

Computer Devices

The **Computer devices** section contains an overview of the devices managed by RayManageSoft Unified Endpoint Manager.

Operating system	Display name	Hostname	Domain	Last update	Locked	Last inventory	Managed
Windows	desktop-rei7sug	desktop-test	WORKGROUP	Feb 13, 2023, 2:48:30 PM	No	Feb 10, 2023, 11:09:01 AM	Yes
Windows	desktop-rei7sug	desktop-rei7sug	WORKGROUP	Feb 2, 2023, 1:05:06 PM	No	Feb 2, 2023, 1:47:20 PM	Yes
macOS	rmsqavms-Virtual-Machine	rmsqavms-virtual-machine	-	Feb 8, 2023, 9:36:37 AM	No	Feb 7, 2023, 11:10:02 AM	Yes
macOS	rmsqavms-virtual-machine	rmsqavms-virtual-machine	-	Feb 13, 2023, 3:10:01 PM	No	Feb 10, 2023, 5:14:01 PM	Yes
macOS	rmsqavms-Virtual-Machine	rmsqavms-virtual-machine	-	Feb 13, 2023, 3:10:06 PM	No	Feb 13, 2023, 11:21:02 AM	Yes

The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the screen can be used to refresh the view.
- **Edit** - The **Edit** button on the top left of the screen can be used to edit a device if one computer in the list has been selected. For more information see [Edit a Device](#).
- **Delete** - The **Delete** button on the top left of the screen can be used to delete one or more devices if one or more computers in the list have been selected.
- **Download Agent** - The **Download Agent** button can be used to open the dialog that can be used to download the RayManageSoft Unified Endpoint Manager Windows Agent. For more information see [Download Agent](#).
- **Autopilot** - The **Autopilot** will be added in an upcoming version of RayManageSoft Unified Endpoint Manager.
- **Advanced filter** - The **Advanced filter** is available on the top right of the screen. A description on how to use the **Advanced filters** can be found in the [Using Sorting, Filter, and Search Options](#) section.
- **Search field** - The **Search** field can be found on the top right of the screen. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.

When clicking on the **Display name** of a computer, the device details will be opened.



Device Details

There are two different types of devices which will be listed in the **Computer Devices** section of RayManageSoft Unified Endpoint Manager. The devices can be separated into managed devices and unmanaged devices. Managed devices are those devices where the RayManageSoft Unified Endpoint Manager agent has been installed. Unmanaged devices are those which are known to exist, but do not have the RayManageSoft Unified Endpoint Manager agent installed and which can therefore not be managed using RayManageSoft Unified Endpoint Manager.

For managed devices the following tabs with information will be visible when opening the **Device Details**.

- [Inventory](#)
- [Direct assignments](#)
- [Install states](#)
- [Device logs](#)

For unmanaged devices these tabs will be visible but with the exception of **Inventory** they will be empty and the **Inventory** tab will only contain the following notice:

⚠ This device was imported from a third party application. It is not yet connected to a managed device agent. To enable further functionality connect the device to RMS UEM device. [Connect]

Furthermore, the following information is always available in the device details of a managed device.

DISPLAY NAME:	win-am1qr9r2itg	🔗
HOSTNAME:	win-am1qr9r2itg	
DOMAIN:	WORKGROUP	
LAST UPDATE:	Oct 27, 2022, 1:03:07 PM	
LAST INVENTORY:	Oct 26, 2022, 9:33:07 AM	
LAST POLICY UPDATE:	Oct 27, 2022, 1:03:07 PM	
AGENT VERSION:	12.4.0.11715	
MACHINE GUID:	{4D1E6DDC-70F0-4402-B65F-DF048B657DF1}	

This information will always be shown on the left side of the device details. If a device is linked to the Azure Active Directory, a corresponding symbol will be shown located on the right side of the **Display Name**.

For unmanaged devices the information will vary. For unmanaged devices this field will contain the display name, hostname, domain, owner, ad join type, and ad register date. The ad join type for an unmanaged device can be unknown.



Inventory

The **Inventory** tab in the **Device Details** is further divided into the following sub-tabs.

- [Summary](#)
- [Software](#)
- [Hardware](#)
- [Services](#)
- [Vulnerabilities](#)

Summary

The **SUMMARY** sub-tab shows general information about the device.

The screenshot displays the Raymanagesoft interface for a device named 'win-am1q9r2itg'. The left sidebar shows metadata: DISPLAY NAME, HOSTNAME, DOMAIN, LAST UPDATE, LAST INVENTORY, LAST POLICY UPDATE, AGENT VERSION, and MACHINE GUID. The main panel is titled 'Inventory' and has sub-tabs: SUMMARY (selected), SOFTWARE (4), HARDWARE, SERVICES (194), and Vulnerabilities. The SUMMARY sub-tab shows details for 'Windows Server 2019 10.0.17763 (64-bit) Standard'. It lists hardware components: Windows Server (64-bit), BIOS (2), CPU (AMD Ryzen 7 3700U with Radeon Vega Mobile Gfx [1 core(s)]), and PHYSICAL MEMORY (RAM) (791.55 MB). It also shows storage information: A: 0 Bytes free of 0 Bytes, C: 115.99 GB free of 126.46 GB, and D: 0 Bytes free of 5.19 GB. The UUID is 4C4BF5BD-1673-4F5F-B9BB-64CE08CF603E.

Information in this tab includes the operating system, the IPv4 and IPv6 address, the CPU, the UUID, the drives, the BIOS, and the physical memory (RAM) of the device.

Software

The **SOFTWARE** sub-tab shows all known information about the installed software on the device. It is further divided into two more tabs:

- [Products](#)
- [Raw Data](#)

Products

In the **Products** tab, information about the installed products are shown. This information is based on the raw data that is collected during the inventory of the device.



Be aware:

In order to get the product information, a working Catalog integration is needed. Information on how to setup the Catalog integration can be found [here](#).

Inventory

Direct assignments2

Install states2

Device logs

SUMMARY

SOFTWARE118

HARDWARE

SERVICES170

Vulnerabilities846

Products64

Raw data118

Adobe

	Product name	Product version	Vendor	Vulnerabilities	
	Adobe Refresh Manager	1.x	Adobe	0	^
	Adobe Refresh Manager	1.8.0			
	Adobe Acrobat Reader DC - Deutsch	18.x		0	v
	Adobe Refresh Manager	1.8.x	Adobe	0	v
	Adobe Acrobat Reader DC	2018	Adobe	834	v

The information includes the name of the product, the version of the product, the vendor of the application, and if there are any known vulnerabilities. To get more specific information click on the entry for the application. The entry will be expanded and some additional information will be shown. Only one entry can be expanded at a time. If an entry has already been expanded and another entry is being expanded, the first entry will be collapsed.

The search field can be used to lower the number of products shown in the list. More information on how to use the search field can be found in the [Search Options](#) chapter.

Raw Data

In the **Raw data** tab, the raw data collected for the device that has been collected during the inventory is shown.



The screenshot shows the RayManageSoft interface with the 'Software' tab selected. The top navigation bar includes 'Inventory', 'Direct assignments' (5), 'Install states' (8), and 'Device logs'. Below this, the 'SUMMARY' section has tabs for 'SOFTWARE' (17), 'HARDWARE', 'SERVICES' (267), and 'Vulnerabilities'. Under 'SOFTWARE', there are sub-tabs for 'Products' (4) and 'Raw data' (17). A search bar labeled 'Type to search...' is present. The main table lists installed software with columns for application type, name, version, size, and install date.

Type	Name	Version	Size	Install Date
MSI	BabelEdit	3.0.0.0	96.96 MB	2 months ago
EXE	Connection Manager	(unknown version)	(unknown size)	(unknown install date)
MSI	ManageSoft for managed devices	12.4.0.11704	71.17 MB	2 months ago
MSI	ManageSoft for managed devices	2.3.0.11700	70.8 MB	2 months ago
EXE	Microsoft Edge	105.0.1343.50	(unknown size)	(unknown install date)
EXE	Microsoft Edge Update	1.3.167.21	(unknown size)	(unknown install date)

This information includes the type of the application, name of the application, the version number, the size of the installation, and the install date (if known).

The search field can be used to lower the number of raw data shown in the list. More information on how to use the search field can be found in the [Search Options](#) chapter.

Hardware

The **HARDWARE** sub-tab is subdivided into a number of tabs. These are as follows.

- [Network Adapters](#)
- [Hard Drives](#)
- [Graphic Cards](#)
- [Physical Memory \(RAM\)](#)

Network Adapters

The **NETWORK ADAPTERS** tab contains the information about the network adapters (both virtual and physical) that have been discovered for a device.



Inventory | Direct assignments 4 | Install states 6 | Device logs

SUMMARY | SOFTWARE 4 | **HARDWARE** | SERVICES 194 | Vulnerabilities

NETWORK ADAPTERS 2 | HARD DRIVES 3 | GRAPHIC CARDS 1 | PHYSICAL MEMORY (RAM)

Hide virtual network adapters ☐

Adapter Name	IP addresses	Subnet mask	Default IP gateway
Microsoft Kernel Debug Network Adapter		(unknown)	(unknown)
Microsoft Hyper-V Network Adapter 00:15:5D:B2:18:06	172.23.25.25 fe80::a8b7:3a18:6a4a:5541	255.255.240.0.64	172.23.16.1

It is possible to only show the physical network adapters by checking the **Hide virtual network adapters** checkbox.

Hard Drives

The **HARD DRIVES** tab contains information about the hard drives that have been discovered.

Inventory | Direct assignments 4 | Install states 6 | Device logs

SUMMARY | SOFTWARE 4 | **HARDWARE** | SERVICES 194 | Vulnerabilities

NETWORK ADAPTERS 2 | **HARD DRIVES 3** | GRAPHIC CARDS 1 | PHYSICAL MEMORY (RAM)

Drive Letter	Free Space	Total Space	File system	Serial number	Description
A:	0 Bytes free of 0 Bytes		(unknown)	(unknown)	3 1/2 Inch Floppy Drive
C:	115.99 GB free of 126.46 GB		NTFS	D6E90026	Local Fixed Disk
D:	0 Bytes free of 5.19 GB		UDF	D12D1B1C	CD-ROM Disc

The tab shows information for each drive like free and total disk space, the file system, the serial number, and the type of the drive.

Graphic Cards

The **GRAPHIC CARDS** tab shows the information about the discovered graphic cards.



Inventory | Direct assignments 4 | Install states 6 | Device logs

SUMMARY | SOFTWARE 4 | **HARDWARE** | SERVICES 194 | Vulnerabilities

NETWORK ADAPTERS 2 | HARD DRIVES 3 | **GRAPHIC CARDS 1** | PHYSICAL MEMORY (RAM)

Microsoft Hyper-V Video

Driver date: 16 years ago | Driver version: 10.0.17763.1

It shows information for the graphic card like version and date of the installed driver.

Physical Memory (RAM)

The **PHYSICAL MEMORY (RAM)** tab shows the amount of RAM that has been discovered for the managed device.

Inventory | Direct assignments 4 | Install states 6 | Device logs

SUMMARY | SOFTWARE 4 | **HARDWARE** | SERVICES 194 | Vulnerabilities

NETWORK ADAPTERS 2 | HARD DRIVES 3 | GRAPHIC CARDS 1 | **PHYSICAL MEMORY (RAM)**

791.55 MB

Services

The **SERVICES** sub-tab shows all services discovered for the managed device.

Inventory | Direct assignments 4 | Install states 6 | Device logs

SUMMARY | SOFTWARE 4 | **HARDWARE** | **SERVICES 194** | Vulnerabilities

Type to search...

AllJoyn Router Service · AJRouter	[Stopped]
Routes AllJoyn messages for the local AllJoyn clients. If this service is stopped the AllJoyn clients that do not have their own bundled routers will be unable to run.	
Application Layer Gateway Service · ALG	[Stopped]
Provides support for 3rd party protocol plug-ins for Internet Connection Sharing	
Application Identity · ApplDSvc	[Stopped]
Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced.	
Application Information · Appinfo	[Stopped]
Facilitates the running of interactive applications with additional administrative privileges. If this service is stopped, users will be unable to launch applications with the additional administrative privileges they may require to perform desired user tasks.	
Application Management · AppMgmt	[Stopped]
Processes installation, removal, and enumeration requests for software deployed through Group Policy. If the service is disabled, users will be unable to install, remove, or enumerate software deployed through Group Policy. If this service is disabled, any services that explicitly depend on it will fail to start.	
App Readiness · AppReadiness	[Stopped]



It shows information about the functionality of the service as well as if the service is currently running or if it is stopped.

Vulnerabilities

The **Vulnerabilities** sub-tab will only be available if vulnerabilities for software installed on the device have been identified.



Be aware:

In order to get the vulnerability information, a working Catalog integration is needed. Information on how to setup the Catalog integration can be found [here](#).

Inventory				
Direct assignments 2				
Install states 2				
Device logs				
SUMMARY SOFTWARE 118 HARDWARE SERVICES 170 Vulnerabilities 846				
Type to search...				
CWE ID	CWE Name	Score	Published	Summary
CVE-2019-7037	Out-of-bounds Write	9.8	2019-05-24	Adobe Acrobat and Reader versions 2019.010.20099 and earlier, 2019.010.20099 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-3801	Use After Free	9.8	2020-03-25	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2019-8206	Out-of-bounds Write	9.8	2019-10-17	Adobe Acrobat and Reader versions 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-3805	Use After Free	9.8	2020-03-25	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2019-7772	Use After Free	9.8	2019-05-22	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free

The vulnerabilities shown are sorted by their vulnerability score, showing the vulnerabilities with the highest impact first and those with the lowest impact last. The following information will be shown for each vulnerability:

- **CWE ID:** The ID that is used for the vulnerability in the [Common Weakness Enumeration \(CWE\) List](#).
- **CWE Name:** The name that is used for the vulnerability in the [Common Weakness Enumeration \(CWE\) List](#).
- **Score:** The score defining the impact of the vulnerability.
- **Published:** The date when the information about the vulnerability was published.
- **Summary:** General information about the vulnerability such as the affected software versions and a short description of the vulnerability and the risks it poses.



Direct Assignments

The **Direct Assignments** tab shows an overview of the packages for which a direct assignment to the device currently exists.

Package name	Force install	Exclusive Flag	Removable
Default Device Settings	Yes	No	No
Default Device Schedule	Yes	No	No
7-Zip-22.01-x64	No	No	No

The following actions are available in the **Direct Assignments** tab.

- **Refresh** - The **Refresh** button on the top left of the list can be used to refresh the view.
- **Assign package** - The **Assign package** button on the top left of the list can be used to directly assign a package to the device. For more information see [Add a Package Assignment to an Endpoint](#).
- **Edit** - The **Edit** button on the top left of the list can be used to edit a package assignment if one assignment in the list has been selected. For more information see [Edit a Package Assigned to an Endpoint](#).
- **Delete** - The **Delete** button on the top left of the list can be used to delete one or more selected assignments.
- **Search field** - The **Search** field can be found on the top right of the list. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.

Add a Package Assignment to an Endpoint

With the **Add package assignment** dialog, it is possible to add a new package assignment from the list of the available packages to the device. It contains three different tabs:

- [General tab](#)
- [Postponement tab](#)
- [Lifetime tab](#)



Best Practice:

Avoid assigning a package that has already been assigned (and installed on a managed device). This should always be avoided, even if it is a different version, as this might lead to some unpredictable results regarding the actual installations and install states.

Before assigning the package, first unassign the old package. Then ensure that the policy has been updated and the inventory has been executed. Only after these steps has been executed, the new assignment should be committed.



In case the package stays installed on the managed device (no exclusive setting) it can be expected that the upgrade of the existing package will be done correctly and the install states will be updated accordingly.

General Tab

In the **General** tab the application for the assignment is chosen. Furthermore, its installation behavior and the behavior once the assignment has been removed are configured here.

Add package assignment

General Postponement Lifetime

PACKAGE

7-Zip 22.00 x64 edition 22.0.0.0 (Applications)

FORCE INSTALL

☒ **This application is required**
Install the application automatically. You can configure [postponement settings](#), to allow the user to defer the installation for a short time.

☐ **This application is required but can be uninstalled**
Install the application automatically, but allow the user to uninstall it. You can configure [postponement settings](#), to allow the user to defer the installation for a short time.

☐ **This application is optional**
Allow the user to choose whether or not to install the application from a catalog of available applications.

OUT-OF-POLICY BEHAVIOR
What should happen if the assignment of this application is removed?

☒ **The application should stay on the device**
The application and its data will stay, and it will be fully functional even if the application is no longer assigned to the device.

☐ **The application should be removed from the device**
The application will be automatically removed by the next policy update. Application data and content will not be removed.

Add Discard

- **PACKAGE:** Select the package that should be used for the assignment. This field supports auto completion.
- **FORCE INSTALL:** This field can be used to define the installation behavior for the package. There are three different options available.
 - **This application is required:** If this option is chosen, the application will be configured automatically. The user can defer the installation for up to a predefined amount of time. The time frame can be configured in the [Postponement](#) tab.
 - **This application is required but can be uninstalled:** If this option is chosen, the installation will be installed, but the user has the option to uninstall it afterward. The user can defer the installation for up to a predefined amount of time. The time frame can be configured in the [Postponement](#) tab.
 - **This application is optional:** If this option is chosen, the user can choose whether to install the application from a catalog of available applications.
- **OUT-OF-POLICY BEHAVIOR:** This setting defines what happens with the application once the assignment for the application is removed.
 - **The application should stay on the device:** If this option is chosen, the application will



stay on the device and its data and content will remain untouched once the application has been removed from the assignments.

- **The application should be removed from the device:** If this option is chosen, the application will be automatically removed by the next policy update. Application data and content will not be removed.

Postponement Tab

In the **Postponement** tab, the postponement for the installation can be configured. This tab is only available if **This application is required** or **This application is required but can be uninstalled** have been selected in the [General](#) tab.

The screenshot shows a dialog box titled "Add package assignment" with a close button (X) in the top right corner. It has three tabs: "General", "Postponement" (which is selected and underlined), and "Lifetime". Under the "POSTPONE THE INSTALLATION" section, there are two checkboxes. The first is "Postpone by days" with a text input field containing the number "0". The second is "Postponement by date" with a date and time input field showing "06/02/2023 02:05 PM". Below this field are two radio buttons: "Local Time" (which is selected) and "UTC Time". At the bottom of the dialog are two buttons: "Add" (in blue) and "Discard" (in grey).

- **POSTPONE THE INSTALLATION:** This option is used to specify the time for which the installation can be postponed.
 - **Postpone by days:** If this option is selected, define the number of days for which the installation can be postponed.
 - **Postponement by date:** If this option is selected, define the exact date and time up to when the installation can be postponed. Also define if the local time is used or if UTC is chosen for the installation date.
 - **Local Time:** Select Local Time in order to use the local time of the device.
 - **UTC Time:** Select UTC Time in order to use the Coordinated Universal Time.



Lifetime Tab

In the **Lifetime** tab, the time frame during which the assignment will be active can be defined. By default, an assignment will be active from the time of its creation until it will be deleted manually.

- **LIFETIME OF ASSIGNMENT:** This defines the time the assignment will be active.
 - **Always active:** If this option is selected, the application will be available as soon as the assignment has been created.
 - **Effective from:** If this option is selected, the application will become available at the specified date and time.
 - **Local Time:** Select **Local Time** in order to use the local time of the device.
 - **UTC Time:** Select **UTC Time** in order to use the Coordinated Universal Time.
 - **Effective range:** If this option is selected, the package will only be available during the time frame defined by the Effective range setting. If the **The application should be removed from the device** option has been selected in the [General](#) tab, the package will be uninstalled as soon as the expiry date has been reached.
 - **Local Time:** Select **Local Time** in order to use the local time of the device.
 - **UTC Time:** Select **UTC Time** in order to use the Coordinated Universal Time.

Edit a Package Assigned to an Endpoint

The **Edit package assignment** dialog is used to edit the settings for an existing package assignment. It contains three different tabs:

- [General tab](#)
- [Postponement tab](#)
- [Lifetime tab](#)



General Tab

In the **General** tab the application for the assignment is chosen. Furthermore, its installation behavior and the behavior once the assignment has been removed are configured here.

The screenshot shows the 'Edit package assignment' dialog box with the 'General' tab selected. The 'PACKAGE' field contains '7-Zip 22.00 x64 edition - 22.0.0.0'. Under 'FORCE INSTALL', the option 'This application is required but can be uninstalled' is selected. Under 'OUT-OF-POLICY BEHAVIOR', the option 'The application should stay on the device' is selected. At the bottom are 'Save changes' and 'Discard' buttons.

- **PACKAGE:** Select the package that should be used for the assignment. This field supports auto completion.
- **FORCE INSTALL:** This field can be used to define the installation behavior for the package. There are three different options available.
 - **This application is required:** If this option is chosen, the application will be configured automatically. The user can defer the installation for up to a predefined amount of time. The time frame can be configured in the [Postponement](#) tab.
 - **This application is required but can be uninstalled:** If this option is chosen, the installation will be installed, but the user has the option to uninstall it afterward. The user can defer the installation for up to a predefined amount of time. The time frame can be configured in the [Postponement](#) tab.
 - **This application is optional:** If this option is chosen, the user can choose whether to install the application from a catalog of available applications.
- **OUT-OF-POLICY BEHAVIOR:** This setting defines what happens with the application once the assignment for the application is removed.
 - **The application should stay on the device:** If this option is chosen, the application will stay on the device and its data and content will remain untouched once the application has been removed from the assignments.
 - **The application should be removed from the device:** If this option is chosen, the application will be automatically removed by the next policy update. Application data and content will not be removed.



Postponement Tab

In the **Postponement** tab, the postponement for the installation can be configured. This tab is only available if **This application is required** or **This application is required but can be uninstalled** have been selected in the [General](#) tab.

Edit package assignment

General Postponement Lifetime

POSTPONE THE INSTALLATION

☐ Postpone by days 0

☐ Postponement by date 06/02/2023 02:10 PM

☒ Local Time ☐ UTC Time

Save changes Discard

- **POSTPONE THE INSTALLATION:** This option is used to specify the time for which the installation can be postponed.
 - **Postpone by days:** If this option is selected, define the number of days for which the installation can be postponed.
 - **Postponement by date:** If this option is selected, define the exact date and time up to when the installation can be postponed. Also define if the local time is used or if UTC is chosen for the installation date.
 - **Local Time:** Select Local Time in order to use the local time of the device.
 - **UTC Time:** Select UTC Time in order to use the Coordinated Universal Time.



Lifetime Tab

In the **Lifetime** tab, the time frame during which the assignment will be active can be defined. By default, an assignment will be active from the time of its creation until it will be deleted manually.

Edit package assignment

General Postponement **Lifetime**

LIFETIME OF ASSIGNMENT

☒ **Always active**

☐ **Effective from**

06/02/2023 02:10 PM

☒ Local Time ☐ UTC Time

☐ **Effective range**

06/02/2023 02:10 PM - 06/02/2023 02:10 PM

☒ Local Time ☐ UTC Time

The application is available immediately

Save changes Discard

- **LIFETIME OF ASSIGNMENT:** This defines the time the assignment will be active.
 - **Always active:** If this option is selected, the application will be available as soon as the assignment has been created.
 - **Effective from:** If this option is selected, the application will become available at the specified date and time.
 - **Local Time:** Select **Local Time** in order to use the local time of the device.
 - **UTC Time:** Select **UTC Time** in order to use the Coordinated Universal Time.
 - **Effective range:** If this option is selected, the package will only be available during the time frame defined by the Effective range setting. If the **The application should be removed from the device** option has been selected in the [General](#) tab, the package will be uninstalled as soon as the expiry date has been reached.
 - **Local Time:** Select **Local Time** in order to use the local time of the device.
 - **UTC Time:** Select **UTC Time** in order to use the Coordinated Universal Time.



Install States

The **Install State** tab shows the current deployment state of the packages assigned to the device.

Package Name	Package Version	Source	Deployment State
Default Device Settings	1.0.0.0	Direct Assignment	Installed
Default Device Schedule	1.0.0.0	Direct Assignment	Installed
7-Zip-22.01-x64	22.1.0.0	Direct Assignment	Optional

In the **Deployment State** column the current state is shown using color-coded icons.

State	Icon	Description
Pending		The deployment and/or installation of the package has not yet finished.
Upgrade Pending		An upgrade for the package has not yet been applied.
Optional		An optional package is available but has not been installed yet.
Installed		The package has been successfully deployed and installed.
Uninstalled		The package has been uninstalled.
Failed		The deployment and/or installation of the package has failed. If the deployment has failed, in addition to showing the Deployment Status as Failed an additional attention symbol is shown which will contain information on why the deployment has failed:

By clicking on the **Package Name** it is possible to switch to the details of the specific package. For more information on the details refer to the respective details chapter.

The **Refresh** button on the top left of the list can be used to refresh the view.



Device Logs

The **Device Logs** tab shows the log for the latest activities of the device.

Inventory

Direct assignments2

Install states2

Device logs

Refresh

Advanced filter

Time ago	Action	Package	File	Error
3 months ago	Requested policy	-	-	-
3 months ago	Log uploaded	-		-
3 months ago	Requested policy	-	-	-
3 months ago	Requested policy	-	-	-
3 months ago	Requested policy	-	-	-
3 months ago	Requested policy	-	-	-
3 months ago	Requested policy	-	-	-
3 months ago	Requested policy	-	-	-
3 months ago	Requested policy	-	-	-
3 months ago	Requested policy	-	-	-
3 months ago	Requested policy	-	-	-
3 months ago	Requested policy	-	-	-

First

123

Last

Entries per page: 10

Entries containing more specific log files are marked in the **File** column. When clicking on the specific entry, the detailed log will be shown.

The following actions are available in the **Device Logs** tab.

- **Refresh** - The **Refresh** button on the top left of the list can be used to refresh the view.
- **Advanced filter** - The **Advanced filter** is available on the top right of the screen. A description on how to use the **Advanced filters** can be found in the [Using Sorting, Filter, and Search Options](#) section.

Edit a Device

In the **Edit device** dialog information about the selected device can be changed.



Edit device

DISPLAY NAME *
example-device

OWNER

NOTE

LOCKED

If a device is locked, it is prohibited from uploading files or obtaining new packages.

OPERATING SYSTEM TYPE
Unspecified

Save changes Discard

It is possible to change the following details.

- **DISPLAY NAME:** The display name is the name the device will be shown with in the device overview. This field is mandatory and cannot be left empty.
- **OWNER:** The owner of the device can be entered here. This field is optional.
- **NOTE:** This field is for additional information regarding the device. This field is optional.
- **LOCKED:** The device can either be locked or unlocked.
- **OPERATING SYSTEM TYPE:** This dropdown field can be used to define the type of the device. There are three options available:
 - **Windows:** Select this entry for Windows devices.
 - **macOS:** Select this entry for macOS devices.
 - **Unspecified:** Select this entry for devices where the OS is unknown or which are neither Windows nor macOS devices.



Be aware:

If a device is locked, it can no longer upload files or obtain new packages!

Download Agent

This dialog is used to download the Windows agent and the MacOS agent. Once the agent has been installed on a device, RayManageSoft Unified Endpoint Manager will be able to manage the device.



Download agent

Download

Download the RayManageSoft UEM Windows agent:

Download Windows agent

Download the RayManageSoft UEM MacOS agent:

Download MacOS agent

Install

Download the managed device client relevant for your OS from this page and install it on the computer you want to manage. Once the agent is started, the device will appear in the **Desktop devices** tab.

After installing

After starting the agent on your machine you may view different information about your current device. This includes the following:

- View your currently installed programs
- View optional programs to install
- Uninstall optional programs
- Repairing your installation
- View inventories of your device

Close

Advanced information on how to configure managed devices can be found in the [Appendix I: Preference Settings for Managed Devices](#).

The following agents are available for download:

- [Windows agent](#)
- [MacOS agent](#)

Windows Agent

The following chapters describe how to install and use the RayManageSoft Unified Endpoint Manager Windows Agent.

- [Install the RayManageSoft Unified Endpoint Manager Windows Agent](#)
- [The RayManageSoft Unified Endpoint Manager Windows Agent](#)



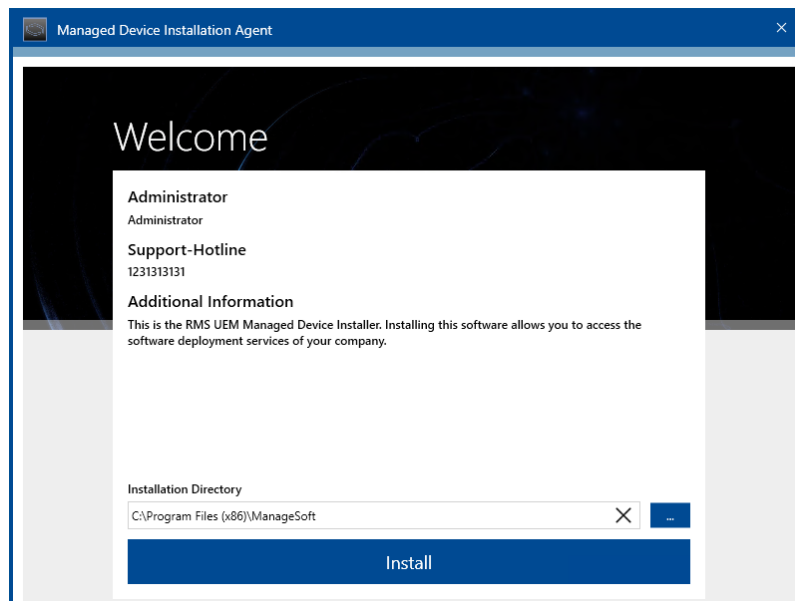
Install the Windows Agent

- After downloading the Windows Agent, copy the file to the target machine and extract the .zip file.
- Double-click on the extracted `setup.exe` file. The Managed Device Installation Agent will start.

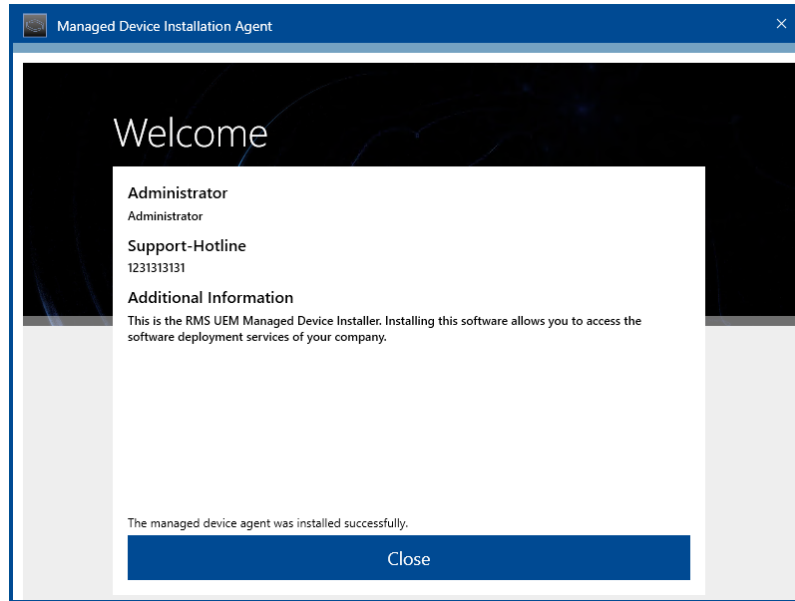


Be aware:

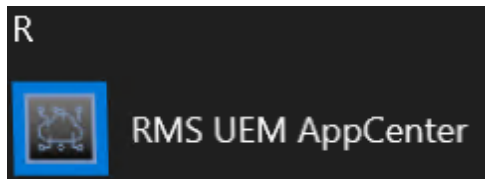
Administrator privileges are needed in order to install the Windows Agent.



- Define the target directory by either entering a directory manually or by using the **Browse [...]** button and select the target directory in the browser (by default the target directory is `c:\Program Files (x86)\ManageSoft`).
- Click on the **Install** button to start the installation.



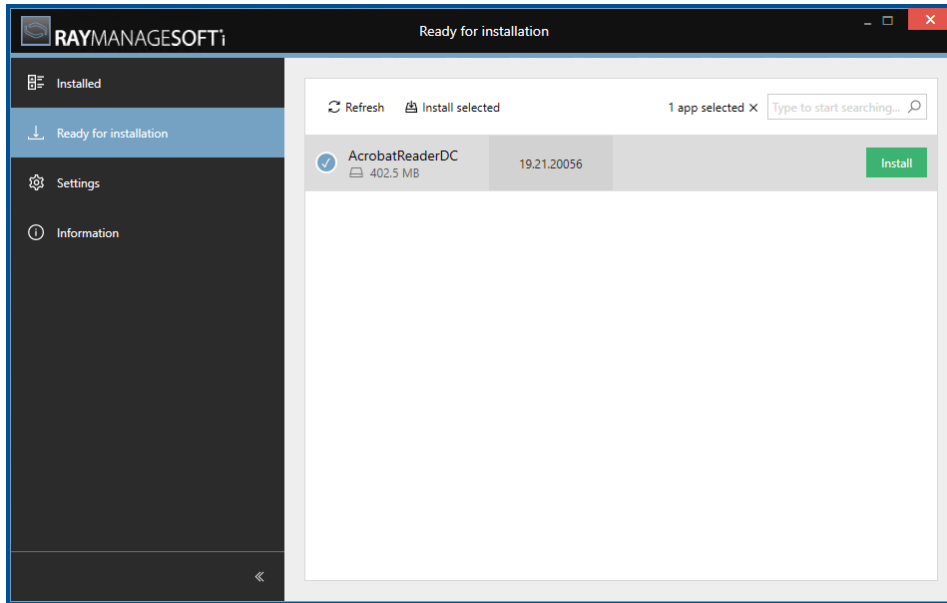
- After the installation has been finished, click on the **Close** button to close the RayManageSoft Unified Endpoint Manager Windows Agent.
- The RayManageSoft Unified Endpoint Manager agent has now been successfully installed on the device and can be accessed by clicking on the **RMS UEM AppCenter** entry in the **Start** menu.



The Windows Agent

The Windows Agent is divided into four different tabs.

- [Installed](#)
- [Ready for Installation](#)
- [Settings](#)
- [Information](#)



Installed

The **Installed** tab shows a list of all managed software that is currently installed on the endpoint. It shows information about the installed software, like the size of the package and its version.



Note:

The list of software displayed does not include applications that were installed before the Windows agent was installed or software that was not installed using RayManageSoft Unified Endpoint Manager installation routines. To manage applications that are not listed use the **Add/Remove program** functionality of the operating system.

Information on how to use the search field can be found in the [Using Sorting, Filter, and Search Options](#) chapter of this guide. If one or more software packages in the list are selected, this is shown next to the search field.

The **Refresh** button can be used to manually refresh the list.



If the software is configured to allow for installation and uninstallation by the user, it is possible to uninstall a selected software by clicking on the **Uninstall** button. Furthermore, if the software is not working correctly, a repair can be initiated by clicking on the **Repair** button.



Be aware:

Keep in mind, that the settings for the specific software package determine in how far a user can influence the installation status on the endpoint.

Ready for Installation

The **Ready for Installation** tab shows a list of the software that still needs to be installed or can be installed on the client. If a software package has already been installed, it will be shown in the **Installed** tab instead. The list shows the size of the package, the current version of the package, and the status in form of a button located at the right side of the list.

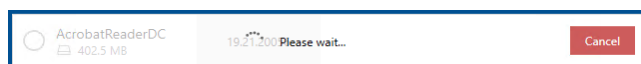
Information on how to use the search field can be found in the [Using Sorting, Filter, and Search Options](#) chapter of this guide. If one or more software packages in the list are selected, this is shown next to the search field.

The list can be manually refreshed by clicking the **Refresh** button on the top left of the list.



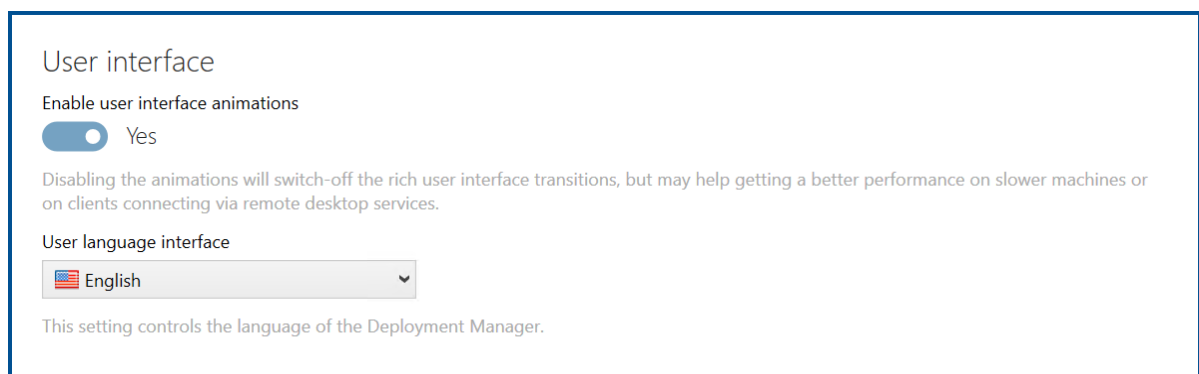
In order to start the installation process for one or more selected software packages, click on the **Install selected** button on top of the list. If a specific software package should be installed, click on the **Install** button that is located on the right side of the entry.

As long as it is not yet finished, the installation can be aborted by clicking the **Cancel** button.



Settings

The **Settings** tab contains the settings for Windows agent.





The following options are available in this tab.

- **Enable user interface animations:** Set the switch to **No** to turn off the animations of the user interface. By default, the animations are turned on.
- **User language interface:** The dropdown menu can be used to change the language used in the user interface. By default, the language is set to English.

Furthermore, it is possible to manually start a check for updates. Click on the **This user (me)** button to start a check for updates for the user environment. In order to check for updates for the computer, click on the **This computer** button.



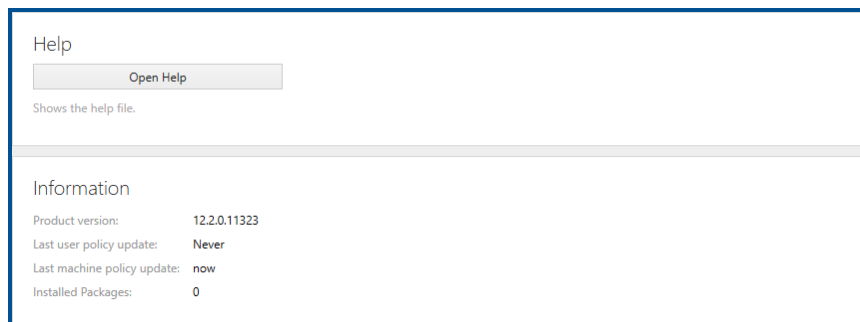
Be aware:

To manually start the check for updates for the computer, administrator privileges are needed!

The update process usually runs automatically in the background and gets the updates a few times a day. The buttons in the settings are used to force the update process to run immediately and thereby to ensure that the machine is up-to-date.

Information

In the **Information** tab, information about the Windows agent can be found.



It is possible to access the help file by clicking on the **Open Help** button located in this tab.

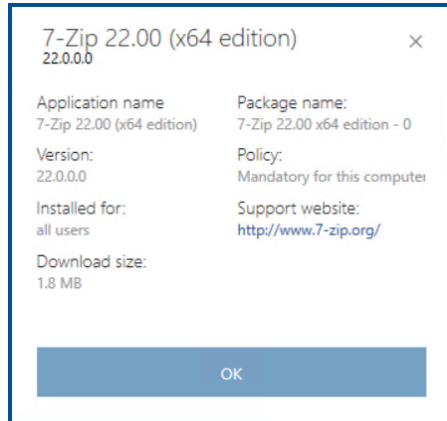
Furthermore, the following information are shown in this tab.

- **Product version:** The version of the Windows agent.
- **Last user policy update:** The last time the user policy has been updated.
- **Last machine policy update:** The last time the machine policy has been updated.
- **Installed packages:** The number of packages installed on the endpoint.



Package Details

Clicking on a package in the list, both in the **Installed** and the **Ready for Installation** tab, will open the details for the package.



The following information for the package will be shown:

- **Application name:** The name of the application contained in the package.
- **Package name:** The name of the package.
- **Version:** The version of the application.
- **Policy:** The policy used for the package. This contains the information whether the package is mandatory or optional.
- **Installed for:** The users for which the package is installed.
- **Download size:** The size of the package.

MacOS Agent

The following chapters describe how to install and use the RayManageSoft Unified Endpoint Manager MacOS Agent.

- [Install the MacOS Agent](#)
- [ManageSoft.app](#)
- [MGSPolicyUpdate.app](#)
- [Uninstall the MacOS Agent](#)

Install the MacOS Agent

In order to install the MacOS agent on the target client execute the following steps:

1. If it has not already been downloaded to the correct device, copy the `UEM-MacOS-Agent.zip` file to the target device.
2. Decompress the `UEM-MacOS-Agent.zip` file.
3. The resulting folder should contain the following files:
 - a. `/UEM-MacOS-Agent/bin/Managed Device Default Machine Schedule/Default`



Machine Schedule.nds

b. /UEM-MacOS-Agent/bin/ManageSoft for managed devices.pkg

c. /UEM-MacOS-Agent/mgssetup.sh

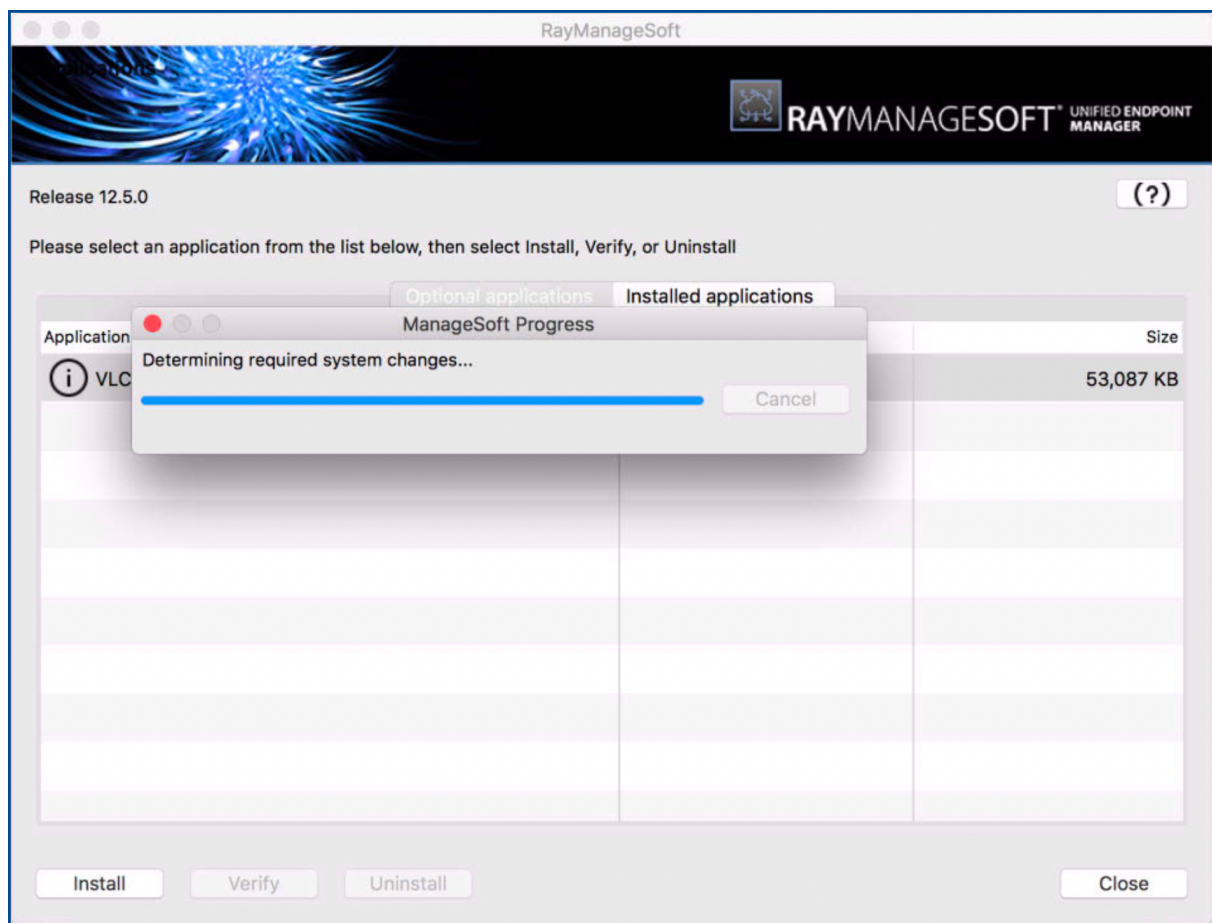
4. Open the Terminal application and use the following command to install the MacOS agent application:

```
sudo bash /[Full Path]/UEM-MacOS-Agent/mgssetup.sh
```

5. The MacOS agent will now be installed automatically, including an initial schedule.

ManageSoft.app

The `ManageSoft.app` can be used to manage the packages that have been deployed to the device.



The **(?)** in the upper right corner can be used to open the help file.

The **Close** button in the lower right corner can be used to close the application.

There are two tabs available in the application.

- [Optional applications](#) tab
- [Installed applications](#) tab

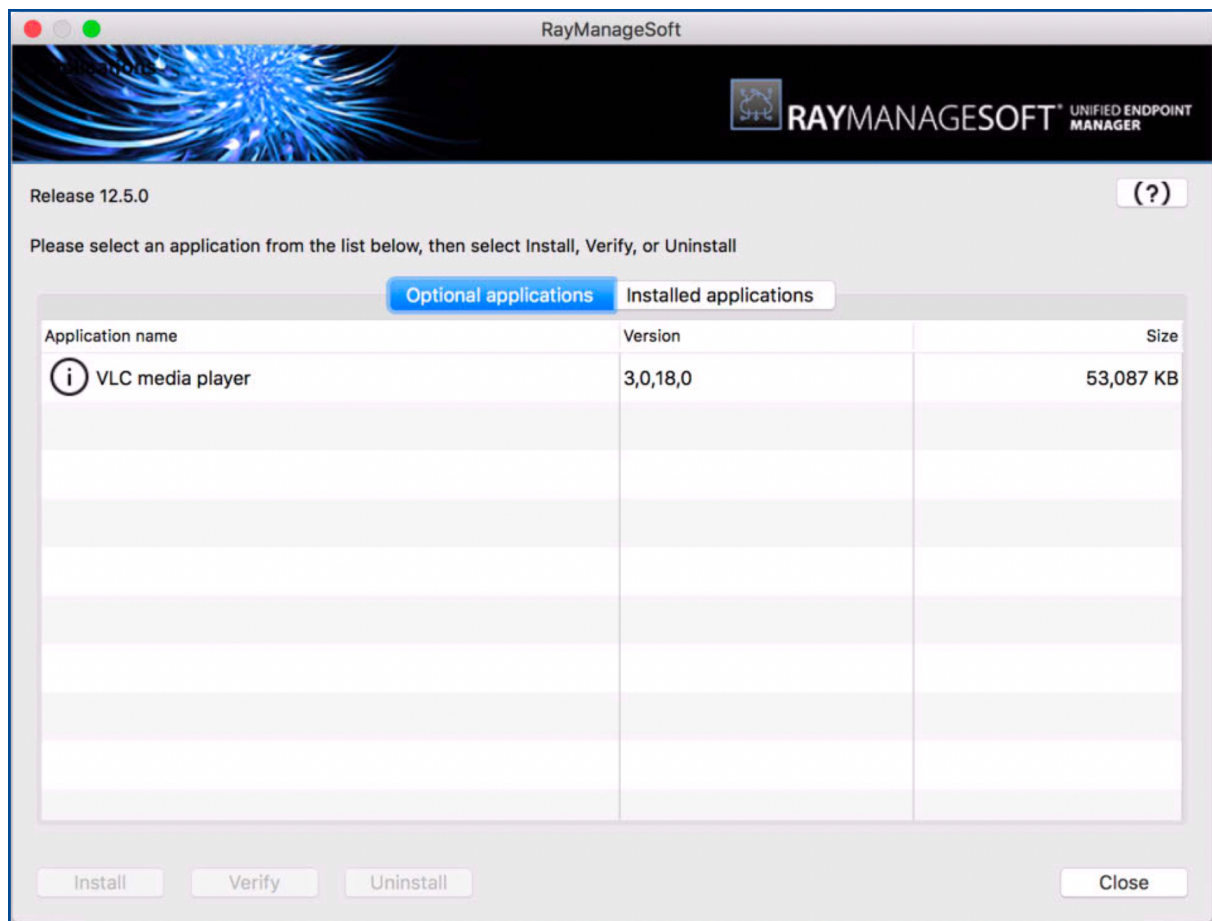
There are three buttons in the lower left corner.

- [Install button](#)
- [Verify button](#)
- [Uninstall button](#)

If the buttons are active or inactive depends on the selected tab.

Optional Applications

In the **Optional applications** tab, all packages that are optional for the device are shown.



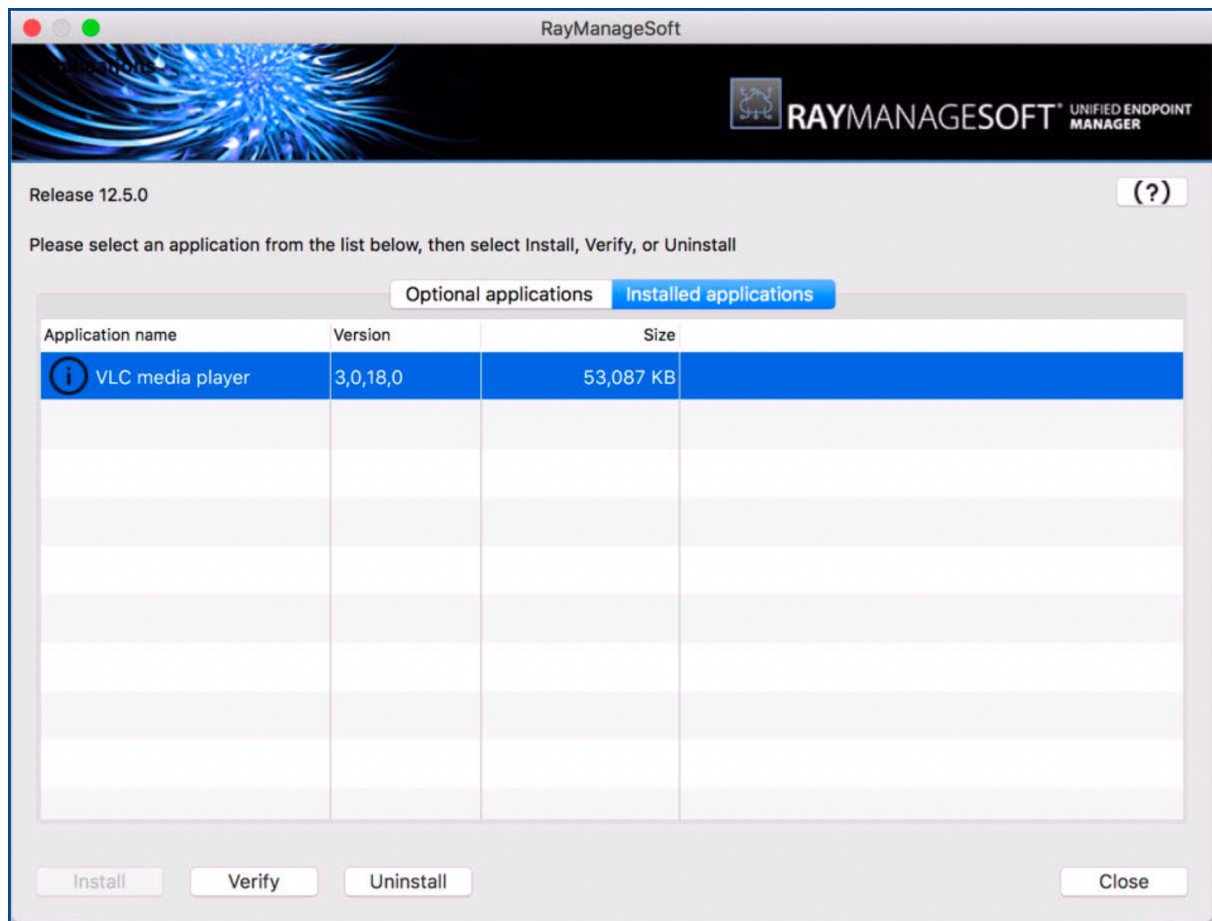
The following options are available in this tab:

Install

A selected optional package that has not yet been installed can be installed using the **Install** button.

Installed Applications

In the **Installed applications** tab, all packages that have been installed on the device are shown.



The following options are available in this tab:

Verify

The **Verify** button can be used in order to compare the selected package on the client with the package in RayManageSoft Unified Endpoint Manager. If the packages vary, the package on the client can be updated.

Uninstall

The **Uninstall** button can be used to uninstall the selected package from the client.

MGSPolicyUpdate.app

The `MGSPolicyUpdate.app` does not have a GUI. Manually executing the `MGSPolicyUpdate.app` will trigger a policy update.

It is not necessary to manually trigger a policy update as scheduled policy updates will occur on



a regular basis.

Uninstall the MacOS Agent

1. Open the Terminal application and use the following command to uninstall the MacOS agent:

```
sudo bash /opt/managesoft/bin/uninstall-managesoft.command
```

2. When asked enter the password of the administrator account used for the client.

3. When asked to proceed answer with **yes**.

4. Confirm the uninstallation of the MacOS agent by typing **yes**.

5. The MacOS agent will now be uninstalled.

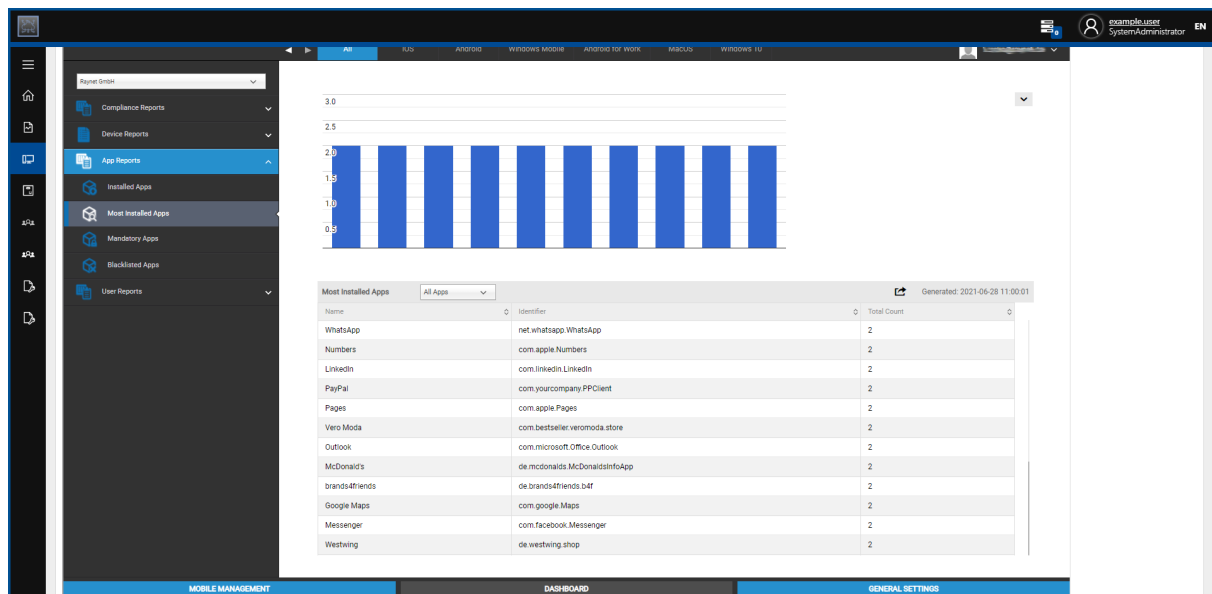


Note:

This will only remove the MacOS agent. The settings will be saved for later use. The can still be found in the `/var/opt/managesoft/` folder. In order to also remove the settings, they must be deleted manually.

Mobile Devices

In order to use this option, RayMobile needs to be configured for usage with RayManageSoft Unified Endpoint Manager. If the RayMobile integration has been configured, this page will show the information about the mobile devices received from the integration. More information on already configured integrations and on how to add an integration can be found in the [Integrations](#) chapter.



In the upper right corner of the page there are three symbols which can be used in order to configure the view.



The three buttons can be used to configure the **Console Width** that will be used by the integration. The following values can be configured.

- : Sets the **Console Width** to 1280 pixels. This is the default setting.
- : Sets the **Console Width** to 1440 pixels.
- : Sets the **Console Width** to 1600 pixels.

More information on how to work with RayMobile and how to configure it can be found in the *Administration Manual*

In order to download the *Administration Manual* execute the following steps:

1. Login to RayMobile.
2. Select the **General Settings** tab by clicking on the tab located on the right of the bottom bar of the RayMobile instance.
3. Select the **Account Overview** tab by clicking on the tab located at the top of the sidebar on the left side of the RayMobile Instance.
4. Select the **Manuals & FAQ** tab by clicking on the tab in the top bar of the RayMobile instance.
5. Download the *Administration Manual* by clicking on the **Click here** button located next to the entry for the manual.



Applications

The **Applications** section is used to manage and deploy software to the endpoints.

Name	Status	Type	Display name	Version	Manufacturer
MacOS Packages					
Firefox	OK	Apple	Firefox	108.0.2.0	mozilla
JDK 8 Update 351	OK	Apple	JDK 8 Update 351	1.8.351.10	oracle
Third-party Packages					
7-Zip	OK	Windows	7-Zip	22.0.0.0	Igor Pavlov
Microsoft .NET 6.0.8 - Windows Server HostingProductVersion6.0.8.22363DVarFile	OK	Windows	Microsoft .NET 6.0.8 - Windows Server HostingProductVersion6.0.8.22363DVarFile	6.0.8.22363	Microsoft Corporation
Microsoft Sql Server Installer	OK	Windows	Microsoft Sql Server Installer	15.2204.5490.2	Microsoft Corporation
Windows Packages					
Raynet GmbH					
RayEval	OK	Windows	RayEval	7.2.2280.2378	Raynet GmbH
RayPack	OK	Windows	RayPack	7.2.6639.3437	Raynet GmbH
7-Zip 22.00 x64 edition	OK	Windows	7-Zip 22.00 (x64 edition)	22.0.0.0	Igor Pavlov
VLC media player	OK	Apple	VLC media player	3.0.18.0	videolan

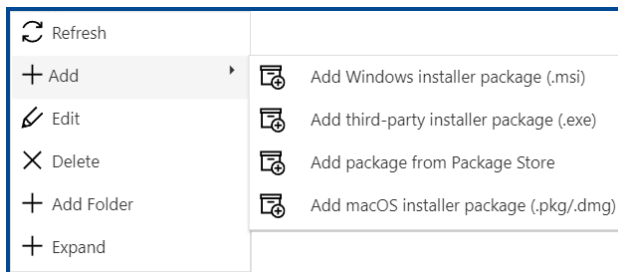
The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the screen can be used to refresh the view.
- **Add** - The **Add** button on the top left of the screen can be used to add a package. For more information see [Add a Package](#).
- **Edit** - The **Edit** button on the top left of the screen can be used to edit a package if one package in the list has been selected. For more information see [Edit a Package](#).
- **Delete** - The **Delete** button on the top left of the screen can be used to delete one or more packages if one or more packages in the list have been selected.
- **Add Folder** - The **Add Folder** button can be used to add a new folder to the folder view. For more information see [Add a Folder](#).
- **Folder View / List View** - The **Folder View / List View** button can be found on the top right of the screen. It is used to switch between the [List View](#) and the [Folder View](#) and changes its name depending on the selected view.
- **Advanced filter** - The **Advanced filter** is available on the top right of the screen. A description on how to use the **Advanced filters** can be found in the [Using Sorting, Filter, and Search Options](#) section.
- **Search field** - The **Search** field can be found on the top right of the screen. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.

The packages are divided into Windows installer and Third-party installer. The status informs about the packaging status of the package. It is possible to click on the name of a package in order to get to the **Package Details**. This only works if the package is in the **OK** status.



When clicking on a folder or a package, a context menu will be opened. This context menu is available in both views.



The following options are available in the context menu:

- **Refresh:** Can be used to refresh the page.
- **Add:** Can be used to add a package to RayManageSoft Unified Endpoint Manager.
 - Add Windows installer package (.msi): Choose this option to add an .msi package.
 - Add third-party installer package (.exe): Choose this option to add an .exe package.
 - Add package from the Package Store: Choose this option to add a package from the Package Store.
 - Add macOS installer package (.pkg/.dmg): Choose this option to add a macOS package.
- **Edit:** Choose this option to edit the selected package or folder.
- **Delete:** Choose this option to delete the selected package or folder.
- **Add Folder:** Choose this option to add a new folder.
- **Expand:** Choose this option to expand the folders in the **Folder View**.

The following chapters are available in this section:

- [List View](#)
- [Folder View](#)
- [Package Details](#)
- [Add a Package](#)
- [Edit a Package](#)



List View

In the List View the packages that are available in the library are shown as list.

The screenshot shows the 'List View' of the application library. At the top, there are navigation buttons: Refresh, Add, Edit, Delete, and Add Folder. On the right, there are tabs for 'Folder View' and 'Advanced filter', and a search bar labeled 'Type to search...'. The main area is titled 'APPLICATIONS' and contains a table with the following columns: Status, Type, Name, Display name, Version, and Manufacturer. The first row is highlighted, showing '7-Zip' with a status of 'Available' (green dot) and a type of 'Application' (EXE icon). Other rows include 'Microsoft Sql Server Installer', 'Microsoft .NET 6.0.8 - Windows Server Hosting', 'Firefox', 'VLC media player', 'JDK 8 Update 351', 'RayPack', 'RayEval', and '7-Zip 22.00 x64 edition'.

Status	Type	Name	Display name	Version	Manufacturer
Available	Application	7-Zip	7-Zip	22.0.0.0	Igor Pavlov
Available	Application	Microsoft Sql Server Installer	Microsoft Sql Server Installer	15.2204.5490.2	Microsoft Corporation
Not Available	Application	Microsoft .NET 6.0.8 - Windows Server HostingProductVersion6.0.8.22363DVarFileInfo	Microsoft .NET 6.0.8 - Windows Server Hosting-CPProductVersion6.0.8.22363DVarFileInfo	6.0.8.22363	Microsoft CorporationD:\FileDescriptionM
Available	Application	Firefox	Firefox	108.0.2.0	mozilla
Available	Application	VLC media player	VLC media player	3.0.18.0	videolan
Available	Application	JDK 8 Update 351	JDK 8 Update 351	1.8.351.10	oracle
Available	Application	RayPack	RayPack	7.2.6639.3437	Raynet GmbH
Available	Application	RayEval	RayEval	7.2.2280.2378	Raynet GmbH
Available	Application	7-Zip 22.00 x64 edition	7-Zip 22.00 (x64 edition)	22.0.0.0	Igor Pavlov

Entries per page: 15

Use the different filter options, order options, and search options to narrow down the list of applications. In order to select one or more specific packages, mark the packages by clicking in the circle in front of the package. Selected packages are highlighted and have a checkmark in the circle.

Folder View

In the Folder View it is possible to create a tree structure of folders in which the packages can be stored.

The screenshot shows the 'Folder View' of the application library. At the top, there are navigation buttons: Refresh, Add, Edit, Delete, and Add Folder. On the right, there are tabs for 'List View' and 'Advanced filter', and a search bar labeled 'Type to search...'. The main area is titled 'APPLICATIONS' and shows a tree structure of folders. The folders are 'MacOS Packages', 'Third-party Packages', and 'Windows Packages'. Under 'MacOS Packages', there are two sub-folders: 'Firefox' and 'JDK 8 Update 351'. Under 'Third-party Packages', there are no sub-folders. Under 'Windows Packages', there are no sub-folders. The 'Firefox' and 'JDK 8 Update 351' sub-folders are expanded, showing their contents in a table with columns: Name, Status, Type, Display name, Version, and Manufacturer.

Name	Status	Type	Display name	Version	Manufacturer
Firefox	Available	Application	Firefox	108.0.2.0	mozilla
JDK 8 Update 351	Available	Application	JDK 8 Update 351	1.8.351.10	oracle

Existing packages and folders can be ordered by using the drag and drop functionality.

- [Add a folder](#)
- [Delete a folder](#)

Add a Folder

In order to add a new folder to the **Folder View**, click on the **Add Folder** button on the top left of the view.



APPLICATIONS					
☐ Name	Status	Type	Display name	Version	Manufacturer
☐ MacOS Packages					
☐ Third-party Packages					
☐ Windows Packages					
☐ RayEval	●	Windows	RayEval	7.2.2280.2378	Raynet GmbH
☐ RayPack	●	Windows	RayPack	7.2.6639.3437	Raynet GmbH

Clicking on the button will open the **Add Folder** dialogue.

Add Folder

FOLDER NAME: *

Example Folder

PARENT FOLDER:

Windows Packages

IMAGE

Add

Discard

Enter a name for the folder into the **FOLDER NAME** field. This is the only mandatory option in this dialogue.

If the folder should be part of a folder hierarchy, it is possible to enter the parent folder in the **PARENT FOLDER** field. The **PARENT FOLDER** field supports auto-completion and it is possible to select the parent folder from the list of possible entries that will be shown. This field is optional.

Furthermore it is possible to add a custom image to the folder by clicking on the image below the **PARENT FOLDER** field. A file browser will be opened. Browse for an image file to customize the image used for the report (the following file formats are supported: .gif, .jpg/.jpeg, and .png). Adding an image is optional.

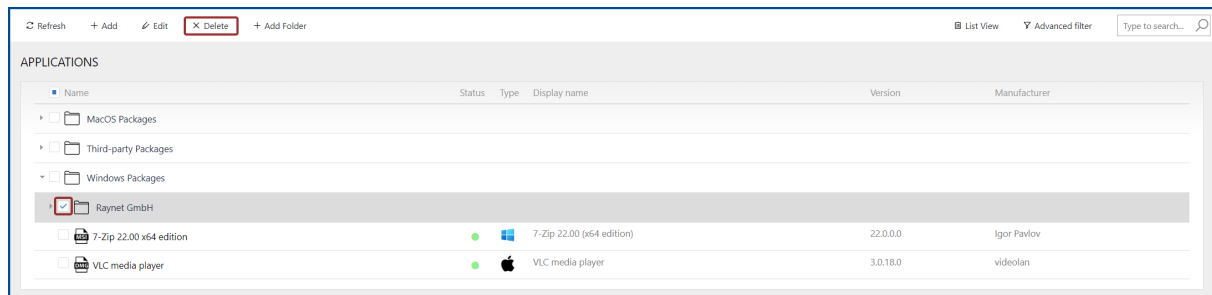
After finishing all entries the folder can be created by clicking on the **Add** button.

Delete a Folder

In order to delete one or more folders in the Folder View, it is necessary to first mark the folders that are to be deleted by clicking into the checkbox in front of the folder. Marked folders will



show a checkmark in the box. Once all folders are marked, click on the Delete button located on the top left of the view.



WARNING
The content of the folder will also be deleted! If the content of the folder should be kept, move it to another folder!

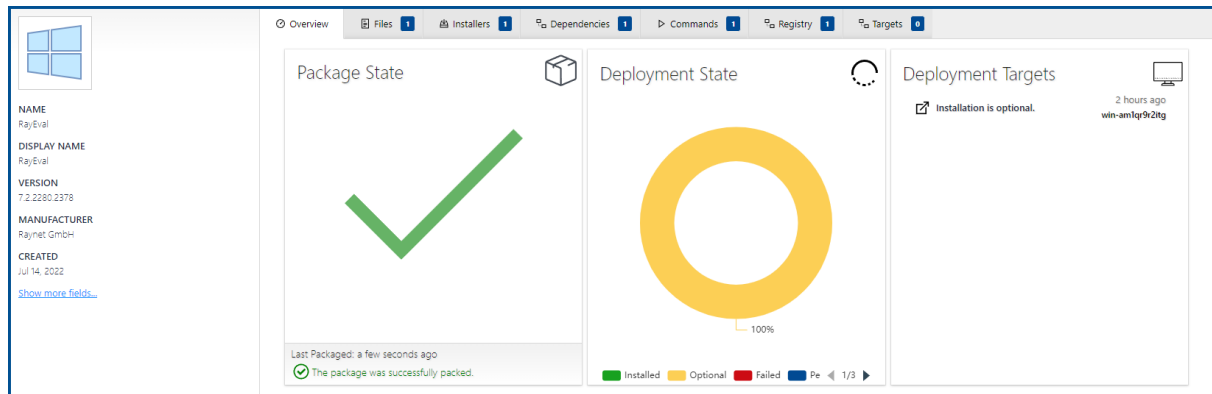
Package Details

The **Package Details** page shows information about the specific package. On the left side of the page it shows **Name**, **Display Name**, **Version**, **Manufacturer**, **Created** (date the package has been created), **Release Website**, **Support Website**, and **Customer Contact** for the specific package. Furthermore, the icon on top shows the type of the package (.msi, .exe, .pkg, .dmg) or if it is a package from the Package Store. On the right side of the page, the content is divided into different tabs. It contains the following tabs.

- [Overview](#)
- [Files](#)
- [Installers](#)
- [Dependencies](#)
- [Commands](#)
- [Registry](#)
- [Targets](#)
- [Show options](#)

Overview

The **Overview** tab shows general information about the package.

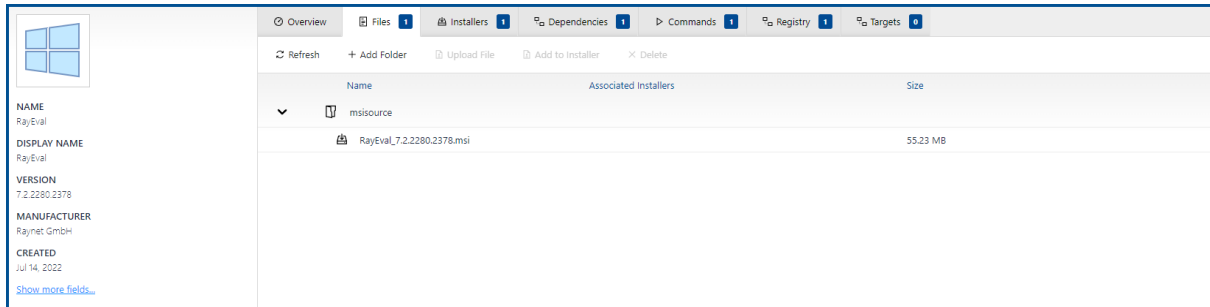


- **Packaging State:** This part of the tab shows the current state of the packaging for this package. If an error during packaging occurred, more detailed information about what happened can be found here. Furthermore, the date of the last packaging attempt is shown here.
- **Deployment State:** This part of the tab shows the progress of the deployment for the package. When calculating the progress, different states of deployment can be excluded by clicking on their color-coding located below the chart.
- **Deployment Targets:** This is a list of the devices on which the package is being installed. It shows the date, the devices name, and if the installation is optional or mandatory. Selecting a device will lead to the **Device Details** page of the device.



Files

The **Files** tab shows a list of the files that are included into the package and their folder structure.

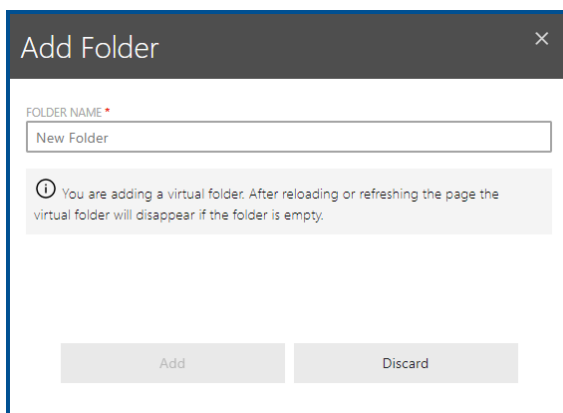


The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the tab can be used to refresh the view.
- **Add Folder** - The **Add Folder** button on the top left of the tab can be used to add a folder to the structure. The folder will be added to the currently selected location. If no folder is selected, it will be added next to an already existing folder. If a folder is being selected, it will be added as a subfolder of the selected folder.
- **Upload File** - The **Upload File** button can be used to upload a file into a selected folder. If no folder is selected, the option is not available.
- **Add to Installer** - The **Add to Installer** button can be used to add a file to an existing installer. The option is only available if a file is selected.
- **Delete** - The **Delete** button can be used to delete a selected entry. If a folder is deleted, all files located inside of the folder will be deleted.

Add Folder

The **Add Folder** dialog is used to add a folder to the folder structure of a package.

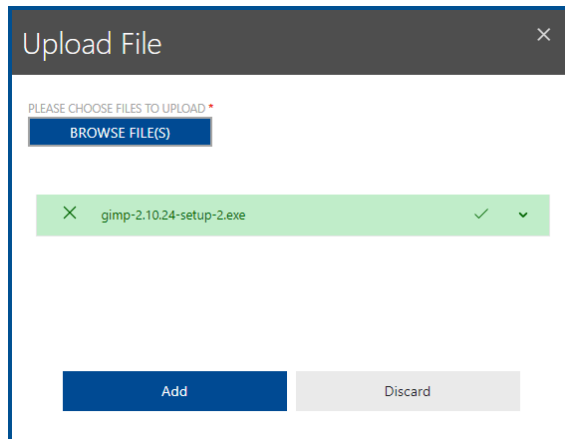


FOLDER NAME is the only available field and it is also mandatory. The field needs to contain the name of the new folder. By default, the name is set to "New Folder". The field cannot be empty.



Upload File

The **Upload File** dialog is used to upload a new file to a package.



The **BROWSE FILE(S)** button is used to open the file browser of the logged in user. Search for the file to be added and select it in the browser. It will then be added to the dialog.

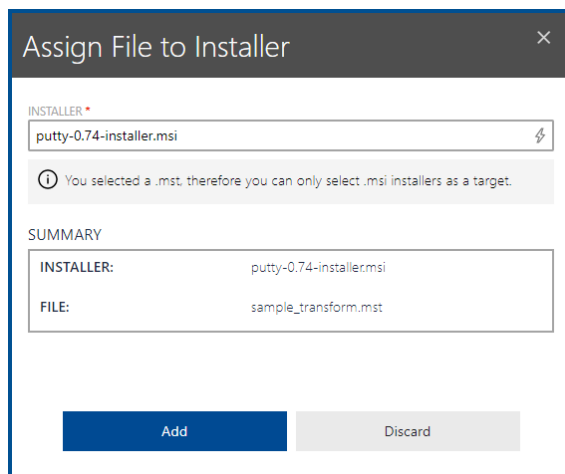
It is possible to upload more than one file at once by either using the **BROWSE FILE(S)** button more than once or by selecting more than one file in the browser.

To delete a file from the list of files to upload, click on the **X** button located left of the file name. The file will be removed from the list.

When the file selection is finished, the files can be added by clicking the **Add** button.

Add to Installer

The **Assign File to Installer** dialog can be used to add a file to an installer.



In order to select a valid target for the file, the **INSTALLER** dropdown menu can be used. The

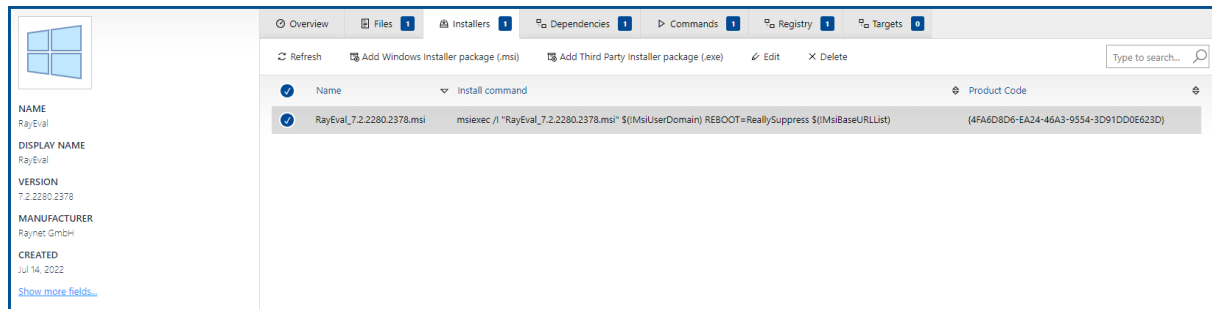


dropdown menu will only show valid targets for the selected file. It is mandatory to choose a target for the file. If no valid target for a file is available, abort the action by clicking on the **Discard** button.



Installers

The **Installers** tab shows information about the installers that are included in the package.



The following actions are available in this tab.

- **Refresh** - The **Refresh** button on the top left of the tab can be used to refresh the view.
- **Add Windows Installer** - The **Add Windows Installer** button on the top left of the tab can be used to add a Windows installer to the package. For more information see [Add a Windows Installer](#). This option is not available for MacOS packages.
- **Add Third Party Installer (. exe)** - The **Add Third Party** button on the top left of the tab can be used to add a third party installer to the package. For more information see [Add a Third Party Installer](#). This option is not available for MacOS packages.
- **Edit** - The **Edit** button on the top left of the tab can be used to edit an installer if one installer in the list has been selected. For more information see [Edit an Installer](#).
- **Delete** - The **Delete** button on the top left of the tab can be used to delete one or more installers if one or more installers in the list have been selected. This option is not available for MacOS packages.

Add a Windows Installer

The **Add Installer** dialog for Windows installers is divided into two tabs.

- [MSI](#): This tab is used to add further installers to the package.
- [Transforms](#): This tab is used to include transforms to the installer that is being added.

MSI

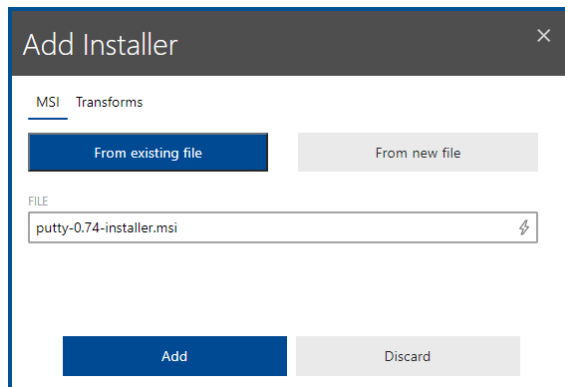
The **MSI** tab of the **Add Installer** dialog for Windows installers is further divided into two sub-tabs.

- [From existing file](#): Is used to add an already existing installer to the package.
- [From new file](#): Is used to add an installer that is not yet available in RayManageSoft Unified Endpoint Manager.



From Existing File

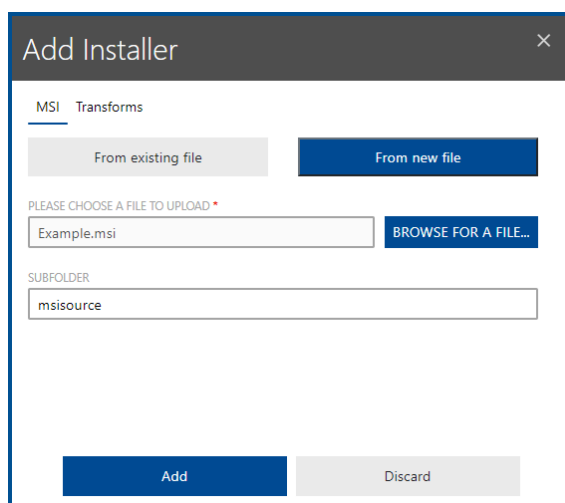
This tab of the dialog can be used to add an installer that already exists in RayManageSoft Unified Endpoint Manager to the package.



When clicking into the **FILE** field a list of the available installers will be shown and the target installer can be selected from the list. When the installer has been selected, it can either be added to the package by clicking on the **Add** button or it is possible to add **Transforms** to the installer by selecting the Transforms tab before adding the installer.

From New File

This tab of the dialog can be used to add an installer that does not yet exist in RayManageSoft Unified Endpoint Manager to the package.



A file to upload to RayManageSoft Unified Endpoint Manager and add to the package can be selected by clicking on the **BROWSE FOR A FILE...** button in order to open the file browser. Select the target file in the browser.

Furthermore, it is possible to specify a subfolder to which to add the file. The folder name needs



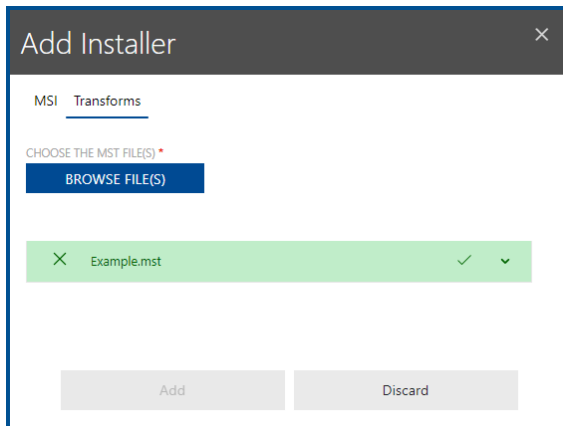
to be added to the **SUBFOLDER** field. By default, the subfolder is called "msisource".

When the installer has been selected, it can either be added to the package by clicking on the **Add** button or it is possible to add **Transforms** to the installer by selecting the Transforms tab before adding the installer.



Transforms

The **Transforms** tab is used to add one or more transforms to the selected installer.



The **BROWSE FILE(S)** button is used to open the file browser of the logged in user. Search for the transform to be added and select it in the browser. It will then be added to the dialog.

It is possible to upload more than one transform at once by either using the **BROWSE FILE(S)** button more than once or by selecting more than one transform in the browser.

To delete a transform from the list of transforms to upload, click on the **X** button located left of the file name. The transform will be removed from the list.

When the selection of transforms is finished and if the installer has been selected the transforms and the installer can be added by clicking the **Add** button.



Be aware:

Any property changed by the MST are not considered during the creation of the package.

MSTs should not contain changes of basic properties such as product code, upgrade code, or version. If an MST contains changes of basic properties, it will be necessary to manually adjust the version of the package.

Add a Third Party Installer

The **Add Installer** dialog for third party installer is divided into four tabs.

- [General](#): This tab is used to add an installer.
- [Files](#): This tab shows all files that will be added together with the installer. Furthermore, if there are multiple installers, it can be used to define the selected installer.
- [Detection](#): This tab is used to configure values for the installer that can be used by RayManageSoft Unified Endpoint Manager to detect if the application is installed.
- [Advanced](#): This tab is used for additional information.



General

In the **General** tab, it is possible to either add one `.exe` file by clicking on the **Add file(s)** button, or to add a complete folder with all its content by clicking on the **Add Folder** button. If the **Add Folder** option is chosen, supporting non-installer files that are in the folder will also be added to the package.

After files or a folder have been added, the following information is shown and can be edited:

- **SELECTED INSTALLER FILE:** Shows the installer file that has been chosen. If a folder has been uploaded and the folder contains more than one `.exe` file, the first (in alphabetic order) `.exe` file will automatically be chosen as selected file. This value can be changed by selecting another file while in the **Files** tab.
- **INSTALL COMMAND:** Can be used to add command-line arguments that will be used for the installation of the application.
- **UNINSTALL COMMAND:** Enter a command to uninstall the package into the **UNINSTALL COMMAND** field. The command should be an exact match of the command that would be entered into the command-line of the operating system. If using environment variables to define an uninstall command, the variables need to be used in a specific way. For example, if the `%temp%` variable should be part of the command, it needs to be used as `$ (TEMP) .`



The following table is a list of variables that can be used.

Variable	Usage	Default Path
%SystemDrive%	\$(SystemDrive)	C:\ (The operating system drive)
%SystemRoot%	\$(SystemRoot)	C:\Windows
%WINDIR%	\$(WINDIR)	C:\Windows
%HOMEDRIVE%	\$(HOMEDRIVE)	C:\ (The operating system drive)
%HOMEPATH%	\$(HOMEPATH)	C:\Users\<username>
%USERPROFILE%	\$(USERPROFILE)	C:\Users\<username>
%APPDATA%	\$(APPDATA)	C:\Users\<username>\AppData\Roaming
%ALLUSERSPROFILE%	\$(ALLUSERSPROFILE)	C:\ProgramData
%PROGRAMFILES%	\$(PROGRAMFILES)	C:\Program Files
%PROGRAMFILES(x86)%	\$(PROGRAMFILES(x86)	C:\Program Files (x86)
%PROGRAMDATA%	\$(PROGRAMDATA)	C:\ProgramData
%TEMP%	\$(TEMP)	C:\Users\<Username>\AppData\Local\Tem
%LOCALAPPDATA%	\$(LOCALAPPDATA)	C:\Users\<Username>\AppData\Local
%PUBLIC%	\$(PUBLIC)	C:\Users\Public
%COMMONPROGRAMFILE	\$(COMMONPROGRAMFIL	C:\Program Files\Common Files
%COMMONPROGRAMFILE	\$(%COMMONPROGRAMFI	C:\Program Files (x86)\Common Files

Files

In the **Files** tab, the files and folders contained in the package are available.



Add Installer

General Files Detection Advanced

▼	📁	thirdparty	✕
▼	📁	EXE	✕
	📄	7z2200-x64.exe	☑ ✕
	📄	gimp-2.10.32-setup-1.exe	📄 ✕
	📄	Supporting File Example.txt	✕

Add

Discard

If there are multiple installer in the package, it is possible to switch the installer files by clicking on the icon next to it. The selected installer file is marked by the ☑ icon. All other installers are marked by the 📄 icon.



Folders and files in this view can be deleted by clicking on the ✕ icon located behind the item.



Be aware:

Deleting a folder will also delete all subfolders and packages contained in the folder from the package.

Detection

In the **Detection** tab, it is possible to define information that can be used by RayManageSoft Unified Endpoint Manager in order to detect if the application is already installed on a device.

Add Installer

General

Files

Detection

Advanced

Branding

KEY

NAME

VALUE

The key, name, and value fields are used to specify a registry entry that can be used to determine whether or not this application is already installed.

If you leave detection information empty, the installation agent will invoke the installation multiple times.

Uninstall Key

UNINSTALL REGISTRY KEY NAME

Enter the registry key that can be used to uninstall a previous or current version of this application from the managed device. This key is under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall in the registry.

Add

Discard

The following information can be specified.



- **KEY:** In the **Key** field, the key of the registry hive (below `HKEY_LOCAL_MACHINE`) and the key name of a registry key that can be used to determine whether or not the package is already installed can be specified. For example, if the registry key is in `HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\AdobeAcrobat\6.0\Installer` the entry in the **KEY** field should be `SOFTWARE\Adobe\Adobe Acrobat\6.0\Installer`.
- **NAME:** In the **Name** field, the name of a registry entry that is used in conjunction with the contents of the **KEY** field in order to determine whether or not the package is already installed should be entered. If the name of the registry entry set by the application installation is `Default`, the field is left empty.
- **VALUE:** In the **Value** field, the value that is used in conjunction with the contents of the **KEY** and the **NAME** field in order to determine whether or not the package is already installed should be entered. An example value would be `"C:\Program Files\Adobe\Acrobat 6.0\Acrobat"`.
- **Uninstall Key:** This field should contain the registry key that is used to uninstall the package. The uninstall registry key usually matches the GUID of the application set in curly brackets. An example value would be `{2453DBC8-ACC4-4711-BD03-0C15353AA3D8}`. It is not necessary to enter the whole path, the uninstall registry key is sufficient. It does not matter if the key will have to be in the 32-bit or the 64-bit section of the registry. This will be managed automatically. The key can generally be found in the registry under `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`.

Advanced

In the **Advanced** tab additional information for the package can be configured.

Add Installer [X]

General Files Detection Advanced

IMAGE



SUBFOLDER

thirdparty

Add Discard

The following information can be specified.



- **IMAGE:** Upload a customized image for the application (the following file formats are supported: .gif, .jpg, .jpeg, and .png).
- **SUBFOLDER:** Specifies the folder to which the application is added. By default, the name of the folder is "thirdparty".

Edit an Installer

The **Edit Installer** dialog differs depending on the selected installer. It can be divided into the following sections.

- [Edit a Windows installer](#): The **Edit Installer** dialog for Windows installers is described in this section.
- [Edit a Third Party installer](#): The **Edit Installer** dialog for third party installers is described in this section.
- [Edit a MacOS installer](#): The **Edit Installer** dialog for MacOS installers is described in this section.



Edit a Windows Installer

The **Edit Installer** dialog for Windows installers can be used to change the commands and keys used by the installer. The default values are read from the installer itself.

Edit Installer

General

NAME *

putty-0.74-installer.msi

INSTALL COMMAND *

msiexec /I \"putty-0.74-installer.msi\" \$(MsiUserDomain) REBOOT=ReallySupp

UNINSTALL COMMAND

msiexec /x {8F276E88-8C75-43AF-A245-7112AE5AF2DA} REBOOT=ReallySupp

REPAIR COMMAND

msiexec /I \"{8F276E88-8C75-43AF-A245-7112AE5AF2DA}\" REINSTALLMODE

PRODUCT CODE

{8F276E88-8C75-43AF-A245-7112AE5AF2DA}

UNINSTALL KEY

{8F276E88-8C75-43AF-A245-7112AE5AF2DA}

UPGRADE CODE

DCE70C63-8808-4646-B168-A677BD298385

DIRECTORY

Save changes Discard

- **NAME:** This is the name of the installer file.
- **INSTALL COMMAND:** This field contains the command that is used to install the application. The command matches the command that would be used if entered into the command-line interface of the operating system.
- **UNINSTALL COMMAND:** This field contains the command that is used to uninstall the application. The command matches the command that would be used if entered into the command-line interface of the operating system.
- **REPAIR COMMAND:** This field contains the command that is used to repair the application. The command matches the command that would be used if entered into the command-line interface of the operating system.
- **PRODUCT CODE:** This is the product code of the application.
- **UNINSTALL KEY:** This field contains the uninstall registry key of the application. The uninstall key usually matches the product code of the application in curly brackets.
- **UPGRADE CODE:** This is the upgrade code of the application.
- **DIRECTORY:** This is the directory in which the installer is located in the package.



Edit a Third Party Installer

The **Edit Installer** dialog for third party installers consists of two different tabs.

- [General](#)
- [Detection](#)



General

In the **General** tab of the **Edit Installer** dialog for third party installers the basic commands for the installer can be configured.

The following commands can be specified in the **General** tab.

- **INSTALL COMMAND:** This field can be edited in order to specify how to install the application and pass the appropriate command-line arguments to the application. By default, it contains the name of the file without further command-line arguments. An example would be `readerdc_de_xa_crd_install.exe` for a German version of the Adobe Acrobat Reader.
- **UNINSTALL COMMAND:** Enter a command to uninstall the package into the **UNINSTALL COMMAND** field. The command should be an exact match of the command that would be entered into the command-line interface of the operating system. If using environment variables, to define an uninstall command, the variables need to be used in a specific way. For example, if the `%temp%` variable should be part of the command. It needs to be used as `$(TEMP)`.

The following table is a list of variables that can be used.

Variable	Usage	Default Path
%SystemDrive%	\$(SystemDrive)	C:\ (The operating system drive)
%SystemRoot%	\$(SystemRoot)	C:\Windows
%WINDIR%	\$(WINDIR)	C:\Windows



Variable	Usage	Default Path
%HOMEDRIVE%	\$ (HOMEDRIVE)	c:\ (The operating system drive)
%HOMEPATH%	\$ (HOMEPATH)	C:\Users\<username>
%USERPROFILE%	\$ (USERPROFILE)	C:\Users\<username>
%APPDATA%	\$ (APPDATA)	C:\Users\<username>\AppData\Roaming
%ALLUSERSPROFILE%	\$ (ALLUSERSPROFILE)	C:\ProgramData
%PROGRAMFILES%	\$ (PROGRAMFILES)	C:\Program Files
%PROGRAMFILES (x86)	\$ (PROGRAMFILES (x86)	C:\Program Files (x86)
%PROGRAMDATA%	\$ (PROGRAMDATA)	C:\ProgramData
%TEMP%	\$ (TEMP)	C:\Users\<Username>\AppData\Local\Tem
%LOCALAPPDATA%	\$ (LOCALAPPDATA)	C:\Users\<Username>\AppData\Local
%PUBLIC%	\$ (PUBLIC)	C:\Users\Public
%COMMONPROGRAMFILE	\$ (COMMONPROGRAMFIL	C:\Program Files\Common Files
%COMMONPROGRAMFILE	\$ (%COMMONPROGRAMFI	C:\Program Files (x86)\Common Files

Detection

In the **Detection** tab of the **Edit installer** dialog for third party installers it is possible to define information that can be used by RayManageSoft Unified Endpoint Manager in order to detect if the application is already installed on a device.



Edit Installer

General Detection

Branding

KEY

NAME

VALUE

The key, name, and value fields are used to specify a registry entry that can be used to determine whether or not this application is already installed.

Uninstall Key

UNINSTALL REGISTRY KEY NAME

Enter the registry key that can be used to uninstall a previous or current version of this application from the managed device. This key is under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall in the registry.

Save changes

Discard

The following information can be specified.

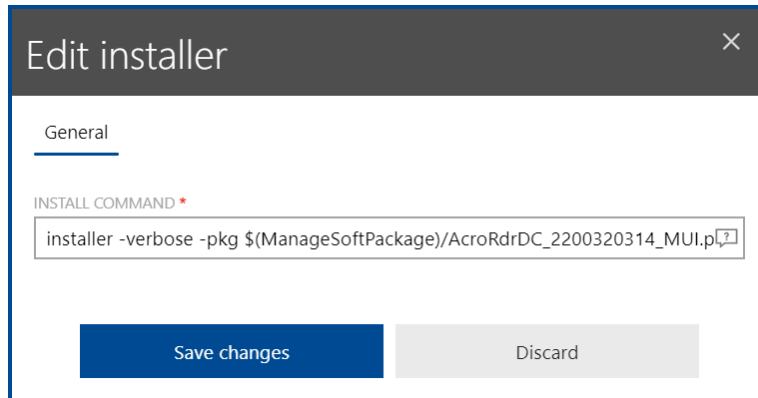
- **KEY:** In the **Key** field , the key of the registry hive (below `HKEY_LOCAL_MACHINE`) and the key name of a registry key that can be used to determine whether or not the package is already installed can be specified. For example, if the registry key is in `HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\AdobeAcrobat\6.0\Installer` the entry in the **KEY** field should be `SOFTWARE\Adobe\Adobe Acrobat\6.0\Installer`.
- **NAME:** In the **Name** field, the name of a registry entry that is used in conjunction with the contents of the **KEY** field in order to determine whether or not the package is already installed should be entered. If the name of the registry entry set by the application install is `Default`, the field is left empty.
- **VALUE:** In the **Value** field, the value that is used in conjunction with the contents of the **KEY** and the **NAME** field in order to determine whether or not the package is already installed should be entered. An example value would be `"C:\Program Files\Adobe\Acrobat 6.0\Acrobat"`.
- **UNINSTALL KEY:** This field should contain the registry key that is used to uninstall the package. The uninstall registry key usually matches the GUID of the application set in curly brackets. An



example value would be {2453DBC8-ACC4-4711-BD03-0C15353AA3D8}. It is not necessary to enter the whole path, the uninstall registry key is sufficient. It does not matter if the key will have to be in the 32-bit or the 64-bit section of the registry. This will be managed automatically.

Edit a MacOS Installer

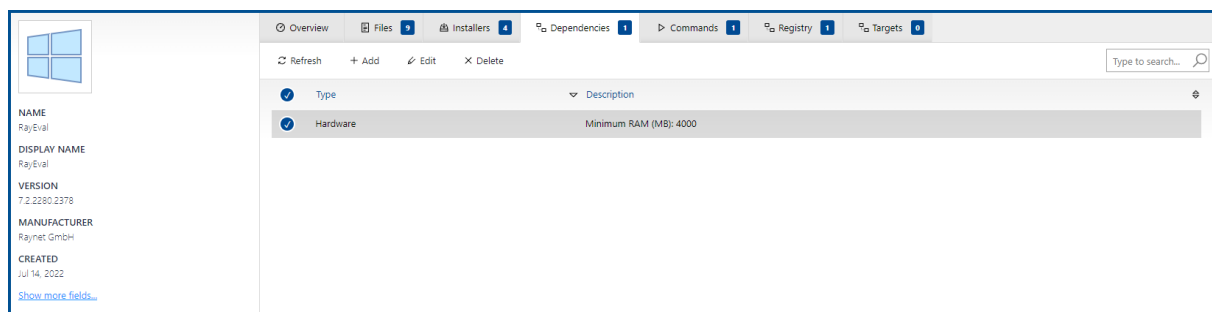
The **Edit Installer** dialog for MacOS installers can be used to change the commands used by the installer. The default values are read from the installer itself.



- **INSTALL COMMAND:** This field contains the command that is used to install the application. The command matches the command that would be used if entered into the command-line interface of the operating system.

Dependencies

In the **Dependencies** tab an overview of the dependencies for a package can be found. In order to apply a package, these dependencies must be fulfilled for the managed device.



There are different types of dependencies for which RayManageSoft Unified Endpoint Manager will check and which can be chosen for a dependency when either adding or editing it.

The following actions are available in this tab.

- **Refresh** - The **Refresh** button on the top left of the list can be used to refresh the view.



- **Add** - The **Add** button on the top left of the list can be used to add a dependency. For more information see [Add a Dependency](#).
- **Edit** - The **Edit** button on the top left of the list can be used to edit a dependency if one dependency in the list has been selected. For more information see [Edit a Dependency](#).
- **Delete** - The **Delete** button on the top left of the list can be used to delete one or more dependencies if one or more dependencies in the list have been selected.
- **Search field** - The **Search** field can be found on the top right of the screen. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.

Add a Dependency

A dependency can be added by using the **Add** button in the **Dependencies** tab. The **Add Dependency** dialog will open.

In the **Add Dependency** dialog, the type of the dependency can be chosen by selecting one of the options in the **RULE FOR** dropdown box. The rest of the dialog will depend on the option that has been selected in this field.

The following types of dependencies are currently available in RayManageSoft Unified Endpoint Manager.

- [Managed Package](#)
- [Unmanaged Package](#)
- [Hardware Inventory](#)
- [WMI Query](#)

Managed Package

If **Managed Package** is selected in the **RULE FOR** dropdown menu, RayManageSoft Unified Endpoint Manager can be configured to install the dependency together with the package that is using the dependency.

The screenshot shows the 'Add Dependency' dialog box. It has a title bar with the text 'Add Dependency' and a close button (X). The dialog is divided into three main sections. The first section is labeled 'RULE FOR' and contains a dropdown menu with 'Managed Package' selected. The second section is labeled 'DEPENDENCY' and contains a text input field with the placeholder text 'Select a package...' and a magnifying glass icon. The third section is labeled 'RUN THE COMMANDS INCLUDED IN THIS PACKAGE' and contains an unchecked checkbox. At the bottom of the dialog are two buttons: 'Add' and 'Discard'.



In the **DEPENDENCY** field, the target package can be selected. It is possible to choose from all packages that are currently managed by RayManageSoft Unified Endpoint Manager. Simply select the target package. Check the **RUN THE COMMANDS INCLUDED IN THIS PACKAGE** checkbox located underneath the **DEPENDENCY** field to tell RayManageSoft Unified Endpoint Manager that all commands in the package shall be executed when installing the dependency.



Unmanaged Package

If **Unmanaged Package** is selected in the **RULE FOR** dropdown field, RayManageSoft Unified Endpoint Manager will check if a version of this dependency is already installed on the endpoint and then act according to the action that is selected in the **ACTION** field.

The screenshot shows a dialog box titled "Add Dependency". It contains the following fields and controls:

- RULE FOR ***: A dropdown menu with "Unmanaged Package" selected.
- ACTION ***: A dropdown menu with "Ensure this package is installed." selected.
- DEPENDENCY**: A text input field with the placeholder "Select a package..." and a magnifying glass icon.
- NAME ***: An empty text input field.
- VERSION ***: An empty text input field.
- PRODUCT CODE**: A text input field with the placeholder "Select an installer..." and a magnifying glass icon.
- At the bottom, there are two buttons: "Add" and "Discard".

The following fields can be configured if **Unmanaged Package** is selected.

- **ACTION:** This field defines the action that RayManageSoft Unified Endpoint Manager will take regarding the dependency. The following actions are available.
 - **Ensure this package is installed.** - RayManageSoft Unified Endpoint Manager will make sure that the dependency is installed on the endpoint. If it is not already installed, RayManageSoft Unified Endpoint Manager will stop the installation of the package.
 - **Stop installation if this package is installed.** - RayManageSoft Unified Endpoint Manager will check if the dependency is installed. If it is installed (no matter which version), RayManageSoft Unified Endpoint Manager will stop the installation of the package.
 - **Stop installation if version is greater than specified.** - RayManageSoft Unified Endpoint Manager will check if the dependency is installed. If it is installed (and the version number is greater than the one specified in the dependency), RayManageSoft Unified Endpoint Manager will stop the installation of the package.
 - **Stop installation if version is less than specified.** - RayManageSoft Unified Endpoint Manager will check if the dependency is installed. If it is installed (and the version number is less than the one specified in the dependency), RayManageSoft Unified Endpoint Manager will stop the installation of the package.
- **DEPENDENCY:** Select a dependency from a list of dependencies offered by RayManageSoft Unified Endpoint Manager or enter a dependency manually. If the dependency is part of the list, RayManageSoft Unified Endpoint Manager will auto-fill all information known into the other fields.
- **NAME:** The name of the dependency.
- **VERSION:** The version number of the dependency.



- **PRODUCT CODE:** The product code for the installer. If the installer is available for RayManageSoft Unified Endpoint Manager, it will read the product code from the installer. It can also be entered manually. An example for a valid product code would be {8F276E88-8C75-43AF-A245-7112AE5AF2DA}.

Hardware Inventory

If **Hardware Inventory** is selected in the **RULE FOR** field, the dependency will be linked to the hardware of the target devices.

The screenshot shows a dialog box titled "Add Dependency". It has a close button (X) in the top right corner. Inside the dialog, there are three fields: "RULE FOR" with a dropdown menu showing "Hardware Inventory", "CONDITION" with a dropdown menu showing "Required CPU type", and "VALUE" with an empty text input field. At the bottom of the dialog, there are two buttons: "Add" and "Discard".

There are two fields for hardware inventory dependencies that need to be defined. All fields in this dialog are mandatory.

- **CONDITION:** In the **CONDITION** dropdown menu, the condition which must be fulfilled is to be defined. It is possible to choose one of the following conditions.
 - **Required CPU type:** If this is chosen, the CPU type needs to be entered into the **VALUE** field.
 - **Required CPU manufacturer:** If this is chosen, the name of the manufacturer needs to be entered into the **VALUE** field. Example values would be *Intel* or *AMD*.
 - **Minimum CPU speed (MHZ):** The minimum CPU speed needed should be entered here. For example, for a 1.6 GHz CPU the entry in the **VALUE** field would be *1600*.
 - **Minimum disk space (MB):** The required disk space in MB needs to be entered into the **VALUE** field if this is the selected condition.
 - **Minimum RAM (MB):** The required RAM in MB needs to be entered into the **VALUE** field if this is the selected condition. For example, if 2 GB RAM are required for an application, the entry would be *2048*.
 - **Required CPU model:** This field is used if a specific CPU model is required for the package. An example value would be *i5-3570*.
 - **Requires a CD-ROM drive:** If this is chosen, the **VALUE** field will not be available, but the package can only be installed if a CD-ROM drive has been detected for the device.
 - **Minimum OS Service Pack:** Specify the Service Pack for an operating system that is the minimum required service pack to be installed.
- **VALUE:** **VALUE** is a mandatory field. The entry in the **VALUE** field depends on the condition selected in the **CONDITION** field.



WMI Query

It is also possible to define a Windows Management Instrumentation (WMI) query as a dependency for a package. In order to define a WMI query, select the **WMI Query** option in the **RULE FOR** dropdown field.

The screenshot shows the 'Add Dependency' dialog box. It contains the following fields and controls:

- RULE FOR:** A dropdown menu currently showing 'WMI Query'.
- HARDWARE CLASS:** A text field with the placeholder 'Select a hardware class...' and a magnifying glass icon.
- HARDWARE PROPERTY:** A text field with the placeholder 'Select a hardware property...' and a magnifying glass icon.
- CONDITIONS:** A dropdown menu showing 'Equal to', followed by an empty text input field and an 'Add' button.
- Buttons:** 'Add' (blue) and 'Discard' (grey) buttons at the bottom.

- **HARDWARE CLASS:** For example, `Win32_IDEController` for IDE & SATA controllers.
- **HARDWARE PROPERTY:** For example, `DeviceID` could be used as property for the `Win32_IDEController` class selected in the **HARDWARE CLASS** field.
- **CONDITION:** The condition of the query can be defined using the dropdown menu and the value field. The dropdown menu offers the following options:
 - **Equal to:** The result of the query must match the condition.
 - **Greater than:** The result of the query must be greater or equal to the defined condition value.
 - **Less than:** The result of the query must be less or equal to the defined condition value.
 - **Not equal to:** The result of the query must not match the defined condition value.

After selecting one of the options in the **CONDITION** dropdown box, a related value needs to be entered into the value field. For example, a value for a `DeviceID` can look like `PIC18F2520`.

For detailed information about WMI, refer to the [Microsoft Windows Management Instrumentation](#) page.

Edit a Dependency

A dependency can be added by using the **Edit** button in the **Dependencies** tab if a dependency has been selected. The **Edit Dependency** dialog for the selected dependency will open.

In the **Edit Dependency** dialog, the type of the dependency can be chosen by selecting an option in the **RULE FOR** dropdown box. The rest of the dialog will depend on the option selected in this field.

The following types of dependencies are currently available in RayManageSoft Unified Endpoint



Manager.

- [Managed Package](#)
- [Unmanaged Package](#)
- [Hardware Inventory](#)
- [WMI Query](#)

Managed Package

If **Managed Package** is selected in the **RULE FOR** dropdown menu, RayManageSoft Unified Endpoint Manager can be configured to install the dependency together with the package that is using the dependency.

Edit Dependency

RULE FOR *

Managed Package

DEPENDENCY *

Adobe Acrobat Reader DC - Deutsch

RUN THE COMMANDS INCLUDED IN THIS PACKAGE ☒

Save changes Discard

In the **DEPENDENCY** field, the target package can be selected. It is possible to choose from all packages that are currently managed by RayManageSoft Unified Endpoint Manager. Simply select the target package. Check the **RUN THE COMMANDS INCLUDED IN THIS PACKAGE** checkbox located underneath the **DEPENDENCY** field to tell RayManageSoft Unified Endpoint Manager that all commands in the package shall be executed when installing the dependency.

Unmanaged Package

If **Unmanaged Package** is selected in the **RULE FOR** dropdown field, RayManageSoft Unified Endpoint Manager will check if a version of this dependency is already installed on the endpoint and then act according to the action that is selected in the **ACTION** field.



Edit Dependency

RULE FOR *
Unmanaged Package

ACTION *
Ensure this package is installed.

DEPENDENCY
Select a package...

NAME *

VERSION *

PRODUCT CODE
Select an installer...

Save changes Discard

The following fields need to be configured if **Unmanaged Package** is selected.

- **ACTION:** This field defines the action that RayManageSoft Unified Endpoint Manager will take regarding the dependency. The following actions are available.
 - **Ensure this package is installed.** - RayManageSoft Unified Endpoint Manager will make sure that the dependency is installed on the endpoint. If it is not already installed, RayManageSoft Unified Endpoint Manager will stop the installation of the package.
 - **Stop installation if this package is installed.** - RayManageSoft Unified Endpoint Manager will check if the dependency is installed. If it is installed (no matter which version), RayManageSoft Unified Endpoint Manager will stop the installation of the package.
 - **Stop installation if version is greater than specified.** - RayManageSoft Unified Endpoint Manager will check if the dependency is installed. If it is installed (and the version number is greater than the one specified in the dependency), RayManageSoft Unified Endpoint Manager will stop the installation of the package.
 - **Stop installation if version is less than specified.** - RayManageSoft Unified Endpoint Manager will check if the dependency is installed. If it is installed (and the version number is less than the one specified in the dependency), RayManageSoft Unified Endpoint Manager will stop the installation of the package.
- **DEPENDENCY:** Select a dependency from a list of dependencies offered by RayManageSoft Unified Endpoint Manager or enter a dependency manually. If the dependency is part of the list, RayManageSoft Unified Endpoint Manager will auto-fill all information known into the other fields.
- **NAME:** The name of the dependency.
- **VERSION:** The version number of the dependency.
- **PRODUCT CODE:** The product code for the installer. If the installer is available for RayManageSoft Unified Endpoint Manager, it will read the product code from the installer. It can also be entered manually. An example for a valid product code would be {8F276E88-8C75-43AF-A245-7112AE5AF2DA}.



Hardware Inventory

If **Hardware Inventory** is selected in the **RULE FOR** field, the dependency will be linked to the hardware of the target devices.

The screenshot shows a dialog box titled "Edit Dependency". It has a close button (X) in the top right corner. Inside the dialog, there are three labeled fields, each with a red asterisk indicating it is mandatory:

- RULE FOR**: A dropdown menu currently showing "Hardware Inventory".
- CONDITION**: A dropdown menu currently showing "Required CPU type".
- VALUE**: An empty text input field.

At the bottom of the dialog, there are two buttons: "Save changes" and "Discard".

There are two fields for hardware inventory dependencies that need to be defined. All fields in this dialog are mandatory.

- **CONDITION**: In the **CONDITION** dropdown menu, the condition which must be fulfilled is to be defined. It is possible to choose one of the following conditions.
 - **Required CPU manufacturer**: If this is chosen, the name of the manufacturer needs to be entered into the **VALUE** field. Example values would be `Intel` or `AMD`.
 - **Minimum CPU speed (MHZ)**: The minimum CPU speed needed should be entered here. For example, for a 1.6 GHz CPU the entry in the **VALUE** field would be `1600`.
 - **Minimum disk space (MB)**: The required disk space in MB needs to be entered into the **VALUE** field if this is the selected condition.
 - **Minimum RAM (MB)**: The required RAM in MB needs to be entered into the **VALUE** field if this is the selected condition. For example, if 2 GB RAM are required for an application the entry would be `2048`.
 - **Required CPU model**: This field is used if a specific CPU model is required for the package. An example value would be `i5-3570`.
 - **Minimum OS Service Pack**: Specify the Service Pack for an operating system that is the minimum required service pack to be installed.
- **VALUE**: **VALUE** is a mandatory field. The entry in value depends on the condition selected in the **CONDITION** field.

WMI Query

It is also possible to define a Windows Management Instrumentation (WMI) query as a dependency for a package. In order to define a WMI query, **WMI Query** needs to be selected in the **RULE FOR** dropdown field.



Edit Dependency

RULE FOR *
Hardware Inventory

CONDITION *
Required CPU type

VALUE *

Save changes Discard

- **HARDWARE CLASS:** For example, `Win32_IDEController` for IDE & SATA controllers.
- **HARDWARE PROPERTY:** For example, `DeviceID` could be used as property for the `Win32_IDEController` class selected in the **HARDWARE CLASS** field.
- **CONDITION:** The condition of the query can be defined using the dropdown menu and the value field. The dropdown menu offers the following options:
 - **Equal to:** The result of the query must match the condition.
 - **Greater than:** The result of the query must be greater or equal to the defined condition value.
 - **Less than:** The result of the query must be less or equal to the defined condition value.
 - **Not equal to:** The result of the query must not match the defined condition value.

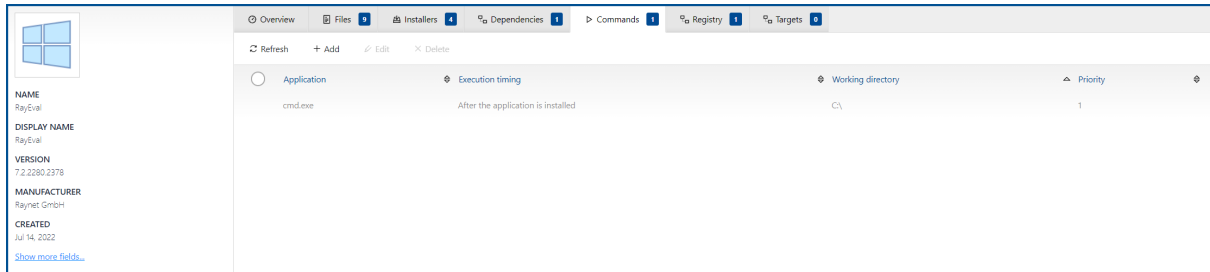
After selecting one of the options in the **CONDITION** dropdown box, a related value needs to be entered into the value field. For example, a value for a `DeviceID` can look like `PIC18F2520`.

For detailed information about WMI, refer to the [Microsoft Windows Management Instrumentation](#) page.



Commands

In the **Commands** tab an overview of the run commands of a package can be found. The run command is used to automatically start a specific application once the requirements or triggers defined in the run command are met.



The following actions are available in this tab.

- **Refresh** - The **Refresh** button on the top left of the list can be used to refresh the view.
- **Add** - The **Add** button on the top left of the list can be used to add a run command. For more information see [Add a Run Command](#).
- **Edit** - The **Edit** button on the top left of the list can be used to edit a run command if one run command in the list has been selected. For more information see [Edit a Run Command](#).
- **Delete** - The **Delete** button on the top left of the list can be used to delete one or more run commands if one or more run commands in the list have been selected.

Add a Command

A run command can be added by clicking on the **Add** button in the **Commands** tab. The **Add Run Command** dialog will open.

The **Add Run Command** dialog is divided into two different tabs. The following tabs are available:

- [Command](#)
- [Advanced](#)



Command

In the **Command** tab, the application and the timing of the run command are configured.

The following settings are available in the **Command** tab.

- **EXECUTION TIMING:** The dropdown menu can be used to configure when the command will be executed. The following options are available.
 - **After The Application Is Installed:** The run command will be executed after the application has been installed.
 - **After The Application Is Uninstalled:** The run command will be executed after the application has been uninstalled.
 - **Before The Application Is Installed:** The run command will be executed before the application is being installed.
 - **Before The Application Is Uninstalled:** The run command will be executed before the application is being uninstalled.
 - **When The Application Is Launched:** The run command will be executed when the application is launched.
- **APPLICATION TO START:** Defines the application that will be started with the run command.
- **WORKING DIRECTORY:** The field is used to define the working directory for the application.



Advanced

The **Advanced** tab contains several switches and fields that can be used to fine tune the run command.

Add run command

Command Advanced

INSTALLATION CONTEXT (SUPPORTING PLATFORM ONLY)
Current User Privileges

USER INTERFACE LEVEL
Minimal

Execute command during application self-heal
☐

Wait for the command to finish
☒

Report non-zero application error codes
☐

Add Discard

The following options are available in the **Advanced** tab.

- **INSTALLATION CONTEXT (SUPPORTING PLATFORM ONLY):** This dropdown menu can be used to select the installation context that will be used for the application.
 - **Current User Privileges:** If this option is chosen, the privileges of the current user will be used for the application.
 - **Full Access Privileges:** If this option is chosen, full access privileges will be chosen for the application.
- **USER INTERFACE LEVEL:** This dropdown menu can be used to select the user interface level for the application.
 - **Minimal:** If this option is chosen, there will only be a minimal interface available to the user.
 - **Complete:** If this option is chosen, the complete interface will be available to the user.
- **Execute command during application self-heal:** Activate to execute the command during the application self-heal. By default, the option is deactivated.
- **Wait for the command to finish:** Deactivate to continue with the processes even though the command has not yet finished. If activated, the command needs to finish before another process is started. By default, the option is activated.
- **Report non-zero application error codes:** Activate to report non-zero application error codes. If deactivated, non-zero error codes will not be reported. By default, the option is deactivated.



Edit a Command

A run command can be edited by selecting the target run command and clicking on the **Edit** button in the **Commands** tab. The **Edit Run Command** dialog will open.

The **Edit Run Command** dialog is divided into two different tabs. The following tabs are available:

- [Command](#)
- [Advanced](#)

Command

In the **Command** tab, the application and the timing of the run command are configured.

The screenshot shows the 'Edit run command' dialog box with the 'Command' tab selected. The dialog has a title bar with a close button. Inside, there are two tabs: 'Command' (active) and 'Advanced'. The 'Command' tab contains the following fields and controls:

- PRIORITY OF THIS COMMAND:** A text input field containing the value '1'.
- EXECUTION TIMING:** A dropdown menu with the selected option 'After The Application Is Installed'.
- APPLICATION TO START*:** A text input field containing 'cmd.exe'. Below this field is a grey informational box with an 'i' icon and the text 'Please specify the command line to start.'
- WORKING DIRECTORY:** An empty text input field. Below this field is a grey informational box with an 'i' icon and the text 'Specify the working directory in which to run the command line.'
- At the bottom, there are two buttons: 'Save changes' (blue) and 'Discard' (grey).

The following settings are available in the **Command** tab.

- **PRIORITY OF THIS COMMAND:** Defines the priority of the command if more than one command are scheduled for execution. Valid values for the field range from 1-99999. The lowest value represents the highest priority and the highest value represents the lowest priority.
- **EXECUTION TIMING:** The dropdown menu can be used to configure when the command will be executed. The following options are available.
 - **After The Application Is Installed:** The run command will be executed after the application has been installed.
 - **After The Application Is Uninstalled:** The run command will be executed after the



- application has been uninstalled.
- **Before The Application Is Installed:** The run command will be executed before the application is being installed.
- **Before The Application Is Uninstalled:** The run command will be executed before the application is being uninstalled.
- **When The Application Is Launched:** The run command will be executed when the application is launched.
- **APPLICATION TO START:** Defines the application that will be started with the run command.
- **WORKING DIRECTORY:** The field is used to define the working directory for the application.

Advanced

The **Advanced** tab contains several switches and fields that can be used to fine-tune the run command.

Edit run command

Command Advanced

INSTALLATION CONTEXT (SUPPORTING PLATFORM ONLY)
Current User Privileges

USER INTERFACE LEVEL
Minimal

EXECUTE COMMAND DURING APPLICATION SELF-HEAL
☐

WAIT FOR THE COMMAND TO FINISH
☒

REPORT NON-ZERO APPLICATION ERROR CODES
☐

Save changes Discard

The following options are available in the **Advanced** tab.

- **INSTALLATION CONTEXT (SUPPORTING PLATFORM ONLY):** This dropdown menu can be used to select the installation context that will be used for the application.
 - **Current User Privileges:** If this option is chosen, the privileges of the current user will be used for the application.
 - **Full Access Privileges:** If this option is chosen, full access privileges will be chosen for the application.
- **USER INTERFACE LEVEL:** This dropdown menu can be used to select the user interface level for the application.
 - **Minimal:** If this option is chosen, there will only be a minimal interface available to the user.
 - **Complete:** If this option is chosen, the complete interface will be available to the user.

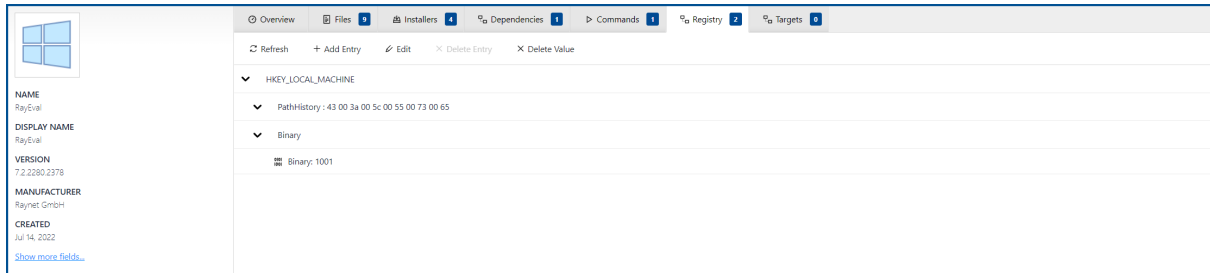


- **Execute command during application self-heal:** Activate to execute the command during the application self-heal. By default, the option is deactivated.
- **Wait for the command to finish:** Deactivate to continue with the processes even though the command has not yet finished. If activated, the command needs to finish before another process is started. By default, the option is activated.
- **Report non-zero application error codes:** Activate to report non-zero application error codes. If deactivated, non-zero error codes will not be reported. By default, the option is deactivated.



Registry

In the **Registry** tab an overview of the registry entries of the package can be found.



The following actions are available in this tab.

- **Refresh** - The **Refresh** button on the top left of the list can be used to refresh the view.
- **Add Entry** - The **Add Entry** button on the top left of the list can be used to add a registry key entry. For more information see [Add a Registry Entry](#).
- **Edit** - The **Edit** button on the top left of the list can be used to edit a registry key entry if one registry entry in the list has been selected. For more information see [Edit a Registry Entry](#).
- **Delete Entry** - The **Delete Entry** button on the top left of the list can be used to delete the selected registry entry. Deleting a registry entry will also delete all associated registry values.
- **Delete Value** - The **Delete Value** button on the top left of the list can be used to delete the selected registry value.

Add a Registry Entry

A registry entry can be added by clicking on the **Add Entry** button in the **Registry Keys** tab. The **Add Registry Entry** dialog will open.

The **Add Registry Entry** dialog is divided into two different tabs.

- [Registry Entry](#)
- [Registry Values](#)



Registry Entry

In the **Registry Entry** tab the basic information for the registry key is defined.

The following settings are available in the **Registry Entry** tab.

- **ROOT KEY:** Select the root key from the dropdown menu. The following options are available.
 - **HKEY_CLASSES_ROOT:** Select this option if the registry entry should be set for both, the HKEY_CLASSES_ROOT.
 - **HKEY_CURRENT_USER:** Select this option if the registry entry should be set in HKEY_CURRENT_USER.
 - **HKEY_LOCAL_MACHINE:** Select this option if the registry entry should be set in HKEY_LOCAL_MACHINE.
 - **HKEY_USERS:** Select this option if the registry entry should be set in HKEY_USERS.
- **KEY:** This field should contain the target key.
- **VALUE:** Can be used to define a single value for the registry entry.
- **Write only if registry entry is missing:** The checkbox can be used to define if the registry entry and its values should always be written or only if the registry entry does not exist.



Registry Values

In the **Registry Values** tab, the value or values for the specific registry key entry can be defined.

In order to add a new registry value to the registry entry, click on the **Add Registry Value** button.

After using the button to add a new value, the following options are available for the new registry value.

- **NAME:** Enter the name of the registry value into field.
- **TYPE:** This defines the type of the registry value. The following types are available.

- **Binary:** If this option is selected, the value can be binary data in any form.
- **DWORD:** If this option is selected, the value can be a 32-bit number.
- **Multi String:** If this option is selected, the value can be a sequence of null-terminated strings terminated by an empty string.



- **Expanded:** If this option is selected, the value can be an expandable string (for example an environment variable which will then be resolved to the folder path).
- **String:** If this option is selected, the value can be a null-terminated string. Depending on if Unicode or ANSI functions are used, it can either be a Unicode or an ANSI string.
- **VALUE:** This field should contain the value. This is a mandatory field. The format of the value depends on what has been selected in the **TYPE** field.
- **Write only if registry entry is missing:** The checkbox can be used to define if the registry entry and its values should always be written or only if the registry entry does not exist.

Edit a Registry Entry

A registry entry can be edited by selecting the target registry entry and clicking on the **Edit** button in the **Registry Entry** tab. The **Edit Registry Entry** dialog will open. If a registry entry has multiple registry values, select the specific value and click on the **Edit** button to edit this value only.

The **Edit Registry Entry** dialog is divided into two different tabs.

- [Registry Entry](#)
- [Registry Values](#)

Registry Entry

In the **Registry Entry** tab, the basic information for the registry key is defined.

Edit Registry Entry

Registry Entry Registry Values

ROOT KEY

HKEY_LOCAL_MACHINE

KEY*

Binary\\

VALUE

☐ Write only if registry entry is missing

Save changes Discard

The following settings are available in the **Registry Entry** tab.

- **ROOT KEY:** Select the root key from the dropdown menu. The following options are available.
 - **HKEY_CLASSES_ROOT:** Select this option if the registry entry should be set for both, the HKEY_CLASSES_ROOT.



- **HKEY_CURRENT_USER**: Select this option if the registry entry should be set in `HKEY_CURRENT_USER`.
- **HKEY_LOCAL_MACHINE**: Select this option if the registry entry should be set in `HKEY_LOCAL_MACHINE`.
- **HKEY_USERS**: Select this option if the registry entry should be set in `HKEY_USERS`.
- **KEY**: This field should contain the target key.
- **VALUE**: Can be used to define a single value for the registry entry.
- **Write only if registry entry is missing**: The checkbox can be used to define if the registry entry and its values should always be written or only if the registry entry does not exist.



Registry Values

In the **Registry Value** tab the value or values for the specific registry key entry can be defined.

Edit Registry Entry

Registry Entry Registry Values

Binary: 1001

Example: Value

NAME*

Example

TYPE

String

VALUE*

Value

☐ Write only if registry value is missing

PathHistory:

Add Registry Value

Save changes Discard

In order to add a new registry value to the registry entry, click on the **Add Registry Value** button.

After using the button to add a new value, the following options are available for the new registry value.

- **NAME:** Enter the name of the registry value into field.
- **TYPE:** This defines the type of the registry value. The following types are available.

TYPE

Binary

Binary

DWORD

Expanded

Multi String

String

- **Binary:** If this option is selected, the value can be binary data in any form.
- **DWORD:** If this option is selected, the value can be a 32-bit number.
- **Multi String:** If this option is selected, the value can be a sequence of null-terminated strings terminated by an empty string.



- **Expanded:** If this option is selected, the value can be an expandable string (for example an environment variable which will then be resolved to the folder path).
- **String:** If this option is selected, the value can be a null-terminated string. Depending on if Unicode or ANSI functions are used, it can either be a Unicode or an ANSI string.
- **VALUE:** This field should contain the value. This is a mandatory field. The format of the value depends on what has been selected in the **TYPE** field.
- **Write only if registry entry is missing:** The checkbox can be used to define if the registry entry and its values should always be written or only if the registry entry does not exist.

Targets

The **Targets** tab varies depending on the type of the selected package.

- [Target tab for Windows packages](#)
- [Target tab for MacOS packages](#)

Targets for Windows Packages

In the **Targets** tab the valid targets for a package can be defined.

The screenshot displays the 'Targets' tab for a Windows package. The sidebar on the left contains the following information:

- NAME:** .NET Runtime-6.0.8-x64
- DISPLAY NAME:** .NET Runtime 6.0.8 for 64-bit
- VERSION:** 6.0.8.0
- MANUFACTURER:** Microsoft
- CREATED:** Oct 28, 2022
- [Show more fields...](#)

The main content area is divided into four subcategories:

- Supported desktop systems:** Includes radio buttons for 'No desktops' and 'Only these desktops'. A range is selected from 'Windows 2000' to 'Windows 11 (22H1)'.
- Supported server systems:** Includes radio buttons for 'No servers' and 'Only these servers'.
- Supported languages:** Includes radio buttons for 'All languages', 'Only these languages', and 'All except these languages'.
- Supported architectures:** Includes radio buttons for 'All architectures', 'Only these architectures', and 'All except these architectures'.

The **Targets** tab is divided into four subcategories which can be used to define the valid targets for the package.

- [Supported Desktop Systems](#)
- [Supported Server Systems](#)
- [Supported Languages](#)
- [Supported Architectures](#)



Supported Desktop Systems

The **Supported Desktop Systems** option can either be set to **No desktops** or to **Only these systems**. If the only these systems option is chosen, it is necessary to choose the desktop OS that are supported on a "from ... to" basis.



Be aware:

Only server systems or desktop systems can be set to **No system**. At least one has to have a range selected.

When clicking into the **from** or into the **to** field, a list of available choices will be shown. If an OS has been selected in the **from** field, only this OS or newer OS will be available for selection in the **to** field. If an OS has been selected in the **to** field, only this OS or older OS will be available for selection in the **from** field. The following desktop OS systems are available:

- Windows NT 4.0
- Windows 2000
- Windows XP
- Windows Vista
- Windows Vista (SP1)
- Windows Vista (SP2)
- Windows Vista (SP2 U1)
- Windows 7
- Windows 7 (SP1)
- Windows 8
- Windows 8.1
- Windows 10 (1507)
- Windows 10 (1511)
- Windows 10 (1607)
- Windows 10 (1703)
- Windows 10 (1709)
- Windows 10 (1803)
- Windows 10 (1809)
- Windows 10 (1903)
- Windows 10 (1909)
- Windows 10 (2004)
- Windows 10 (20H2)
- Windows 10 (21H1)
- Windows 10 (21H2)
- Windows 10 (22H2)
- Windows 11 (21H2)
- Windows 11 (22H2)



Supported Server Systems

The **Supported Server Systems** option can either be set to **No system** or to **Only these systems**. If the only these systems option is chosen, it is necessary to choose the server OS that are supported on a "from ... to" basis.



Be aware:

Only server systems or desktop systems can be set to **No system**. At least one has to have a range selected.

When clicking into the **from** or into the **to** field, a list of available choices will be shown. If an OS has been selected in the **from** field, only this OS or newer OS will be available for selection in the **to** field. If an OS has been selected in the **to** field, only this OS or older OS will be available for selection in the **from** field. The following desktop OS systems are available:

- Windows Server 4.0 TS
- Windows Server 4.0
- Windows Server 2000 TS
- Windows Server 2000
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 (SP1)
- Windows Server 2008 (SP2)
- Windows Server 2008 (SP2 U1)
- Windows Server 2008 R2
- Windows Server 2008 R2 (SP1)
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Supported Languages

The **Supported Languages** option can either be set to **All languages** (default), **Only these languages** (the checked languages are valid), or **All except these languages** (the checked languages will be omitted).



Supported Languages

☐ All languages
☒ Only these languages
☐ All except these languages

+ Add Language

GERMAN POLISH SWEDISH ENGLISH

When **Only these languages** or **All except these languages** is chosen, the **+ Add Language** button will become visible. Click on the button to open the **Add Target Language** dialog. Use the checkboxes in the dialog to add all relevant languages to the list. Those languages that have been checked will later be shown underneath the option. In order to delete a language from the list, hover over the language and click on the small **x** button that will be shown.

Add Target Language

Search...

	Language
☐	Portugese (Portugal)
☐	Chinese (Traditional)
☐	Norwegian (Nynorsk)
☐	Hungarian
☐	Arabic
☐	Thai
☐	German
☐	Chinese (Simplified)
☐	Chinese (Hong Kong)
☐	Danisch
☐	Greek
☐	Hebrew
☐	Turkish
☐	Polish
☐	French
☐	Russian
☐	Dutch
☐	Italian
☐	Slovakian
☐	Swedish
☐	Portugese (Brasil)
☐	English
☐	Slovenian

Add Discard



The following languages are available in the **Add Target Language** dialog:

- Portugese (Portugal)
- Chinese (Traditional)
- Norwegian (Nynorsk)
- Hungarian
- Arabic
- Thai
- German
- Chinese (Simplified)
- Chinese (Hong Kong)
- Danisch
- Greek
- Hebrew
- Turkish
- Polish
- French
- Russian
- Dutch
- Italian
- Slovakian
- Swedish
- Portugese (Brazil)
- English
- Slovenian
- Spanish
- Finnish
- Japanese
- Korean
- Czech



Supported Architectures

The **Supported Architectures** option can either be set to **All architectures** (default), **Only these architectures** (the checked architectures are valid), or **All except these architectures** (the checked architectures will be omitted).



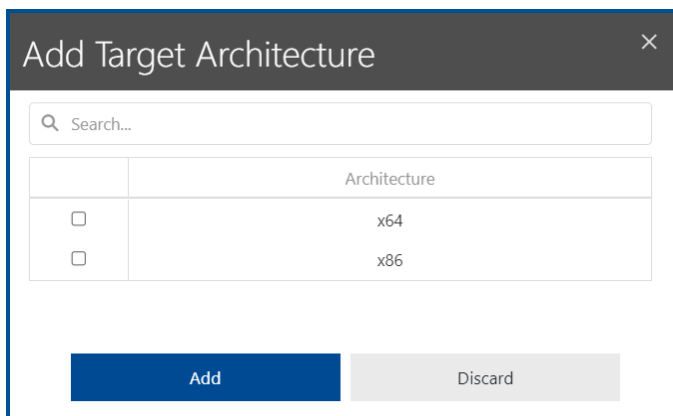
Supported Architectures

☐ All architectures
☒ Only these architectures
☐ All except these architectures

+ Add Architecture

X64 X86

When **Only these architectures** or **All except these architectures** is chosen, the **+ Add Architectures** button will become visible. Click on the button to open the **Add Target Architectures** dialog. Use the checkboxes in the dialog to add all relevant architectures to the list. Those architectures that have been checked will later be shown underneath the option. In order to delete an architecture from the list, hover over the architecture and click on the small **x** button that will be shown.



Add Target Architecture

Search...

	Architecture
☐	x64
☐	x86

Add Discard

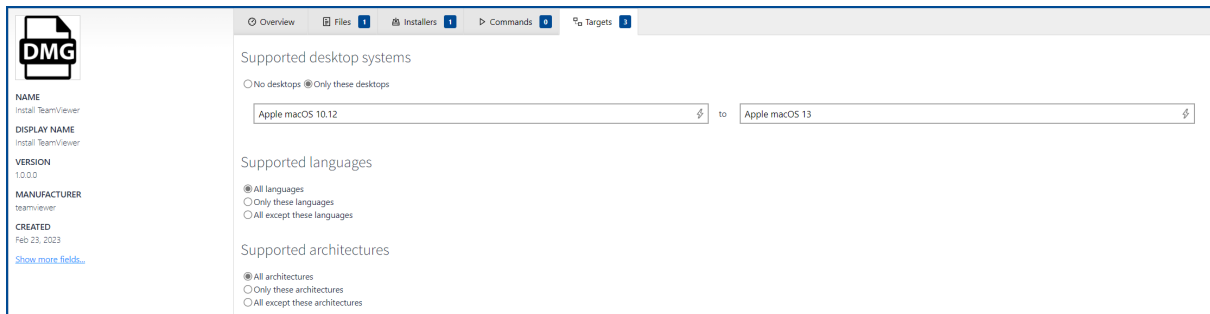
The following architectures are available in the **Add Target Architecture** dialog:

- x64
- x86



Targets for MacOS Packages

In the **Targets** tab the valid targets for a package can be defined.

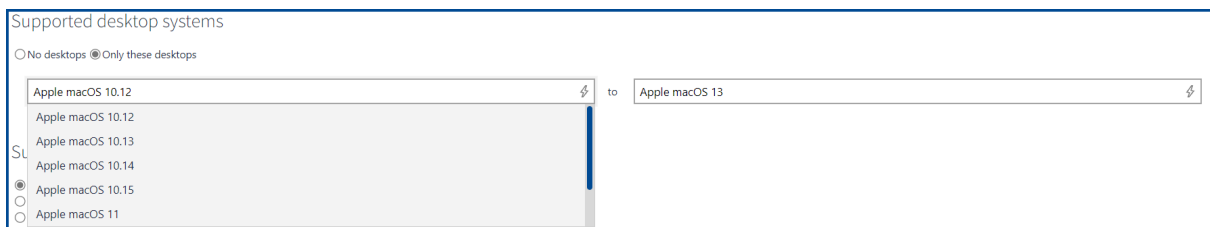


The **Targets** tab is divided into four subcategories which can be used to define the valid targets for the package.

- [Supported Desktop Systems](#)
- [Supported Languages](#)
- [Supported Architectures](#)

Supported Desktop Systems

For the **Supported Desktop Systems** option it is necessary to choose the desktop OS that are supported on a "from ... to" basis.



When clicking into the **from** or into the **to** field, a list of available choices will be shown. If an OS has been selected in the **from** field, only this OS or newer OS will be available for selection in the **to** field. If an OS has been selected in the **to** field, only this OS or older OS will be available for selection in the **from** field. The following desktop OS systems are available:

- Apple Mac OS 10.12
- Apple Mac OS 10.13
- Apple Mac OS 10.14
- Apple Mac OS 10.15
- Apple Mac OS 11
- Apple Mac OS 12
- Apple Mac OS 13



Supported Languages

The **Supported Languages** option can either be set to **All languages** (default), **Only these languages** (the checked languages are valid), or **All except these languages** (the checked languages will be omitted).

Supported Languages

☐ All languages

☒ Only these languages

☐ All except these languages

+ Add Language

GERMAN POLISH SWEDISH ENGLISH

When **Only these languages** or **All except these languages** is chosen, the **+ Add Language** button will become visible. Click on the button to open the **Add Target Language** dialog. Use the checkboxes in the dialog to add all relevant languages to the list. Those languages that have been checked will later be shown underneath the option. In order to delete a language from the list, hover over the language and click on the small **x** button that will be shown.



Add Target Language

Search...

	Language
☐	Portugese (Portugal)
☐	Chinese (Traditional)
☐	Norwegian (Nynorsk)
☐	Hungarian
☐	Arabic
☐	Thai
☐	German
☐	Chinese (Simplified)
☐	Chinese (Hong Kong)
☐	Danisch
☐	Greek
☐	Hebrew
☐	Turkish
☐	Polish
☐	French
☐	Russian
☐	Dutch
☐	Italian
☐	Slovakian
☐	Swedish
☐	Portugese (Brasil)
☐	English
☐	Slovenian

Add

Discard

The following languages are available in the **Add Target Language** dialog:

- Portugese (Portugal)
- Chinese (Traditional)
- Norwegian (Nynorsk)
- Hungarian
- Arabic
- Thai
- German
- Chinese (Simplified)
- Chinese (Hong Kong)
- French
- Russian
- Dutch
- Italian
- Slovakian
- Swedish
- Portugese (Brazil)
- English
- Slovenian



- Danish
- Greek
- Hebrew
- Turkish
- Polish
- Spanish
- Finnish
- Japanese
- Korean
- Czech

Supported Architectures

The **Supported Architectures** option can either be set to **All architectures** (default), **Only these architectures** (the checked architectures are valid), or **All except these architectures** (the checked architectures will be omitted).



Supported Architectures

☐ All architectures

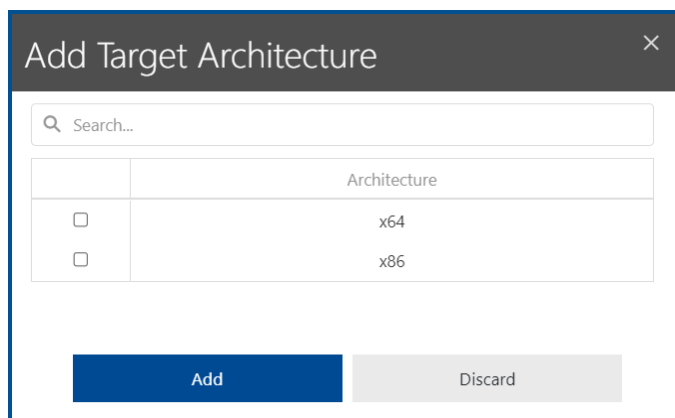
☒ Only these architectures

☐ All except these architectures

+ Add Architecture

X64 X86

When **Only these architectures** or **All except these architectures** is chosen, the **+ Add Architectures** button will become visible. Click on the button to open the **Add Target Architectures** dialog. Use the checkboxes in the dialog to add all relevant architectures to the list. Those architectures that have been checked will later be shown underneath the option. In order to delete an architecture from the list, hover over the architecture and click on the small **x** button that will be shown.



Add Target Architecture

Search...

	Architecture
☐	x64
☐	x86

Add Discard

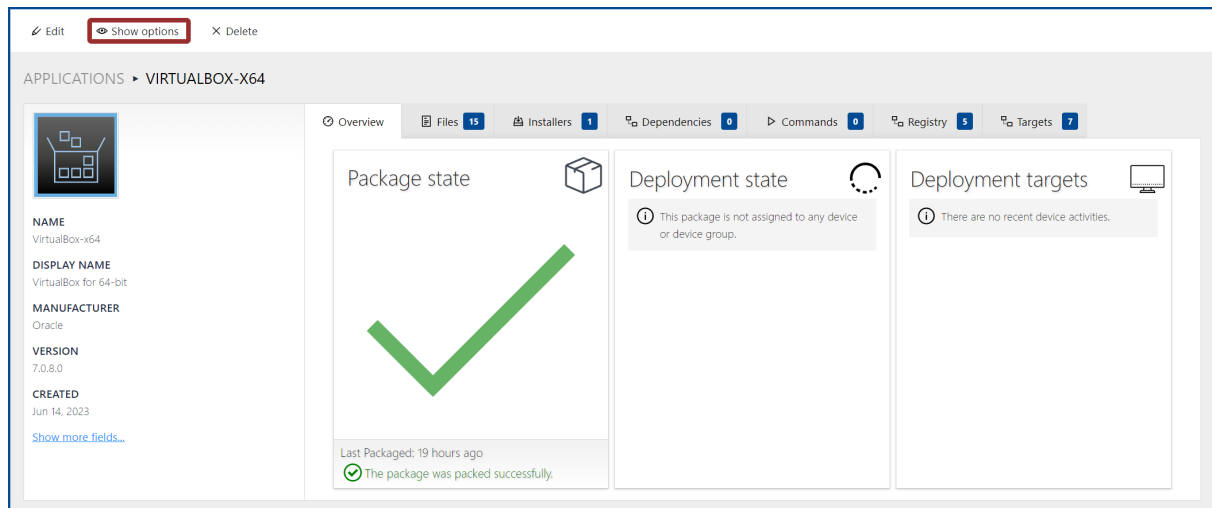
The following architectures are available in the **Add Target Architecture** dialog:

- x64
- x86



Show Options

The **Show options** button on the top left of the **Package Details** can be used to view the Package Store options for Package Store packages. This option is only available for Package Store packages.



Clicking on the button will open the **Package options** dialog. The dialog is divided into the **Package Store options** tab and the **Advanced Package Store options** tab.



Package options

Package Store options

Advanced Package Store options

Configurable options

INSTALL FOR ALL USERS

SUPPRESS REBOOTS

DISABLE ADD/REMOVE PROGRAMS INTERACTION

PREVENT DOWNGRADE

Standard application features

SUPPORT SILENT INSTALLATION

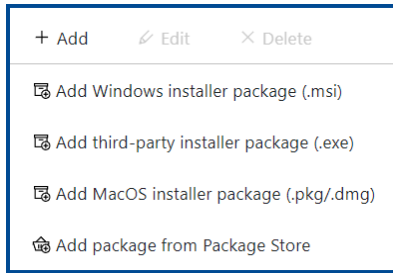
SUPPORT SILENT UNINSTALLATION

Close

In the tabs the options that have been configured for the package will be shown. The options shown depend on the specific package. This dialog is view-only. The **Package Store options** and the **Advanced Package Store options** are defined when downloading the package from the Package Store. More information about adding a package from the Package Store can be found [here](#).

Add a Package

The **Add** button in the **Applications** section of RayManageSoft Unified Endpoint Manager can be used to add packages to the **Applications** section.



The following options are available for the **Add** button.

- **Add Windows installer package (.msi)** - The **Add Windows installer package (.msi)** option is used to add a new Windows installer package to the packages available in RayManageSoft Unified Endpoint Manager. For more information on how to add a Windows installer package refer to the [Add a Windows Installer Package](#) section.
- **Add Third Party installer package (.exe)** - The **Add Third Party installer package (.exe)** option is used to add a new third-party installer package to the packages available in RayManageSoft Unified Endpoint Manager. For more information on how to add a third-party installer package refer to the [Add a Third Party Installer Package](#) section.
- **Add MacOS installer package (.pkg/.dmg)** - The **Add MacOS installer package (.pkg/.dmg)** option is used to add a new MacOS installer package to the packages available in RayManageSoft Unified Endpoint Manager. For more information on how to add a MacOS installer package refer to the [Add a MacOS Installer Package](#) section.
- **Add package from Package Store** - The **Add package from Package Store** option is used to add a new package from the Package Store. For more information on how to add a package using the Package Store refer to the [Add a Package from the Package Store](#) section.



Be aware:

Do not close the web page while uploading files! Any progress will be lost. While a package is being uploaded, the progress is shown in the **Task List**.



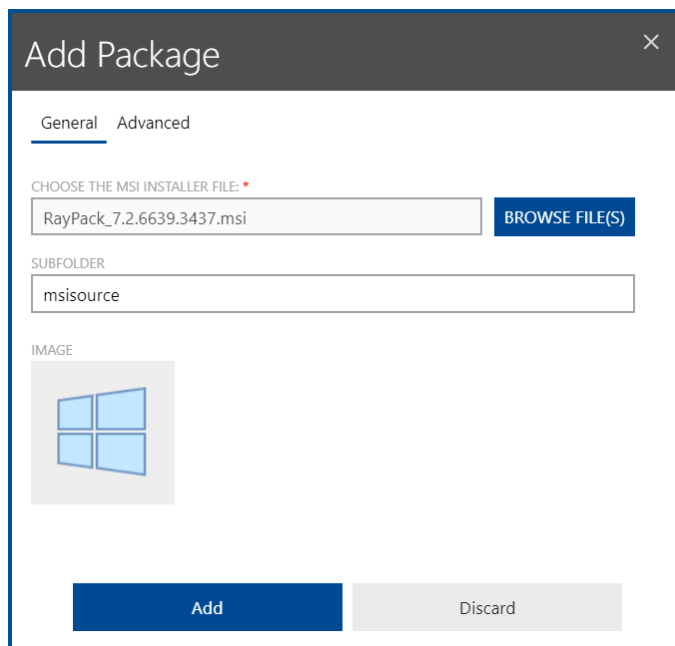
Add a Windows Installer Package

The **Add Package** dialog for Windows installers is divided into two tabs.

- [General](#): This tab is used to add an installer file to the package.
- [Advanced](#): This tab is used to include transforms for the installer that is being added to the package.

General

This tab of the dialog can be used to add a package to RayManageSoft Unified Endpoint Manager.



A file to upload to RayManageSoft Unified Endpoint Manager and add to the package can be selected by clicking on the **BROWSE FILE(S)** button in order to open the file browser. Select the target file in the browser.

Furthermore, it is possible to specify a folder to which to add the file. The folder name needs to be added to the **SUBFOLDER** field. By default, the subfolder used is called **msisource**.

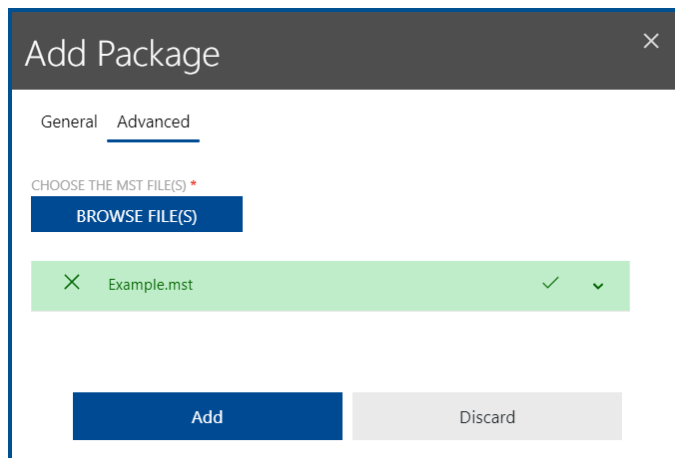
Clicking on the Image button will also open a file browser. It is possible to add a custom image to a package by opening an image from the browser (the following file formats are supported: .gif, .jpg, .jpeg, and .png).

When the installer has been selected, it can either be added to the package by clicking on the **Add** button or it is possible to add transforms to the installer by selecting the **Advanced** tab.



Advanced

The **Advanced** tab is used to add one or more transforms to the selected package.



The **BROWSE FILE(S)** button is used to open the file browser for the logged in user. Search for the transform to be added and select it in the browser. It will then be added to the dialog.

It is possible to upload more than one transform at once by either using the **BROWSE FILE(S)** button more than once or by selecting more than one transform in the browser.

To delete a transform from the list of transforms to upload, click on the **X** button located left of the file name. The transform will be removed from the list.

When the selection of transforms is finished and if the installer has been selected, the transforms and the installer can be added by clicking the **Add** button.



Be aware:

Any property changed by the MST are not considered during the creation of the package.

MSTs should not contain changes of basic properties such as product code, upgrade code, or version. If an MST contains changes of basic properties, it will be necessary to manually adjust the version of the package.

Add a Third Party Installer Package

The **Add Package** dialog for third party installer is divided into four tabs.

- [General](#): This tab is used to add an installer.
- [Files](#): This tab shows all files that will be added to the package. Furthermore, if there are multiple installers, it can be used to define the selected installer for the package.
- [Detection](#): This tab is used to configure values for the installer that can be used by RayManageSoft Unified Endpoint Manager to detect if the application is already installed.



- [Advanced](#): This tab is used for additional information.



General

In the **General** tab it is possible to either add one `.exe` file by clicking on the **Add file(s)** button or to add a complete folder with all its content by clicking on the **Add Folder** button. If the **Add Folder** option is chosen, supporting non-installer files that are in the folder will also be added to the package.

After files or a folder have been added, the following information is shown and can be edited:

- **SELECTED INSTALLER FILE:** Shows the installer file that has been chosen. If a folder has been uploaded and the folder contains more than one `.exe` file, the first (in alphabetic order) `.exe` file will automatically be chosen as selected file. This value can be changed by selecting another file while in the **Files** tab.
- **INSTALL COMMAND:** Can be used to add command-line arguments that will be used for the installation of the application.
- **UNINSTALL COMMAND:** Enter a command to uninstall the package into the **UNINSTALL COMMAND** field. The command should be an exact match of the command that would be entered into the command-line of the operating system. If using environment variables, to define an uninstall command, the variables need to be used in a specific way. For example, if the `%temp%` variable should be part of the command, it needs to be used as `$ (TEMP) .`



Be aware:

The type of the installer (`.exe`) is automatically identified in the background. Additionally, an install and an uninstall parameter will be suggested. Nevertheless, these parameters are only a suggestion and should always be verified and be adapted to the current need. Depending on the installer, parameters can vary. Always verify the suggested parameters by checking the manufacturer page of the package (For example: the parameter for a silent installation can be `/s` for one installer and `/silent` for another installer).

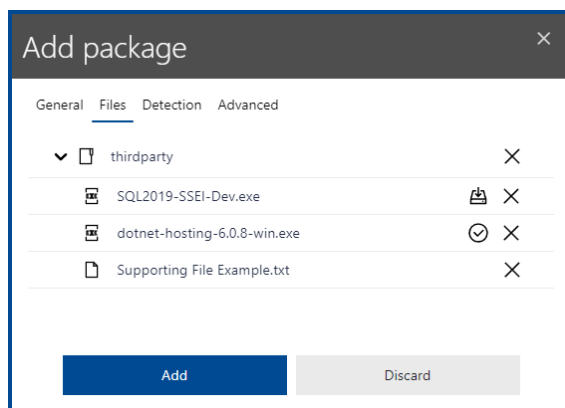


The following table is a list of example variables that can be used.

Variable	Usage	Default Path
%SystemDrive%	\$(SystemDrive)	C:\ (The operating system drive)
%SystemRoot%	\$(SystemRoot)	C:\Windows
%WINDIR%	\$(WINDIR)	C:\Windows
%HOMEDRIVE%	\$(HOMEDRIVE)	C:\ (The operating system drive)
%HOMEPATH%	\$(HOMEPATH)	C:\Users\<username>
%USERPROFILE%	\$(USERPROFILE)	C:\Users\<username>
%APPDATA%	\$(APPDATA)	C:\Users\<username>\AppData\Roaming
%ALLUSERSPROFILE%	\$(ALLUSERSPROFILE)	C:\ProgramData
%PROGRAMFILES%	\$(PROGRAMFILES)	C:\Program Files
%PROGRAMFILES(x86)%	\$(PROGRAMFILES(x86)	C:\Program Files (x86)
%PROGRAMDATA%	\$(PROGRAMDATA)	C:\ProgramData
%TEMP%	\$(TEMP)	C:\Users\<Username>\AppData\Local\Tem
%LOCALAPPDATA%	\$(LOCALAPPDATA)	C:\Users\<Username>\AppData\Local
%PUBLIC%	\$(PUBLIC)	C:\Users\Public
%COMMONPROGRAMFILE	\$(COMMONPROGRAMFIL	C:\Program Files\Common Files
%COMMONPROGRAMFILE	\$(%COMMONPROGRAMFI	C:\Program Files (x86)\Common Files

Files

In the **Files** tab the files and folders contained in the package are available.



If there are multiple installer in the package, it is possible to switch the installer files by clicking on the icon next to it. The selected installer file is marked by the ☑ icon. All other installers are



marked by the  icon.

Folders and files in this view can be deleted by clicking on the  icon located behind the item.



Be aware:

Deleting a folder will also delete all subfolders and packages contained in the folder from the package.

Detection

In the **Detection** tab it is possible to define information that can be used by RayManageSoft Unified Endpoint Manager in order to detect if the application is already installed on a device.

Add Package

General Files Detection Advanced

Branding

KEY

NAME

VALUE

 The key, name, and value fields are used to specify a registry entry that can be used to determine whether or not this application is already installed.

 If you leave detection information empty, the installation agent will invoke the installation multiple times.

Uninstall Key

UNINSTALL REGISTRY KEY NAME

 Enter the registry key that can be used to uninstall a previous or current version of this application from the managed device. This key is under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall in the registry.

Add

Discard

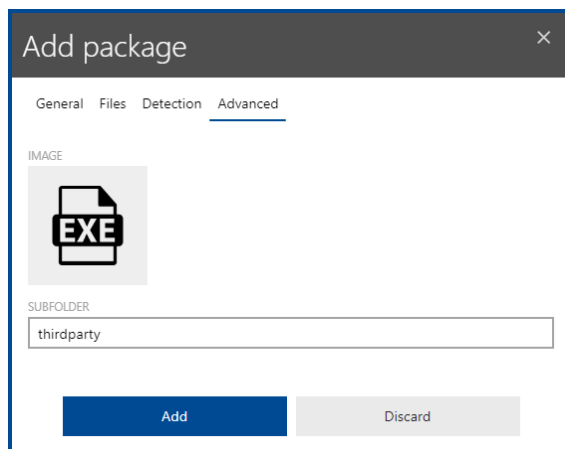


The following information can be specified.

- **KEY:** In the **Key** field the key of the registry hive (below `HKEY_LOCAL_MACHINE`) and the key name of a registry key that can be used to determine whether or not the package is already installed can be specified. For example, if the registry key is in `HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\Adobe Acrobat\6.0\Installer` the entry in the **KEY** field should be `SOFTWARE\Adobe\Adobe Acrobat\6.0\Installer`.
- **NAME:** In the **Name** field the name of a registry entry that is used in conjunction with the contents of the **KEY** field in order to determine whether or not the package is already installed can be specified. If the name of the registry entry set by the application installation is `Default` the field is left empty.
- **VALUE:** In the **Value** field the value that is used in conjunction with the contents of the **KEY** and the **NAME** field in order to determine whether or not the package is already installed can be specified. An example value would be `"C:\Program Files\Adobe\Acrobat 6.0\Acrobat"`.
- **Uninstall Key:** This field should contain the registry key that is used to uninstall the package. The uninstall registry key usually matches the GUID of the application set in curly brackets. An example value would be `{2453DBC8-ACC4-4711-BD03-0C15353AA3D8}`. It is not necessary to enter the whole path, the uninstall registry key is sufficient. It does not matter if the key will have to be in the 32-bit or the 64-bit section of the registry. This will be managed automatically. The key can generally be found in the registry under `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`.

Advanced

In the **Advanced** tab additional information for the package can be configured.



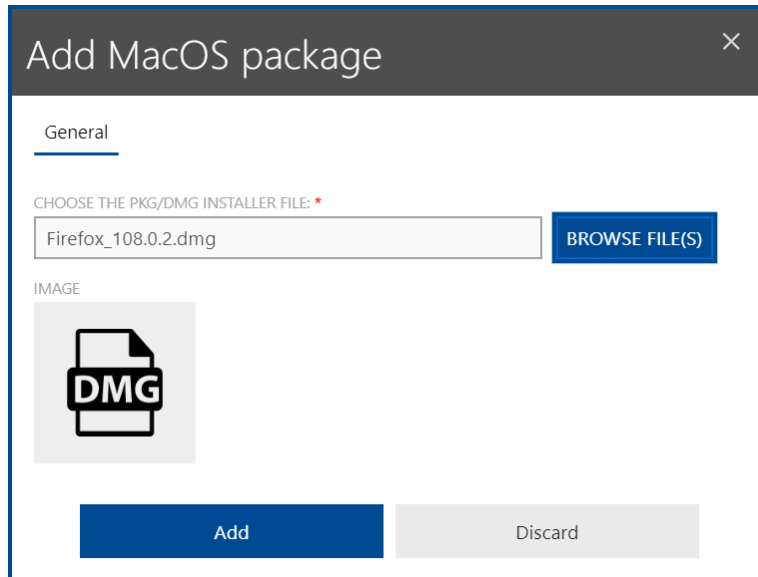
The following information can be specified.

- **IMAGE:** Upload a customized image for the application (the following file formats are supported: `.gif`, `.jpg`, `.jpeg`, and `.png`).
- **SUBFOLDER:** Specifies the folder to which the application is added. By default, the folder name is `"thirdparty"`.



Add a MacOS Installer Package

The Add MacOS package dialog can be used to add a MacOS installer package to the applications library of RayManageSoft Unified Endpoint Manager. Detailed information on which packages are supported by RayManageSoft Unified Endpoint Manager can be found in the [Supported MacOS Packages](#) chapter.





The following options are available in the Add MacOS package dialog:

- **CHOOSE THE PKG/DMG INSTALLER FILE:** Click on the **BROWSE FILE(S)** button next to the field in order to select the target package. Browse to the folder containing the package and select it. This option is mandatory.



WARNING:

For `.pkg` and `.dmg` files only letters, numbers, dash '-', dot '.', and underscore '_' are allowed as characters for the file name.

The maximum length of a file name for `.pkg` and `.dmg` files is 255 characters.

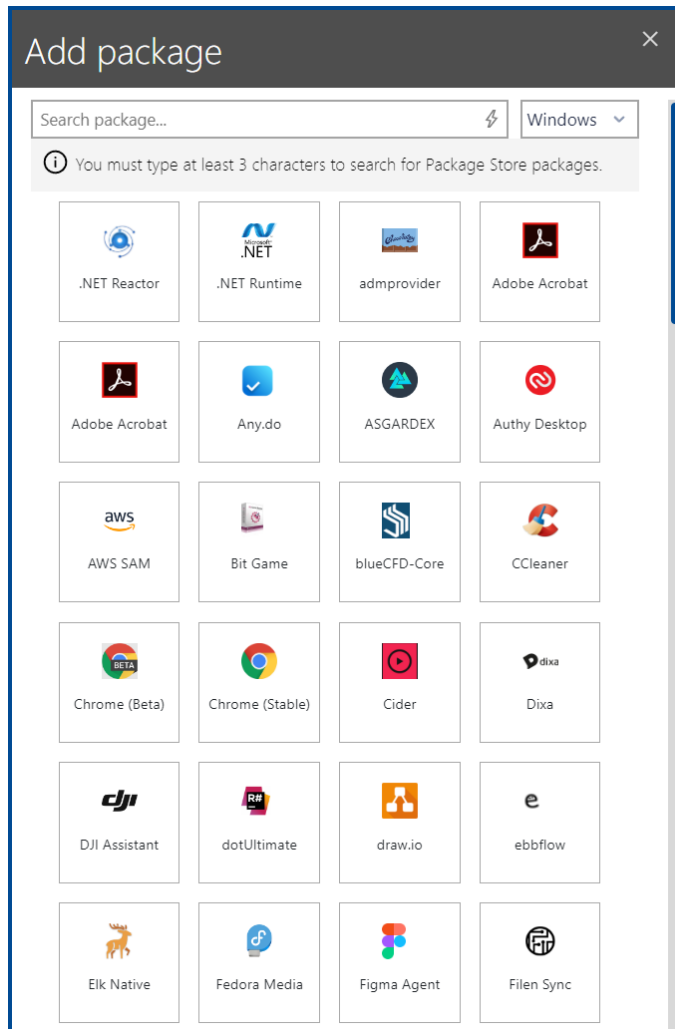
- **IMAGE:** Upload a customized image for the application (the following file formats are supported: `.gif`, `.jpg`, `.jpeg`, and `.png`). This option is optional.

Supported MacOS Packages

RayManageSoft Unified Endpoint Manager supports `.pkg` packages and most `.dmg` packages. RayManageSoft Unified Endpoint Manager does not support `.dmg` packages that contain `.pkg` packages. If this is the case, the `.pkg` package must be manually extracted. After the `.pkg` package has been extracted, it can be added to the library.

Add a Package from the Package Store

With RayManageSoft Unified Endpoint Manager it is possible to easily import prepackaged software packages from the Raynet Package Store. In order to import a package, click on the **+** **Add** button and select the **Add package from Package Store** option. The **Add Package** dialog for Package Store packages will be opened.



Select a package from the list of packages that will be shown by clicking on the package. It is possible to use the search field on top of the list to reduce the number of packages shown. To switch between packages for Windows and packages for macOS, select the target OS in the dropdown that is located in the top right corner of the dialog.



Be aware:

A full list of the packages matching the expression in the search field will only be shown if at least 3 characters have been entered into the search field. If less characters or no characters have been entered, only the most popular packages will be shown.

After a package has been selected, the **Add Package** dialog for this specific packages will be shown. The new dialog is divided into three different tabs:

- **General:** This tab is used to select the specific version of the package that will be imported from the Package Store.
- **Options:** This tab is used to configure standard application features for the package. The options available for configuration depend on the selected package.



- **Advanced:** This tab is used to configure further options like a custom installation directory or a custom log directory. The options available for configuration depend on the selected package. It is also possible that this tab is not available for a specific package.



There is also a **Back** button located at the top left of the dialog which can be used to return to the package selection.

General

In the **General** tab the version of the selected package can be selected. Furthermore some general information for the package will be loaded from the Package Store.

Add package [X]

General Options Advanced

 **NAME:** .NET Reactor

PARENT FOLDER: Windows [⚡]

VERSION: 6.8.0.0 [v]

MANUFACTURER: Eziriz

LANGUAGE: Not specified

LICENSE: Commercial

DESCRIPTION:

Unmatched .NET code protection system which completely stops anyone from decompiling your code.

Add **Discard**

The following information will be shown in this tab:

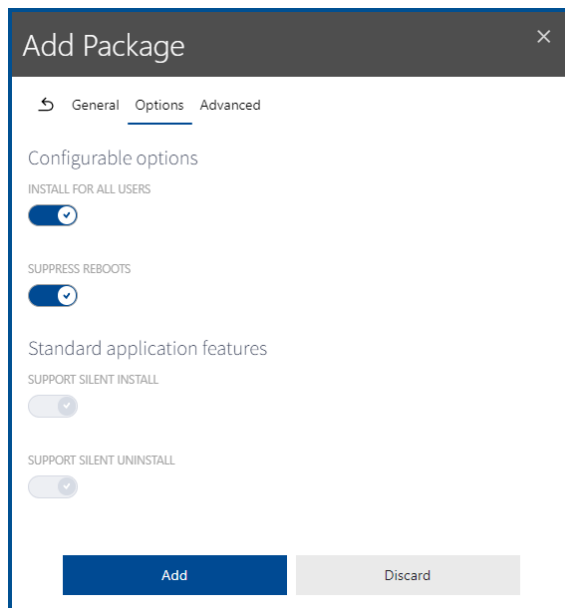
- **Name:** The name of the package.
- **Parent folder:** In this field, define the folder the package will be located. The selected folder must already exist. It is not possible to create a new folder using this field. The field supports auto completion.
- **Version:** Use the dropdown menu to select the version of the package.



- **Manufacturer:** The manufacturer of the package.
- **Language:** The language of the package.
- **License:** The type of licensing necessary for the package.
- **Description:** A description of the package and its functionality.

Options

The **Options** tab contains some standard options that can be configured for the package. The content of the tab and the configurability depends on the selected package. The content of the tab is gained dynamically from the Package Store.



The following options can be available in this tab:

- **Disable add/remove programs interaction:** Activate in order to disable any interaction with the **add/remove programs** tool.
- **Disable automatic updates:** Activate in order to disable automatic updates.
- **Install for all users:** Activate in order to install the application for all users of a device.
- **Prevent downgrade:** Activate in order to prevent the downgrade of a higher version.
- **Remove desktop shortcuts:** Activate in order to remove any desktop shortcuts for the application.
- **Support silent installation:** Activate in order to support the option for a silent install of the application.
- **Support silent uninstallation:** Activate in order to support the option for a silent uninstall of the application.
- **Suppress reboots:** Activate in order to suppress reboots when installing the application.



Advanced

The **Advanced** tab contains some advanced options for the package. The existence and the content of the tab depends on the selected package. The content of the tab is gained dynamically from the Package Store.

The screenshot shows the 'Add Package' dialog box with the 'Advanced' tab selected. It features three toggle switches and text input fields for customizing installation and logging. The 'Add' button is highlighted in blue.

The following options can be available in this tab:

- **Use custom installation directory:** Activate to define a custom installation directory. Enter the directory into the **Destination** folder field located below the button.
- **Use custom log file:** Activate to define a custom name for the log file. Enter the name into the **Log file** field located below the button.
- **Use custom log directory:** Activate to define a custom directory to which the log files will be written. Enter the directory into the **Destination** folder field located below the button.
- **This is a patch package:** Activate this option define the package as a patch package.
- **No icons in start menu:** Activate to not add an icon for the application to the **Start** menu.
- **Install this package only if another version of this product is already installed:** Activate this option to only install this package if there is already another version of the package installed.
- **Delete all launch conditions:** Activate this option to delete all launch conditions.
- **Deep clean-up during the uninstallation (ZAP):** Activate to define that there will be a deep clean-up removing all remnants of the package during the uninstallation.

Edit a Package

The **Edit package** dialog that is opened by the **Edit** button if a package has been selected in the **Applications** section of RayManageSoft Unified Endpoint Manager. The Edit package dialog varies depending on which type of package will be edited.



- [Edit a Windows Package](#)
- [Edit a MacOS Package](#)

Edit a Windows Package

When opening a Windows package the **Edit package** dialog is divided into two tabs:

- [Details](#)
- [Information](#)



Details

In the **Details** tab of the **Edit Package** dialog package specific details can be edited.

Edit package

Details Information

IMAGE

NAME *

7-Zip 22.00 x64 edition

DISPLAY NAME *

7-Zip 22.00 (x64 edition)

COPYRIGHT ©

MANUFACTURER *

Igor Pavlov

VERSION *

22 0 0 0

i The version number is used by the Deployment Manager on the managed devices to coordinate application updates. Increase this number whenever you want to distribute a revised version of your application.

HIDDEN FLAG ☐

i Hidden flag is used to hide package information from the user of the managed device.

Save changes Discard

The following options are available in the dialog.

- **IMAGE:** Clicking on the image will open a file browser. Browse for an image to customize the image for the package (the following file formats are supported: .gif, .jpg, .jpeg, and .png).
- **NAME:** The full name of the application.
- **DISPLAY NAME:** The name that will be displayed.
- **COPYRIGHT @:** The name of the copyright owner.
- **MANUFACTURER:** The name of the creator.
- **VERSION:** The version number of the application which is further divided into:
 - Major
 - Minor



- Build
- Revision

Since the fields have already been separated, no further separators are allowed.

- **HIDDEN FLAG:** Check the **HIDDEN FLAG** option to hide package information from the user of the managed device. This can be used to create prerequisite packages that should be installed but not be visible for the end-user in the RMS UEM AppCenter.



Information

In the **Information** tab of the **Edit Package** dialog general information regarding the package can be edited.

Edit Package

Details Information

RELEASE WEBSITE

SUPPORT CONTACT

SUPPORT WEBSITE

COMMENT

Save changes Discard

The following options are available in the dialog.

- **RELEASE WEBSITE:** The URL of the website where the package can be downloaded.
- **SUPPORT CONTACT:** The name and the contact information of a support contact for the package.
- **SUPPORT WEBSITE:** The URL of a website where support for the package is available.
- **COMMENT:** Further relevant information regarding the package that do not fit into any other category.

Edit a MacOS Package

When opening a MacOS package the **Edit package** dialog is divided into three tabs:

- [Details](#)
- [Information](#)
- [Custom Properties](#)



Details

In the **Details** tab of the **Edit Package** dialog package specific details can be edited.

Edit package

Details Information Custom Properties

IMAGE

NAME *

VLC media player

DISPLAY NAME *

VLC media player

COPYRIGHT ©

MANUFACTURER *

videolan

VERSION *

3 0 18 0

i The version number is used by the Deployment Manager on the managed devices to coordinate application updates. Increase this number whenever you want to distribute a revised version of your application.

HIDDEN FLAG ☐

i Hidden flag is used to hide package information from the user of the managed device.

Save changes Discard

The following options are available in the dialog.

- **IMAGE:** Clicking on the image will open a file browser. Browse for an image to customize the image for the package (the following file formats are supported: .gif, .jpg, .jpeg, and .png).
- **NAME:** The full name of the application.
- **DISPLAY NAME:** The name that will be displayed.
- **COPYRIGHT @:** The name of the copyright owner.
- **MANUFACTURER:** The name of the creator.
- **VERSION:** The version number of the application which is further divided into:
 - Major
 - Minor



- Build
- Revision

Since the fields have already been separated, no further separators are allowed.

- **HIDDEN FLAG:** Check the **HIDDEN FLAG** option to hide package information from the user of the managed device. This can be used to create prerequisite packages that should be installed but not be visible for the end-user in the RMS UEM AppCenter.

Information

In the **Information** tab of the **Edit Package** dialog general information regarding the package can be edited.

The following options are available in the dialog.

- **RELEASE WEBSITE:** The URL of the website where the package can be downloaded.
- **SUPPORT CONTACT:** The name and the contact information of a support contact for the package.
- **SUPPORT WEBSITE:** The URL of a website where support for the package is available.
- **COMMENT:** Further relevant information regarding the package that do not fit into any other category.

Custom Properties

In the **Custom Properties** tab of the **Edit Package** dialog existing custom properties can be edited or deleted and new custom properties can be added.



Edit package

Details

Information

Custom Properties

^ ApplicationInstallDir

NAME*

ApplicationInstallDir

VALUE*

/Applications/VLC.app

^ ApplicationInfoPlistChecksum

NAME*

ApplicationInfoPlistChecksum

VALUE*

414466f8c1fe9d144a5151af540ee300

Add Custom Property

Save changes

Discard

In order to add a new custom property to the package, click on the **Add Custom Property** button. An empty property will be added. There are two fields available for a custom property.

- **NAME:** Enter the name of the custom property. This field is mandatory when adding a new custom property.
- **VALUE:** Enter the value of the custom property. Legit values depend on the custom property. This field is mandatory when adding a new custom property.



Patch Management

The **Patch management** section can be used to implement rules that can be used to automatically update managed packages. It is also possible to fine-tune these updates using these rules in order to only update applications if there are major updates, only download new updates and not automatically install them, etc. In the **Patch management** section a list of the rules is shown. The list shows the package the rule applies to, the version of the application, the latest available version, the type of the rule, the version restriction, and if an update is currently available.



Be aware:

The **Patch management** feature can only be used with packages from the Package Store.

Package	Application Version	Available Version	Type	Version Restriction	Update Available
NET Runtime-6.0.9-x64	6.0.0.0	6.0.0.0	Update	Unrestricted	No

The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the screen can be used to refresh the view.
- **Add** - The **Add** button on the top left of the screen can be used to add a rule. For more information see [Add a Rule](#).
- **Edit** - The **Edit** button on the top left of the screen can be used to edit a rule if one rule in the list has been selected. For more information see [Edit a Rule](#).
- **Delete** - The **Delete** button on the top left of the screen can be used to delete one or more rules if one or more rules in the list have been selected.
- **Advanced filter** - The **Advanced filter** is available on the top right of the screen. A description on how to use the **Advanced filters** can be found in the [Using Sorting, Filter, and Search Options](#) section.
- **Search field** - The **Search** field can be found on the top right of the screen. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.



Add a Rule

In the **Add Rule** dialog the patch management rules for a package can be configured.

Add rule

General

Package *

Adobe Acrobat Reader DC-22.002.20191-x64 [22.2.20191.0]

Type *

Update

Delete previous package

☒

! If selected, the previous version of the package is deleted upon completion of the update action.

Version Restriction

Unrestricted

Add Discard

The following options are available in the dialog.

- **Package:** Select the package for which the rule will be created from the list of packages available in RayManageSoft Unified Endpoint Manager. The number of packages shown can be lowered down by starting to enter characters into the field. This is a mandatory field.
- **Type:** Select a type for the rule from the dropdown menu. The following options are available in the dropdown menu. This is a mandatory field.

Type

Update

Update

Download

Manual

- **Update:** Select this option in order to automatically update the package. If **Update** is selected as type, the **Delete previous package** switch will be shown.
- **Download:** Select this option in order to automatically download patches for the package without triggering the update itself.
- **Manual:** Select this option in order to manually trigger all steps that concern patches for the



package.



WARNING

Only use the Update type with assignments that have an active exclusive flag!

- **Delete previous package:** This switch can be used to define if the previous package should be deleted after the update, or if the package should be kept.
- **Version Restriction:** Select the patches to which the rule will be applied to. By default, this option is set to **Unrestricted**.

Version Restriction

Unrestricted

Unrestricted

Major

Major and Minor

- **Unrestricted:** Select this option in order to apply the rule to all patches available for the package.
- **Major:** Select this option in order to apply the rule only to major updates for the package (for example if a package is upgraded from 2.x to 3.x).
- **Minor:** Select this option in order to apply the rule to major and minor updates for the package (for example if a package is upgraded from x.1 to x.2).

Edit a Rule

In the **Edit Rule** dialog the patch management rules for a package can be configured.



Edit rule

General

Package
.NET Reactor-6.8.0.0

Type
Update

Delete previous package
☒

Info If selected, the previous version of the package is deleted upon completion of the update action.

Version Restriction
Unrestricted

Save changes Discard

The following options are available in the dialog.

- **Package:** Select the package for which the rule will be created from the list of packages available in RayManageSoft Unified Endpoint Manager. The number of packages shown can be lowered down by starting to enter characters into the field.
- **Type:** Select a type for the rule from the dropdown menu. The following options are available in the dropdown menu.

Type

Update

Update

Download

Manual

- **Update:** Select this option in order to automatically update the package. If **Update** is selected as type, the **Delete previous package** switch will be shown.
- **Download:** Select this option in order to automatically download patches for the package without triggering the update itself.
- **Manual:** Select this option in order to manually trigger all steps that concern patches for the package.

WARNING

Only use the Update type with assignments that have an active exclusive flag!



- **Delete previous package:** This switch can be used to define if the previous package should be deleted after the update, or if the package should be kept.
- **Version Restriction:** Select the patches to which the rule will be applied to.

A screenshot of a web interface showing a dropdown menu titled "Version Restriction". The menu is open, displaying four options: "Unrestricted", "Unrestricted", "Major", and "Major and Minor". The first "Unrestricted" option is highlighted with a blue background. There is a small upward arrow icon at the top right of the dropdown list.

- **Unrestricted:** Select this option in order to apply the rule to all patches available for the package.
- **Major:** Select this option in order to apply the rule only to major updates for the package (for example if a package is upgraded from 2.x to 3.x).
- **Minor:** Select this option in order to apply the rule to major and minor updates for the package (for example if a package is upgraded from x.1 to x.2).



Endpoint Security

The **Endpoint security** category of the sidebar contains the following subcategories:

- [Update Management](#)

Update Management

The **Update Management** section of RayManageSoft Unified Endpoint Manager contains an overview of the **Update Management Packages** that are currently available in the tenant.



Note:

Update Management is a Windows only feature.

The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the screen can be used to refresh the view.
- **Add** - The **Add** button on the top left of the screen can be used to add a package. For more information see [Add an Update Management Package](#).
- **Edit** - The **Edit** button on the top left of the screen can be used to edit a package if one package in the list has been selected. For more information see [Edit an Update Management Package](#).
- **Delete** - The **Delete** button on the top left of the screen can be used to delete one or more **Update Management Packages** if one or more packages in the list have been selected.
- **Advanced filter** - The **Advanced filter** is available on the top right of the screen. A description on how to use the **Advanced filters** can be found in the [Using Sorting, Filter, and Search Options](#) section.
- **Search field** - The **Search** field can be found on the top right of the screen. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.



Update Management Package Details

When opening the details of an **Update Management Package** the information regarding the package are divided into two parts.

Setting	Value	Description
Windows Update	Yes	Enables or disables the windows update functionality on a device. This option should only be disabled in case you have a custom patch management solution in place.
Servicing channel	General Availability Channel (Targeted)	The branch readiness level enables administrators to specify which channel of feature updates the device should receive.
Microsoft product updates	No	Consider updates for other Microsoft products, such as versions of Office that are installed by using Windows installer (MSI). Versions of Office that are installed by using Click-to-Run can't be updated by using Windows Update for Business. Product updates are off by default.
Disable driver updates	No	Disable windows update function for non-Microsoft drivers that are relevant to the devices (e.g. graphics drivers). Driver updates are on by default, but you can turn them off if you prefer.
Quality update deferral period (days)	not configured	Defer quality updates for the specified number of days.
Feature update deferral period (days)	not configured	Defer feature updates for the specified number of days.

The left side contains all general information regarding the package including the name, the version, and the creator of the package.

The right side is divided into tabs where the specific settings are shown. The following tabs are available:

- [Settings](#)
- [User Experience](#)

While in this view, the following actions are available for this package.

- **Edit** - The **Edit** button on the top left of the screen can be used in order to edit the package. For more information see [Edit an Update Management Package](#).
- **Delete** - The **Delete** button on the top left of the screen can be used to delete one or more packages if one or more packages in the list have been selected.

Settings

In the **Settings** tab the available settings for the **Update Management Package** are shown.

Setting	Value	Description
Windows Update	Yes	Enables or disables the windows update functionality on a device. This option should only be disabled in case you have a custom patch management solution in place.
Servicing channel	General Availability Channel (Targeted)	The branch readiness level enables administrators to specify which channel of feature updates the device should receive.
Microsoft product updates	No	Consider updates for other Microsoft products, such as versions of Office that are installed by using Windows installer (MSI). Versions of Office that are installed by using Click-to-Run can't be updated by using Windows Update for Business. Product updates are off by default.
Disable driver updates	No	Disable windows update function for non-Microsoft drivers that are relevant to the devices (e.g. graphics drivers). Driver updates are on by default, but you can turn them off if you prefer.
Quality update deferral period (days)	not configured	Defer quality updates for the specified number of days.
Feature update deferral period (days)	not configured	Defer feature updates for the specified number of days.



Setting	Value / Range	Description
Windows Update	• Yes • No	Enables or disables the windows update agent functionality on a device. This option should only be disabled in case there is a custom patch management solution in place.
Servicing Channel	• General Availability Channel (Targeted) • Reset to default	The branch readiness level enables administrators to specify which channel of feature updates the device should receive.
Microsoft product updates	• Yes • No	Consider the update for other Microsoft products, such as versions of Office that are installed by using Windows Installer (MSI). Versions of Office that are installed by using Click-to-Run cannot be updated by using Windows Update for Business. Product updates are off by default.
Windows driver updates	• Yes • No	Consider updates for non-Microsoft drivers that are relevant for the device. Driver updates are on by default, but they can be turned off.
Quality update deferral period (days)	0-35	Defer quality updates for the specified number of days. The default value is 0 (not deferred) but it is possible to defer quality updates for up to 35 days.
Feature update deferral period (days)	0-365	Defer feature updates for the specified number of days. The default value is 0 (not deferred) but it is possible to defer feature updates for up to 365 days.

User Experience

In the **User Experience** tab the available settings regarding the user interaction and the update schedule are shown.



Settings

User Experience

Automatic update behavior

Auto install at maintenance time

Manages automatic update behavior for scanning, downloading and installing of updates.

Active hours start

9 AM

Configure a period when restart due to update installations will be suppressed.

Active hours end

6 PM

Configure a period when restart due to update installations will be suppressed.

Currently one of the following settings regarding the updated behavior will be selected as **Automatic update behavior**. Depending on the selected behavior further settings can be available in this tab.

Setting	Description	Available Settings
Notify Download	If this option is selected, the user will be notified when an update is being downloaded.	none
Auto install at maintenance time	This option is used to define a period during which updates are suppressed. Updates will only be installed outside of the defined period.	• Active hours start • Active hours end
Auto install and restart at scheduled times	If this option is used, a period during which updates will be suppressed need to be defined. Outside of this period, updates will be installed and a restart will occur.	• Active hours start • Active hours end
Auto install and restart at scheduled times	If this option is used, updates will be installed and a restart will occur at a scheduled day and time that is defined using the settings linked to this option.	• Scheduled install day • Scheduled install time
Auto install and reboot without end-user control	If this option is selected, the end-user has no influence on the update and reboot behavior.	none
Reset to default	If this option is used, the updates will be automatically downloaded and the user will be notified when they are ready to install.	none

The further available settings and their link to the selected update behavior are shown below.

Auto Install at Maintenance Time Settings



Setting	Value / Range	Description
Active hours start	• 12 AM • 1 AM • 2 AM • 3 AM • 4 AM • 5 AM • 6 AM • 7 AM • 8 AM • 9 AM • 10 AM • 11 AM • 12 PM • 1 PM • 2 PM • 3 PM • 4 PM • 5 PM • 6 PM • 7 PM • 8 PM • 9 PM • 10 PM • 11 PM	The start time of the period during which restarts due to update installations will be suppressed.
Active hours end	• 12 AM • 1 AM • 2 AM • 3 AM • 4 AM • 5 AM • 6 AM • 7 AM • 8 AM • 9 AM • 10 AM • 11 AM • 12 PM • 1 PM • 2 PM • 3 PM • 4 PM • 5 PM • 6 PM • 7 PM • 8 PM • 9 PM • 10 PM • 11 PM	The end time of the period during which restarts due to update installations will be suppressed.

Auto Install and Restart at Maintenance Time Settings

Setting	Value / Range	Description
Active hours start	• 12 AM • 1 AM • 2 AM • 3 AM • 4 AM • 5 AM • 6 AM • 7 AM • 8 AM • 9 AM • 10 AM • 11 AM • 12 PM • 1 PM • 2 PM • 3 PM • 4 PM • 5 PM • 6 PM • 7 PM • 8 PM • 9 PM • 10 PM • 11 PM	The start time of the period during which restarts due to update installations will be suppressed.
Active hours end	• 12 AM • 1 AM • 2 AM • 3 AM • 4 AM • 5 AM • 12 PM • 1 PM • 2 PM • 3 PM • 4 PM • 5 PM	The end time of the period during which restarts due to update installations will be suppressed.



Setting	Value / Range	Description
	• 6 AM • 7 AM • 8 AM • 9 AM • 10 AM • 11 AM • 6 PM • 7 PM • 8 PM • 9 PM • 10 PM • 11 PM	

Auto Install and Restart at Scheduled Time Settings

Setting	Value	Description
Scheduled install day	• Any Day • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday • Sunday	The day for the installation of scheduled updates.
Scheduled install time	• 12 AM • 1 AM • 2 AM • 3 AM • 4 AM • 5 AM • 6 AM • 7 AM • 8 AM • 9 AM • 10 AM • 11 AM • 12 PM • 1 PM • 2 PM • 3 PM • 4 PM • 5 PM • 6 PM • 7 PM • 8 PM • 9 PM • 10 PM • 11 PM	The time for the installation of scheduled updates.

Add an Update Management Package

The **Add an Update Management Package** is divided into three tabs:

- [General](#): This tab is used to specify general information regarding the **Update Management Package**.
- [Update Settings](#): This tab is used to define settings like what and how the updates are handled.
- [User Experience](#): This tab is used to define when the updates are installed and the interaction level with the user.



General

The **General** tab is used to configure some general information regarding the **Update Management Package**. The mandatory information are marked by a red asterisk.

The screenshot shows a dialog box titled "Add update management policy" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "General" (selected), "Update Settings", and "User Experience". Under the "General" tab, there is an "IMAGE" section with a circular refresh icon. Below this is a "NAME *" field containing "Example Package". The "MANUFACTURER *" field contains "Raynet GmbH". The "VERSION *" section consists of four input fields with values "1", "0", "0", and "0", separated by dots. A tooltip icon (i) is present next to the version fields, with a text box explaining that the version number is used by the Deployment Manager to coordinate updates and should be increased when a revised version is distributed. Below the version fields are "SUPPORT CONTACT" and "COMMENT" text areas. At the bottom, there are two buttons: "Add" (blue) and "Discard" (grey).

The following information can be configured in this tab.

- **IMAGE:** It is possible to add a custom image to the **Update Management Package**. Click on the image to open the file browser. It is now possible to add a custom image to a package by opening an image from the browser (the following file formats are supported: .gif, .jpg, .jpeg, and .png).
- **NAME:** Enter a name for the **Update Management Package**. This field is mandatory and cannot be left empty.
- **MANUFACTURER:** This field should contain the name of the creator of the **Update Management Package**. This field is mandatory and cannot be left empty.
- **VERSION:** The **VERSION** field is divided into 4 different fields. All 4 fields should contain an integer value. These fields are mandatory since they are used to coordinate application updates. The number should be increased, each time a revised version of the package is distributed. Since the fields are already divided by periods no further division is necessary. The fields are as follows:



- Major
- Minor
- Build
- Revision
- **SUPPORT CONTACT:** This field can be used to enter a support contact for the package. This could either be the name of the person responsible for the support or some sort of contact like an email address or a phone number.
- **COMMENT:** This field can be used to add a comment to the package.

Update Settings

In this tab the update settings that will be used by the devices are defined.

The screenshot shows a dialog box titled "Add update management policy" with a close button (X) in the top right corner. It has three tabs: "General", "Update settings" (which is selected and underlined), and "User experience".

Under the "Update settings" tab, there are several sections:

- WINDOWS UPDATE:** A checkbox is checked. Below it is an information icon (i) and text: "Enables or disables the windows update functionality on a device. This option should only be disabled in case you have a custom patch management solution in place."
- SERVICING CHANNEL:** A dropdown menu is set to "General Availability Channel (Targeted)". Below it is an information icon (i) and text: "The branch readiness level enables administrators to specify which channel of feature updates the device should receive."
- MICROSOFT PRODUCT UPDATES:** A checkbox is unchecked. Below it is an information icon (i) and text: "Consider updates for other Microsoft products, such as versions of Office that are installed by using Windows installer (MSI). Versions of Office that are installed by using Click-to-Run can't be updated by using Windows Update for Business. Product updates are off by default."
- DISABLE DRIVER UPDATES:** A checkbox is unchecked. Below it is an information icon (i) and text: "Disable windows update function for non-Microsoft drivers that are relevant to the devices (e.g. graphics drivers). Driver updates are on by default, but you can turn them off if you prefer."
- QUALITY UPDATE DEFERRAL PERIOD (DAYS):** A text input field containing "not configured".
- FEATURE UPDATE DEFERRAL PERIOD (DAYS):** A dropdown menu set to "not configured".

At the bottom of the dialog, there are two buttons: "Add" (in blue) and "Discard" (in grey).

- **WINDOWS UPDATE**
The **WINDOWS UPDATE** checkbox is used in order to enable or disable the Windows update functionality on a device. This option should only be disabled in case another patch management solution is in place. In order to disable the Windows update functionality, ensure



that the checkbox is unchecked.

- **SERVICING CHANNEL**

The **SERVICING CHANNEL** checkbox can be used in order to specify which channel of feature updates a device should receive. Information on the different servicing channels for Windows updates can be found in the [Microsoft documentation](#). The following channels are available:

- General Availability Channel (Targeted)
- Reset to default

- **MICROSOFT PRODUCT UPDATES**

The **MICROSOFT PRODUCT UPDATES** checkbox is used to specify whether updates for other Microsoft products, such as versions of Microsoft Office that are installed by using Windows Installer (MSI) are considered. Versions of Microsoft Office that are being installed by using Click-to-Run cannot be updated by using Windows Update for Business. Product updates are off by default. In order to consider updates for other Microsoft products ensure that the checkbox is checked.

- **WINDOWS DRIVER**

The **WINDOWS DRIVER** checkbox is used to specify whether updates for non-Microsoft drivers that are relevant for the device are considered. Driver updates are on by default, but they can be turned off if they should not be considered. In order to not consider driver updates ensure that the checkbox is unchecked.

- **QUALITY UPDATE DEFERRAL PERIOD (DAYS)**

This is used to define the time period (in days) during which quality updates are being deferred. They can be deferred for up to 35 days. Any integer between 0 and 35 can be entered as value. If 0 is entered as value, quality updates will not be deferred.

- **FEATURE UPDATE DEFERRAL PERIOD (DAYS)**

This is used to define the time period (in days) during which feature updates are being deferred. They can be deferred for up to 365 days. Any integer between 0 and 365 can be entered as value. If 0 is entered as value, quality updates will not be deferred.

User Experience

The interaction level with the user can be defined in this tab. The values set here define how much information the user receives and how much interaction from the user is possible.

AUTOMATIC UPDATE BEHAVIOR

This option can be used in order to configure the automated behavior that is used for scanning, downloading, and installing updates. The following options are available for selection in the dropdown menu.

- [Notify download](#): Select this option in order to notify the user when the download of the update starts.
- [Auto install at maintenance time](#): Select this option in order to automatically install pending updates during the defined maintenance time.
- [Auto install and restart at maintenance time](#): Select this option in order to automatically install pending updates and restart the device during the defined maintenance time.
- [Auto install and restart at scheduled time](#): Select this option in order to automatically install pending updates at the specified time.
- [Auto install and reboot without end-user control](#): Select this option in order to automatically install pending updates and reboot the device without allowing the end-user the option to



postpone the update.

- [Reset to default](#): Select this options to automatically download the updates and notify the user when they are ready for installation.

Notify Download

A screenshot of a software configuration window titled 'AUTOMATIC UPDATE BEHAVIOR'. It features a dropdown menu with 'Notify download' selected. Below the dropdown is a help icon and the text: 'Manage automatic update behavior to scan, download and install updates.'

When the **Notify download** option is selected, RayManageSoft Unified Endpoint Manager will notify the user when the download is started. No further configurations for this option are necessary.



Auto Install at Maintenance Time

AUTOMATIC UPDATE BEHAVIOR *

Auto install at maintenance time

Manage automatic update behavior to scan, download and install updates.

ACTIVE HOURS START *

9 AM

ACTIVE HOURS END *

6 PM

Configure a period when restarts due to update installations will be suppressed.

When the **Auto install at maintenance time** option has been selected, it is also necessary to specify a period during which update installations will be suppressed. This is done by selecting a start time and an end time in the fields that will appear once this option has been selected.

- **ACTIVE HOURS START**

Define the start time (in full hours) of the period during which restarts in order to update installations will be suppressed.

- **ACTIVE HOURS END**

- Define the end time (in full hours) of the period during which restarts in order to update installations will be suppressed.



Be aware:

The start time for the period must always be before the end time. Furthermore, the difference between the start time and the end time cannot be more than 18 hours.

Auto Install and Restart at Maintenance Time

AUTOMATIC UPDATE BEHAVIOR *

Auto install and restart at maintenance time

Manage automatic update behavior to scan, download and install updates.

ACTIVE HOURS START

9 AM

ACTIVE HOURS END

6 PM

Configure a period during which update installations and automatic restarts will be suppressed.

When the **Auto install and restart at maintenance time** option has been selected, it is also necessary to specify a period during which update installations will be suppressed. This is done by selecting a start time and an end time in the fields that will appear once this option has been selected.



- **ACTIVE HOURS START**

Define the start time (in full hours) of the period during which restarts in order to update installations will be suppressed.

- **ACTIVE HOURS END**

- Define the end time (in full hours) of the period during which restarts in order to update installations will be suppressed.



Be aware:

The start time for the period must always be before the end time. Furthermore, the difference between the start time and the end time cannot be more than 18 hours.

Auto Install and Restart at Scheduled Time

AUTOMATIC UPDATE BEHAVIOR *

Auto install and restart at scheduled time

Manage automatic update behavior to scan, download and install updates.

SCHEDULED INSTALL DAY *

Every Day

Select install day for scheduled updates

SCHEDULED INSTALL TIME *

12 AM

Select automation update installation day and time

When the **Auto install and restart at scheduled time** option has been selected it is necessary to specify the time and date at which scheduled updates will be automatically installed. This is done by selecting the date and the time (in full hours) at which the updates are installed.

- **SCHEDULED INSTALL DAY**

Select the day for the installation by selecting it in the dropdown menu. The following options are available in the dropdown menu:

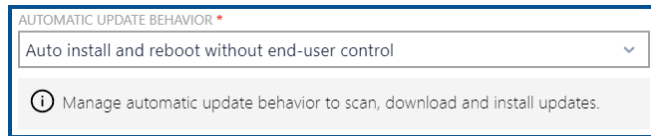
- **Any Day:** If this option is selected, pending updates will be installed at the defined time every day.
- **Monday:** If this option is selected, pending updates will be installed at the defined time every Monday.
- **Tuesday:** If this option is selected, pending updates will be installed at the defined time every Tuesday.
- **Wednesday:** If this option is selected, pending updates will be installed at the defined time every Wednesday.
- **Thursday:** If this option is selected, pending updates will be installed at the defined time every Thursday.
- **Friday:** If this option is selected, pending updates will be installed at the defined time every Friday.
- **Saturday:** If this option is selected, pending updates will be installed at the defined time every Saturday.



- **Sunday:** If this option is selected, pending updates will be installed at the defined time every Sunday.
- **SCHEDULED INSTALL TIME**
Select the time for the installation by selecting the time in the dropdown menu. It is possible to select a value between 12 AM and 11 PM.



Auto Install and Reboot without End-User Control



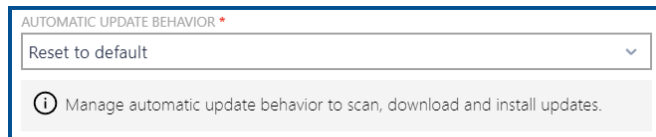
AUTOMATIC UPDATE BEHAVIOR *

Auto install and reboot without end-user control

Manage automatic update behavior to scan, download and install updates.

When the **Auto install and reboot without end-user control** option is selected, RayManageSoft Unified Endpoint Manager automatically install and reboot the device without offering the end-user the option to postpone the update.

Reset to Default



AUTOMATIC UPDATE BEHAVIOR *

Reset to default

Manage automatic update behavior to scan, download and install updates.

When the **Reset to default** option is selected, RayManageSoft Unified Endpoint Manager will automatically download the update and inform the user when the update is ready for installation.

Edit an Update Management Package

The **Edit an Update Management Package** is divided into three tabs:

- [General](#): This tab is used to specify general information regarding the **Update Management Package**.
- [Update Settings](#): This tab is used to define settings like what updates are handled and how the updates are handled.
- [User Experience](#): This tab is used to define when the updates are installed and the interaction level with the user.



General

The **General** tab is used to configure some general information regarding the **Update Management Package**, some of which are mandatory information.

The screenshot shows a dialog box titled "Edit update management policy" with a close button (X) in the top right corner. Below the title bar are three tabs: "General" (selected), "Update Settings", and "User Experience".

Under the "General" tab, there is an "IMAGE" section with a circular refresh icon. Below this is a "NAME *" field containing "Default Update Management Package".

Next is a "MANUFACTURER *" field containing "Raynet GmbH".

Below that is a "VERSION *" section with four input fields separated by dots, containing the values "1", "0", "0", and "0".

A tooltip icon (i) is present next to the version fields with the text: "The version number is used by the Deployment Manager on the managed devices to coordinate application updates. Increase this number whenever you want to distribute a revised version of your application."

Below the version fields is a "SUPPORT CONTACT" field and a "COMMENT" field, both currently empty.

At the bottom are two buttons: "Save changes" (blue) and "Discard" (grey).

The following information can be configured in this tab.

- **IMAGE:** It is possible to add a custom image to the **Update Management Package**. Click on the image to open the file browser. It is now possible to add a custom image to a package by opening an image from the browser (the following file formats are supported: .gif, .jpg, .jpeg, and .png).
- **NAME:** Enter a name for the **Update Management Package**. This field is mandatory and cannot be left empty.
- **MANUFACTURER:** This field should contain the name of the creator of the **Update Management Package**. This field is mandatory and cannot be left empty.
- **VERSION:** The **VERSION** field is divided into 4 different fields. All 4 fields should contain an integer value. These fields are mandatory since they are used to coordinate application updates. The number should be increased, each time a revised version of the package is distributed. Since the fields are already divided by periods no further division is necessary. The fields are as follows:



- Major
- Minor
- Build
- Revision
- **SUPPORT CONTACT:** This field can be used to enter a support contact for the package. This could either be the name of the person responsible for the support or some sort of contact like an email address or a phone number.
- **COMMENT:** This field can be used to add a comment to the package.



Update Settings

In this tab the update settings that will be used by the devices are defined.

The screenshot shows the 'Edit update management policy' dialog box with the 'Update settings' tab selected. The dialog has three tabs: 'General', 'Update settings', and 'User experience'. The 'Update settings' tab contains several sections:

- WINDOWS UPDATE**: A checkbox is checked. Below it is an information icon and text: 'Enables or disables the windows update functionality on a device. This option should only be disabled in case you have a custom patch management solution in place.'
- SERVICING CHANNEL**: A dropdown menu is set to 'Reset to default'. Below it is an information icon and text: 'The branch readiness level enables administrators to specify which channel of feature updates the device should receive.'
- MICROSOFT PRODUCT UPDATES**: A checkbox is unchecked. Below it is an information icon and text: 'Consider updates for other Microsoft products, such as versions of Office that are installed by using Windows installer (MSI). Versions of Office that are installed by using Click-to-Run can't be updated by using Windows Update for Business. Product updates are off by default.'
- DISABLE DRIVER UPDATES**: A checkbox is unchecked. Below it is an information icon and text: 'Disable windows update function for non-Microsoft drivers that are relevant to the devices (e.g. graphics drivers). Driver updates are on by default, but you can turn them off if you prefer.'
- QUALITY UPDATE DEFERRAL PERIOD (DAYS)**: A text input field containing 'not configured'.
- FEATURE UPDATE DEFERRAL PERIOD (DAYS)**: A text input field containing 'not configured'.

At the bottom of the dialog are two buttons: 'Save changes' (blue) and 'Discard' (grey).

- **WINDOWS UPDATE**

The **WINDOWS UPDATE** checkbox is used in order to enable or disable the Windows update functionality on a device. This option should only be disabled in case another patch management solution is in place. In order to disable the Windows update functionality, ensure that the checkbox is unchecked.

- **SERVICING CHANNEL**

The **SERVICING CHANNEL** checkbox can be used in order to specify which channel of feature updates a device should receive. Information on the different servicing channels for Windows updates can be found in the [Microsoft documentation](#). The following channels are available:

- General Availability Channel (Targeted)
- Reset to default

- **MICROSOFT PRODUCT UPDATES**

The **MICROSOFT PRODUCT UPDATES** checkbox is used to specify whether updates for other



Microsoft products, such as versions of Microsoft Office that are installed by using Windows Installer (MSI) are considered). Versions of Microsoft Office that are being installed by using Click-to-Run cannot be updated by using Windows Update for Business. Product updates are off by default. In order to consider updates for other Microsoft products ensure that the checkbox is checked.

- **WINDOWS DRIVER**

The **WINDOWS DRIVER** checkbox is used to specify whether updates for non-Microsoft drivers that are relevant for the device are considered. Driver updates are on by default, but they can be turned off if they should not be considered. In order to not consider driver updates ensure that the checkbox is unchecked.

- **QUALITY UPDATE DEFERRAL PERIOD (DAYS)**

This is used to define the time period (in days) during which quality updates are being deferred. They can be deferred for up to 35 days. Any integer between 0 and 35 can be entered as value. If 0 is entered as value, quality updates will not be deferred.

- **FEATURE UPDATE DEFERRAL PERIOD (DAYS)**

This is used to define the time period (in days) during which feature updates are being deferred. They can be deferred for up to 365 days. Any integer between 0 and 365 can be entered as value. If 0 is entered as value, quality updates will not be deferred.

User Experience

The interaction level with the user can be defined in this tab. The values set here define how much information the user receives and how much interaction from the user is possible.

AUTOMATIC UPDATE BEHAVIOR

This option can be used in order to configure the automated behavior that is used for scanning, downloading, and installing updates. The following options are available for selection in the dropdown menu.

- [Notify download](#): Select this option in order to notify the user when the download of the update starts.
- [Auto install at maintenance time](#): Select this option in order to automatically install pending updates during the defined maintenance time.
- [Auto install and restart at maintenance time](#): Select this option in order to automatically install pending updates and restart the device during the defined maintenance time.
- [Auto install and restart at scheduled time](#): Select this option in order to automatically install pending updates at the specified time.
- [Auto install and reboot without end-user control](#): Select this option in order to automatically install pending updates and reboot the device without allowing the end-user the option to postpone the update.
- [Reset to default](#): Select this options to automatically download the updates and notify the user when they are ready for installation.

Notify Download



AUTOMATIC UPDATE BEHAVIOR *

Notify download

i

Manage automatic update behavior to scan, download and install updates.

When the **Notify download** option is selected, RayManageSoft Unified Endpoint Manager will notify the user when the download is started. No further configurations for this option are necessary.



Auto Install at Maintenance Time

AUTOMATIC UPDATE BEHAVIOR *

Auto install at maintenance time

Manage automatic update behavior to scan, download and install updates.

ACTIVE HOURS START *

9 AM

ACTIVE HOURS END *

6 PM

Configure a period when restarts due to update installations will be suppressed.

When the **Auto install at maintenance time** option has been selected, it is also necessary to specify a period during which update installations will be suppressed. This is done by selecting a start time and an end time in the fields that will appear once this option has been selected.

- **ACTIVE HOURS START**
Define the start time (in full hours) of the period during which restarts in order to update installations will be suppressed.
- **ACTIVE HOURS END**
Define the end time (in full hours) of the period during which restarts in order to update installations will be suppressed.

Be aware:

The start time for the period must always be before the end time. Furthermore, the difference between the start time and the end time cannot be more than 18 hours.

Auto Install and Restart at Maintenance Time

AUTOMATIC UPDATE BEHAVIOR *

Auto install and restart at maintenance time

Manage automatic update behavior to scan, download and install updates.

ACTIVE HOURS START

9 AM

ACTIVE HOURS END

6 PM

Configure a period during which update installations and automatic restarts will be suppressed.

When the **Auto install and restart at maintenance time** option has been selected, it is also necessary to specify a period during which update installations will be suppressed. This is done by selecting a start time and an end time in the fields that will appear once this option has been



selected.

- **ACTIVE HOURS START**

Define the start time (in full hours) of the period during which restarts in order to update installations will be suppressed.

- **ACTIVE HOURS END**

- Define the end time (in full hours) of the period during which restarts in order to update installations will be suppressed.



Be aware:

The start time for the period must always be before the end time. Furthermore, the difference between the start time and the end time cannot be more than 18 hours.

Auto Install and Restart at Scheduled Time

AUTOMATIC UPDATE BEHAVIOR *

Auto install and restart at scheduled time

Manage automatic update behavior to scan, download and install updates.

SCHEDULED INSTALL DAY *

Every Day

Select install day for scheduled updates

SCHEDULED INSTALL TIME *

12 AM

Select automation update installation day and time

When the **Auto install and restart at scheduled time** option has been selected it is necessary to specify the time and date at which scheduled updates will be automatically installed. This is done by selecting the date and the time (in full hours) at which the updates are installed.

- **SCHEDULED INSTALL DAY**

Select the day for the installation by selecting it in the dropdown menu. The following options are available in the dropdown menu:

- **Any Day:** If this option is selected, pending updates will be installed at the defined time every day.
- **Monday:** If this option is selected, pending updates will be installed at the defined time every Monday.
- **Tuesday:** If this option is selected, pending updates will be installed at the defined time every Tuesday.
- **Wednesday:** If this option is selected, pending updates will be installed at the defined time every Wednesday.
- **Thursday:** If this option is selected, pending updates will be installed at the defined time every Thursday.
- **Friday:** If this option is selected, pending updates will be installed at the defined time every Friday.
- **Saturday:** If this option is selected, pending updates will be installed at the defined time



every Saturday.

- **Sunday:** If this option is selected, pending updates will be installed at the defined time every Sunday.

- **SCHEDULED INSTALL TIME**

Select the time for the installation by selecting the time in the dropdown menu. It is possible to select a value between 12 AM and 11 PM.

Auto Install and Reboot without End-User Control

AUTOMATIC UPDATE BEHAVIOR *
Auto install and reboot without end-user control
Manage automatic update behavior to scan, download and install updates.

When the **Auto install and reboot without end-user control** option is selected, RayManageSoft Unified Endpoint Manager automatically install and reboot the device without offering the end-user the option to postpone the update.

Reset to Default

AUTOMATIC UPDATE BEHAVIOR *
Reset to default
Manage automatic update behavior to scan, download and install updates.

When the **Reset to default** option is selected, RayManageSoft Unified Endpoint Manager will automatically download the update and inform the user when the update is ready for installation.



Group Management

The **Group Management** category of the sidebar contains the following subcategories:

- [Groups](#)

Groups

In the **Groups** section of RayManageSoft Unified Endpoint Manager, the different groups that have been configured are listed. The an image for the group as well as the name of the group, as well as the description and the priority assigned to the group are shown.

Name	Description	Priority
First Group	-	1
Second Group	-	2
Third Group	-	3
Fourth Group	-	4

The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the screen can be used to refresh the view.
- **Add** - The **Add** button on the top left of the screen can be used to add a group. For more information see Add a Group.

Be aware:
If AD-Sync is enabled, manual creation of groups as well as all kinds of group assignments are prohibited. In order to use these, AD-Sync needs to be disabled.

- **Edit** - The **Edit** button on the top left of the screen can be used to edit a group if one group in the list has been selected. For more information see Edit a Group.
- **Delete** - The **Delete** button on the top left of the screen can be used to delete one or more groups if one or more groups in the list have been selected.
- **Search field** - The **Search** field can be found on the top right of the screen. More information on how the search field works can be found in the Using Sorting, Filter, and Search Options section.



Group Details

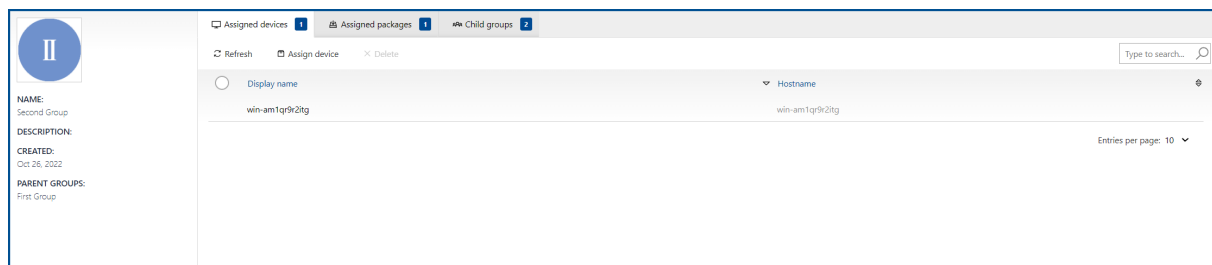
It is possible to open the details for a group by clicking on the group in the list. The **Group Details** show information about a group such as the image assigned to the group, the name of the group,, the description, the date of creation, and the parent groups if applicable.

Furthermore, there are three tabs containing further information which are available in the **Group Details**.

- [Assigned Devices](#)
- [Assigned Packages](#)
- [Child Groups](#)

Assigned Devices

The **Assigned devices** tab shows the list of devices that are assigned to a group. The devices are listed by their **Display name** and their **Hostname**.



The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the tab can be used to refresh the view.
- **Assign device** - The **Assign device** button on the top left of the tab can be used to assign one or more devices to the group.
- **Delete** - The **Delete** button on the top left of the tab can be used to delete one or more devices if one or more devices in the list have been selected.
- **Search field** - The **Search** field can be found on the top right of the tab. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.



Assign a Device to a Group

The **Add device assignment** dialog can be opened by using the **Add** button in the **Assigned Devices** tab.

Add device assignment

DEVICE
win-am1qr9r2itg

DEVICE DETAILS

DISPLAY NAME:	win-am1qr9r2itg
HOSTNAME:	win-am1qr9r2itg
DOMAIN:	WORKGROUP
OPERATING SYSTEM:	Microsoft Windows Server 2019 Standard
OWNER:	
LAST UPDATED:	10/26/22, 2:33 PM

Add Discard

A device can be selected by clicking in the **DEVICE** field. This will open a dropdown menu offering all available devices. To get a more precise list, enter the name of the device or a part of the name into the field. Depending on the devices still matching the string, this will significantly lower the number of devices in the list from which to select.

After selecting a device from the list, some details about the device will be shown below the field. These details include the display name, the hostname, the domain, the operating system, the owner, and the date of the last update. The device can now be added to the group by clicking on the **Add** button at the bottom of the dialog.

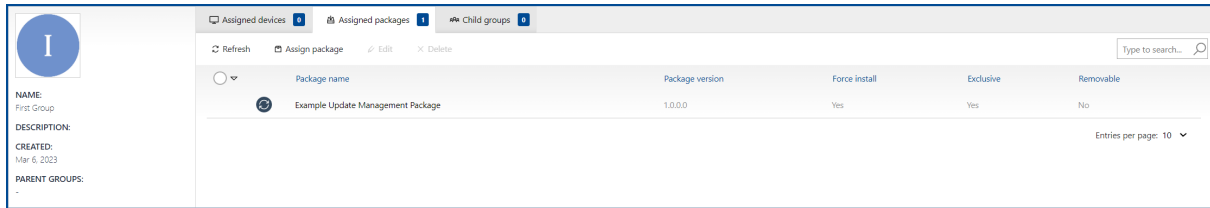


Be aware:

If AD-Sync is enabled, manual creation of groups as well as all kinds of group assignments are prohibited. In order to use these, AD-Sync needs to be disabled.

Assigned Packages

The **Assigned packages** tab shows the list of packages that are assigned to a group. The packages are listed by their **Package name**, if they will force an installation, if they have an exclusive flag and if they can be removed by the end-user.

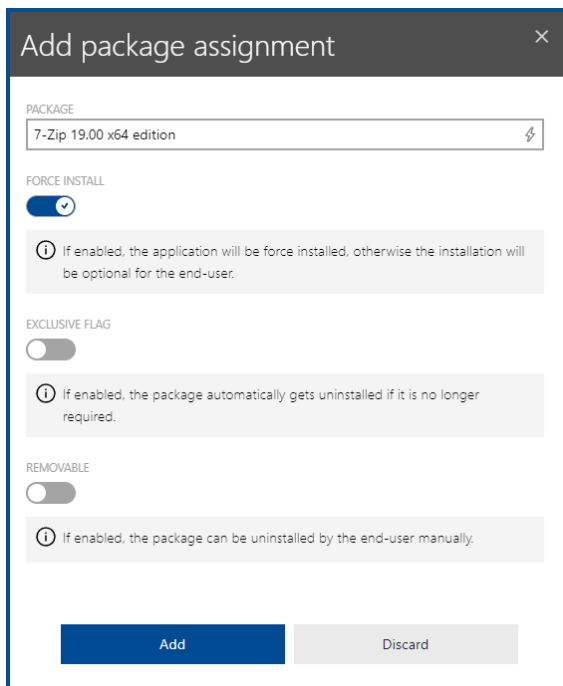


The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the tab can be used to refresh the view.
- **Assign package** - The **Assign package** button on the top left of the tab can be used to assign one or more packages to the group.
- **Edit** - The **Edit** button on the top left of the screen can be used to edit an assigned package if one package in the list has been selected. For more information see [Edit a Package Assigned to a Group](#).
- **Delete** - The **Delete** button on the top left of the tab can be used to delete one or more packages if one or more packages in the list have been selected.
- **Search field** - The **Search** field can be found on the top right of the tab. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.

Assign a Package to a Group

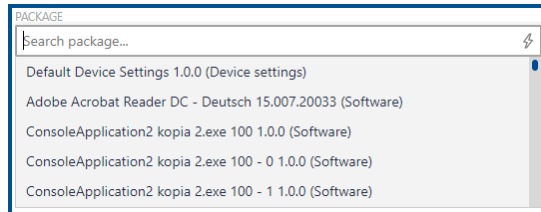
With the **Add package assignment** dialog it is possible to add a new package assignment from the list of the available packages to the group.



First select the package to assign from the list of available packages that will be shown when



clicking on the **PACKAGE** dropdown box. To get a more precise list, enter the name of the package or a part of the name into the field. Depending on the packages still matching the entered string, this will significantly lower the number of packages in the list from which to select.



After a package has been selected, further options of the dialog will become available.

- **FORCE INSTALL:** If this option is disabled, the end-user will be able to decide if the software package should be installed. If it is enabled, the package will be installed and the end-user will not be offered a choice. Furthermore, if this option has been set to active the **REMOVABLE** option will be added to the dialog.
- **EXCLUSIVE FLAG:** If the option is enabled, the package will be uninstalled if it is no longer deemed as required.
- **REMOVE ABLE:** If this option is enabled, the package can be manually uninstalled by the end-user even though **FORCE INSTALL** is enabled and the end-user cannot avoid the installation of the package.



Be aware:

If AD-Sync is enabled, manual creation of groups as well as all kinds of group assignments are prohibited. In order to use these, AD-Sync needs to be disabled.

Edit a Package Assigned to a Group

The **Edit package assignment** dialog is used to edit the settings for an existing package assignment.



Edit package assignment

PACKAGE

KeePass 2.x - 2.48.1.0

FORCE INSTALL

☒

i If enabled, the application will be force installed, otherwise the installation will be optional for the end-user.

EXCLUSIVE FLAG

☐

i If enabled, the package automatically gets uninstalled if it is no longer required.

REMOVABLE

☐

i If enabled, the package can be uninstalled by the end-user manually.

Save changes Discard

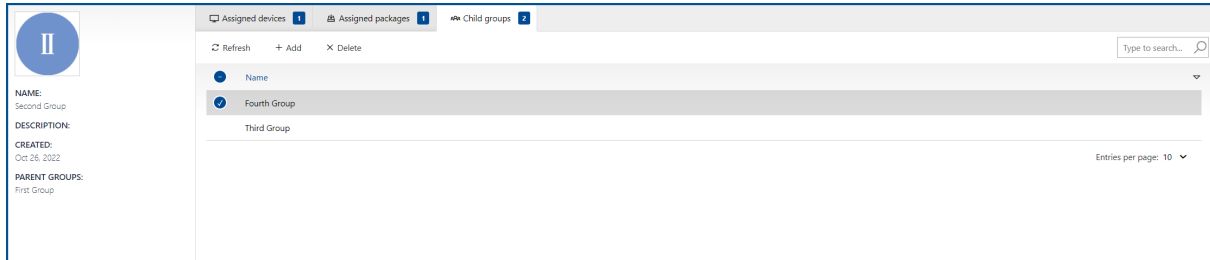
The following options are available for the selected package.

- **FORCE INSTALL:** If this option is disabled, the end-user will be able to decide if the software package should be installed. If it is enabled, the package will be installed and the end-user will not be offered a choice. Furthermore, if this option has been set to active the **REMOVABLE** option will be added to the dialog.
- **EXCLUSIVE FLAG:** If the option is enabled, the package will be uninstalled if it is no longer deemed as required.
- **REMOVE ABLE:** If this option is enabled, the package can be manually uninstalled by the end-user even though **FORCE INSTALL** is enabled and the end-user cannot avoid the installation of the package.



Child Groups

The **Child Groups** tab shows the list of groups that are assigned to the selected parent group. These child groups will inherit the package allocation details from their parent.

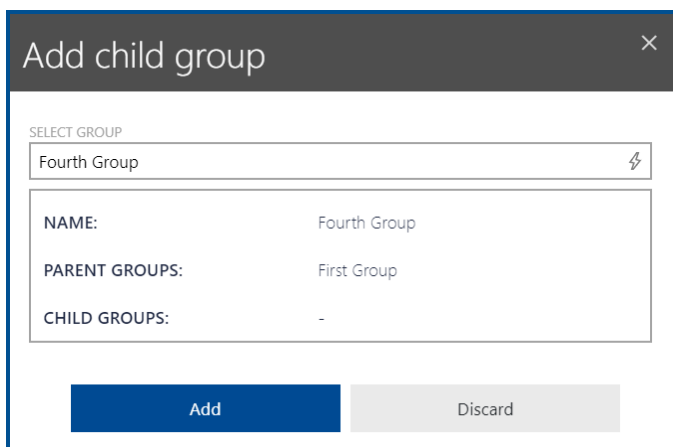


The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the tab can be used to refresh the view.
- **Add** - The **Add** button on the top left of the tab can be used to add a child group to the group.
- **Delete** - The **Delete** button on the top left of the tab can be used to delete one or more child groups if one or more child groups in the list have been selected.
- **Search field** - The **Search** field can be found on the top right of the tab. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.

Add a Child Group to a Group

The **Add child group** dialog can be opened by clicking on the **Add** button in the **Child Groups** tab.



In order to assign a child group, first select the group to assign as child group from the list of groups that will be shown when clicking on the **Group** dropdown box. To get a more precise list, enter the name of the group or a part of the name into the field. Depending on the groups still matching the entered string, this will significantly lower the number of groups in the list from which to select.



When the group has been selected, the name of the group, its parent groups, and its child groups will be shown below the **GROUP** field. The group can now be added as a child group by clicking on the **Add** button.

A group that has been assigned as a child group will inherit all assigned packages from its parent. This means that all devices in a group that has been assigned as a child to another group, will receive all packages from the parent group.

Add a Group

The **Add device group** dialog can be used to add a new group.



Be aware:

If AD-Sync is enabled, manual creation of groups as well as all kinds of group assignments are prohibited. In order to use these, AD-Sync needs to be disabled.



The following options are available in the dialog.

- **NAME:** Enter the name for the group into the **NAME** field. The name of the group needs to be unique. If the name is already in use, there will be a warning. The **NAME** field is mandatory.
- **DESCRIPTION:** A description of the group can be entered here. This field is optional.
- **PRIORITY:** Enter the priority of the group into this field. The value can be between 1 and 99999. The higher the value the lower the priority and the other way round. This means that a group with a priority of 1 most likely has the highest priority of all groups. If more than one group have the same priority, the groups will be sorted by name.
- **PICTURE:** It is possible to add a custom image to the group by clicking on the image in the **PICTURE** field. A file browser will be opened. Browse for an image to customize the image for the package (the following file formats are supported: .gif, .jpg, .jpeg, and .png).

Edit a Group

The **Edit device group** dialog can be used to edit an already existing group.

NAME *

Example Group

DESCRIPTION

Enter a description of the group here!

PRIORITY *

2

i Package assignments must be unique in the resulting policy. Hence, assignments are processed depending on the group priority starting with the highest.

PICTURE

I

Save changes Discard

The following options are available in the dialog.

- **NAME:** Enter the name for the group into the **NAME** field. The name of the group needs to be unique. If the name is already in use, there will be a warning. The **NAME** field is mandatory.



- **DESCRIPTION:** A description of the group can be entered here. This field is optional.
- **PRIORITY:** Enter the priority of the group into this field. The value can be between 1 and 99999. The higher the value the lower the priority and the other way round. This means that a group with a priority of 1 most likely has the highest priority of all groups. If more than one group have the same priority, the groups will be sorted by name.
- **PICTURE:** It is possible to add a custom image to the group by clicking on the image in the **PICTURE** field. A file browser will be opened. Browse for an image to customize the image for the package (the following file formats are supported: .gif, .jpg, .jpeg, and .png).



Administration

The **Administration** category of the sidebar contains the following subcategories.

- [Tenant Settings](#)
- [Device Settings](#)
- [Device Schedules](#)
- [Scheduled Tasks](#)
- [Integrations](#)

Tenant Settings

This section contains all important information regarding the currently selected tenant. It is divided into **Agent Installer Information**, **Device settings**, and **Database Maintenance**.

TENANT SETTINGS	
Agent Installer Information	
Administrator Administrator	The administrator will be visible during the installation process of the managed device agent.
Support Hotline	The support hotline will be visible during the installation process of the managed device agent.
Additional Installer Information This is the RMS UEM Managed Device Installer. Installing this software allows you to access the software deployment services of your company.	
The additional information will be visible during the installation process of the managed device agent.	
Device settings	
Allow new devices ✓	If set to true, the tenant will allow new devices.
Allow automatic merging of new devices X	Devices with the same hostname and domain will be automatically merged if they are not already managed.
Default device settings Default Device Settings (1.0.0.0)	This device settings will be deployed to every client in this tenant, to provide a set of basic settings, every device should have.
Default device schedule Default Device Schedule (1.0.0.0)	This device schedule package will be deployed to every client in this tenant, to provide a set of basic settings, every device should have.
Database Maintenance	
Automatic remove old activity logs Older than 90 days	Activity logs will be removed, if they exceeds the defined amount of days. (0 = Never)
Maximum amount of inventories a device should keep No limit	If there are more than the defined amount of inventories for a device, the oldest will be deleted, to not exceed the maximum amount of inventories. (0 = No limit)

Settings can be edited by clicking on the specific setting. A dialog where the setting can be edited will be opened.

- [Agent Installer Information](#)
- [Database Maintenance](#)
- [Device Settings](#)



Agent Installer Information

The **Agent Installer Information** section of the **Tenant settings** contains the following settings:

- [Administrator](#)
- [Support Hotline](#)
- [Additional Installer Information](#)

Administrator

The **Administrator** setting is used to define who will be shown as administrator during the installation process of the [managed device agent](#).

The screenshot shows a dialog box titled "Edit tenant setting" with a close button (X) in the top right corner. Inside the dialog, there is a label "ADMINISTRATOR:" followed by a text input field containing the word "Administrator". Below the input field is an information icon (i) and a message: "The administrator will be visible during the installation process of the managed device agent." At the bottom of the dialog, there are two buttons: "Save changes" (in blue) and "Discard" (in grey).

The default value is "Administrator".

Support Hotline

The **Support Hotline** setting is used to define if the support hotline will be shown during the installation process of the [managed device agent](#) or not.

The screenshot shows a dialog box titled "Edit tenant setting" with a close button (X) in the top right corner. Inside the dialog, there is a label "SUPPORT HOTLINE:" followed by a toggle switch that is currently turned on (blue with a white checkmark). Below the toggle switch is an information icon (i) and a message: "The support hotline will be visible during the installation process of the managed device agent." At the bottom of the dialog, there are two buttons: "Save changes" (in blue) and "Discard" (in grey).

If set to active (default), the support hotline will be shown. If set to inactive, the support hotline will not be shown.



Additional Installer Information

In the **Additional Installer Information** setting, it is possible to enter additional information that will be shown during the installation process of the [managed device agent](#).

The screenshot shows a dialog box titled "Edit tenant setting" with a close button (X) in the top right corner. Inside the dialog, there is a section labeled "ADDITIONAL INSTALLER INFORMATION:". Below this label is a text input field containing the text: "This is the RMS UEM Managed Device Installer. Installing this software allows y". Below the text field is an information icon (i) followed by the text: "The additional information will be visible during the installation process of the managed device agent." At the bottom of the dialog, there are two buttons: "Save changes" (in blue) and "Discard" (in grey).

By default, the entry is as follows:

"This is the RMS UEM Managed Device Installer. Installing this software allows you to access the software deployment services of your company."

Device Settings

The **Device Settings** section of the **Tenant settings** contains the following settings:

- [Allow new devices](#)
- [Allow automatic merging of new devices](#)
- [Default device settings](#)
- [Default device schedule](#)

Allow New Devices

The **Allow new devices** setting is used in order to define if the tenant will allow the addition of new devices.

The screenshot shows a dialog box titled "Edit tenant setting" with a close button (X) in the top right corner. Inside the dialog, there is a section labeled "ALLOW NEW DEVICES:". Below this label is a toggle switch that is currently turned on (blue) with a checkmark icon. Below the toggle switch is an information icon (i) followed by the text: "If set to true, the tenant will allow new devices." At the bottom of the dialog, there are two buttons: "Save changes" (in blue) and "Discard" (in grey).

If set to active (default), the tenant will allow the addition of new devices. If set to inactive, no new devices can be added to the tenant.



Allow Automatic Merging of New Devices

The **Allow automatic merging of new devices** setting is used in order to define if unmanaged devices with the same hostname and same domain will automatically be merged.

The screenshot shows a dialog box titled "Edit tenant setting" with a close button (X) in the top right corner. Inside the dialog, the section "ALLOW AUTOMATIC MERGING OF NEW DEVICES:" features a toggle switch that is currently turned off. Below the toggle, an information icon (i) is followed by the text: "Devices with the same hostname and domain will be automatically merged if they are not already managed." At the bottom of the dialog, there are two buttons: "Save changes" (in blue) and "Discard" (in grey).

If set to active, the tenant will automatically merge unmanaged devices with the same hostname and the same domain. If set to inactive (default), there will be no auto-merge.

Default Device Settings

The **Default device settings** setting is used in order to define which device settings will be deployed to each client in the tenant. This provides a basic set of settings that every device has.

The screenshot shows a dialog box titled "Edit tenant setting" with a close button (X) in the top right corner. Inside the dialog, the section "DEFAULT DEVICE SETTINGS:" features a text input field containing "Default Device Settings (1.0.0.0)" and a lightning bolt icon on the right. Below the input field, an information icon (i) is followed by the text: "This device settings will be deployed to every client in this tenant, to provide a set of basic settings, every device should have." At the bottom of the dialog, there are two buttons: "Save changes" (in blue) and "Discard" (in grey).

The **DEFAULT DEVICE SETTINGS** field supports auto-completion, therefore a list of all available device settings packages matching the current entry into the field will be shown when clicking into the empty field.

By default, the **Default Device Settings (1.0.0.0)** will be selected.



Default Device Schedule

The **Default device schedule** setting is used in order to define which device schedule package will be deployed to each client in the tenant. This provides a basic schedule for every device.

Edit tenant setting

DEFAULT DEVICE SCHEDULE:

Default Device Schedule (1.0.0.0)

i This device schedule package will be deployed to every client in this tenant, to provide a set of basic settings, every device should have.

Save changes Discard

The **DEFAULT DEVICE SCHEDULE** field supports auto-completion, therefore a list of all available device schedules matching the current entry into the field will be shown when clicking into the empty field.

By default, the **Default Device Schedule (1.0.0.0)** will be selected.

Database Maintenance

The **Database Maintenance** section of the **Tenant settings** contains the following settings:

- [Automatic remove old activity logs](#)
- [Maximum amount of inventories a device should keep](#)

Automatic Remove Old Activity Logs

The **Automatic remove old activity logs** setting is used in order to define the amount of time in days for which activity logs will be stored before they will be automatically deleted.

Edit tenant setting

AUTOMATIC REMOVE OLD ACTIVITY LOGS:

90

i Automatic remove old activity logs

Save changes Discard

Enter the number of days for which the logs shall be kept. It is possible to keep the logs between 1 and 2,147,483,647 days. If 0 is entered, the logs will never be automatically removed. By



default, the setting is set to 90 days.



Maximum Amount of Inventories a Device Should Keep

The **Maximum amount of inventories a device should keep** setting is used in order to define the amount of inventories that will be kept by a devices before the oldest log will be deleted in order to not exceed the maximum amount of inventories.

Enter the number of inventories that a device should keep. Once this number is reached, the oldest inventory will be deleted. It is possible to keep between 1 and 2,147,483,647 inventories. If 0 is entered, there is no limit to the number of inventories that are being kept. By default, this setting is set to 0 (no limit).

Device Settings

The following chapter describes in detail how to add and configure the device settings using RayManageSoft Unified Endpoint Manager and its dialogs. For even more detailed information on device settings and even more advanced ways for their configuration refer to [Appendix I: Preference Settings for Managed Devices](#).

The **Device Settings** section contains an overview of the sets of device settings currently configured.

Status	Name	Version	Comment
OK	Default Device Settings	1.0.0.0	This default device settings will be applied to every device in this tenant. This settings can be overwritten by device settings assigned to a device or group.
OK	New Settings	1.0.0.0	-

The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the screen can be used to refresh the view.
- **Add** - The **Add** button on the top left of the screen can be used to add a new set of device settings to the list. For more information see [Add Device Settings](#).
- **Delete** - The **Delete** button on the top left of the screen can be used to delete one or more sets of device settings if one or more sets in the list have been selected.
- **Search field** - The **Search** field can be found on the top right of the screen. More information



on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.

When clicking on the name of a set of device settings, the set will be opened.

Device Settings Details

When opening the details for a set of device settings, these consist of two parts. The left part contains some general information of the device settings.



On the right side the specific device settings are listed. This part is divided into different tabs which each contain related settings.

The following tabs are available.

- [Common](#)
- [Installation Agent](#)
- [Inventory Agent](#)
- [Policy Agent](#)
- [AppCenter](#)
- [Upload Agent](#)
- [Contact](#)



Default Device Settings

The default device setting will be applied to every device that has no other device settings assigned.

- [Default Device Settings Common tab](#)
- [Default Device Settings Installation Agent tab](#)
- [Default Device Settings Inventory Agent tab](#)
- [Default Device Settings Policy Agent tab](#)
- [Default Device Settings AppCenter tab](#)
- [Default Device Settings Upload Agent tab](#)
- [Default Device Agent Contact tab](#)

Common

Security

Setting	Default Value	Description
Check certificate revocation	Yes	Specifies whether the RMS UEM AppCenter checks the certificate revocation lists when accepting web server certificates from an HTTP server.
Check web server certificate	Yes	Specifies whether the RMS UEM AppCenter validates web server certificates when connecting to an HTTPS server.

Installation Agent

General

Setting	Default Value	Description
Connection attempts	2	Specifies the number of times the installation agent should try to connect to the distribution server.
Detect application version conflicts	No	Specifies whether the installation agent detects and fails differing versions of single applications.
HTTP proxy	{empty}	Specifies the proxy URL to be used by the installation agent.



Logging

Setting	Default Value	Description
Log file	<code>\$(TempDirectory)\ManageSoft\installation.log</code>	Specifies the name of the file used to store the logging information.
Log file size	4000000	Specifies the maximum size of the log file.
Log level	A-z	Specifies the logging level for the policy agent. For detailed information on logging refer to Appendix II: Logging on Managed Devices .
Old log file	<code>\$(TempDirectory)\ManageSoft\installation.old.log</code>	Specifies the name of the file in which additional logging information is stored.

Bandwidth Settings

Setting	Default Value	Description
Network high speed	0	Specifies the lowest network speed (in bits per second) that the RMS UEM AppCenter will consider to be a high speed network connection to a server.
Network high usage	100	Specifies the maximum percentage of bandwidth that the RMS UEM AppCenter uses for uploads and downloads on a high-speed connection.
Network high usage lower limit	100	Specifies the minimum Network high usage value that can be set for a managed device by an end-user moving the bandwidth usage slider control in the installation agent.
Network high usage upper limit	100	Specifies the maximum Network high usage value that can be set for a managed device by an end-user moving the bandwidth usage slider control in the installation agent.
Network low usage	100	Specifies the maximum percentage of bandwidth that the RMS UEM AppCenter uses for uploads and downloads on a low-speed connection.



Setting	Default Value	Description
Network low usage lower limit	100	Specifies the minimum Network low usage value that can be set for a managed device by an end-user moving the bandwidth usage slider control in the installation agent.
Network low usage upper limit	100	Specifies the maximum Network low usage value that can be set for a managed device by an end-user moving the bandwidth usage slider control in the installation agent.
Network max rate	0	Specifies the bytes per second at which the managed device accesses the data over the network. The setting is not used if the network speed setting can be determined and the network high speed is set to a non-zero value.
Network min speed	0	Specifies the minimum network speed (in bits per second) for the RMS UEM AppCenter to initiate a check for updates.
Network retries	1	Specifies the number of times a failed network operation is retried before an alternative download location is attempted.
Network timeout	30	Specifies the length of time in seconds of inactivity after which a network operation will time out.

File Handling

Setting	Default Value	Description
No stage	No	Specifies whether the files are downloaded directly to their destination folder or a staging area.
Force shared file remove	No	Specifies whether the deletion of redundant files in the Windows system folder is allowed.
Stage inactive packages	No	Specifies whether inactive packages are staged before the installation occurs.

MSI Package Processing



Setting	Default Value	Description
Msi reinstall features	ALL	Specifies which MSI component will be installed. This option is Windows only!
Msi reinstall mode level	osmu	Specifies what will be reinstalled. This option is Windows only!
Msi repair	No	Specifies whether the repairs are performed at the same time as the RMS UEM AppCenter self-healing operations. This option is Windows only!
Msi repair level	vomus	Specifies what will be repaired. This option is Windows only!
Msi source location	Windows installer cache	Specifies whether Windows Installer packages are installed from the local Windows Installer cache of the managed device or from a distribution location. This option is Windows only!
Msi UI level	/qb	Specifies the user interaction level for MSI. This option is Windows only!
Msi uninstall args	{empty}	Specifies the arguments for uninstall operations to include in the MSI command-line. This option is Windows only!

Reboot

Setting	Default Value	Description
Allow reboot if locked	No	Specifies whether the RMS UEM AppCenter reboots the managed device even if the machine is locked if the package being installed requires it.
Allow reboot if server	No	Specifies whether the RMS UEM AppCenter reboots the managed device if it is a server. This setting is only used by the adoption agent.
Allow timeout if locked	Yes	Specifies whether the RMS UEM AppCenter reboot events wait for the machine to become unlocked before



Setting	Default Value	Description
		proceeding with a reboot.
Always display reboot	No	Specifies whether the RMS UEM AppCenter displays a warning to the user before performing any reboot required by a package installation.
Continue after command failure	Yes	Specifies whether to proceed with the requested reboot if the prereboot command returns a non-zero exit code.
Display the shutdown button	No	Displays a Shutdown button to the users on the reboot dialog in addition to the Reboot button.
Force reboot	No	Specifies whether the RMS UEM AppCenter forces a reboot if the package installed requires it. This setting suppresses any user interaction required to close other applications that may be running.
Force reboot if locked	Yes	Specifies whether the RMS UEM AppCenter performs a forced reboot if the machine is locked.
Force reboot window to top	No	Forces the reboot dialog to be the top window during the final stage of user prompting
Post reboot command	{empty}	Specifies the command to be run after a RMS UEM AppCenter requested reboot occurs.
Pre reboot command	{empty}	Specifies the command to be run before a RMS UEM AppCenter requested reboot occurs.
Prompt cycle wait time	600	Specifies the length of the reboot prompt cycles in seconds.
Reboot command-line	\$(RebootPath)	Specifies the command used to perform a reboot on the managed device.
Reboot if required	No	Specifies the default response to dialogs that prompt the user to allow a reboot.
Reboot log file	\$(TempDirectory) \ManageSoft \RMSReboot.log	Specifies the name of the file in which to store the logging information.
Reboot path	\$(RebootPath) \RMSReboot.exe	Specifies the full path to the command-



Setting	Default Value	Description
		line used to reboot managed devices.
Reboot prompt cycles	0	Specifies the number of times the user is prompted to reboot. The user is given the option to reboot or to postpone until these cycles are completed.
Security patch reboot if required	Yes	Specifies the default response to dialogs displayed during security patch installation that prompts the user to allow a reboot..
Unlimited reboot prompting	No	If set to Yes , this is the equivalent to an infinite number of Reboot prompt cycles .

Self-heal

Setting	Default Value	Description
Self-heal	True	Specifies whether self-healing should occur. True means that all packages on this endpoint should self-heal. False means that no packages on this endpoint should self-heal. Any other value means, that self-healing is only attempted on packages with a custom property whose name matches the value of <code>SelfHeal</code>. Note: The custom property value is not but it must not have a non-empty to take effect.

Inventory Agent

General

Setting	Default Value	Description
Create inventory event logs	Yes	Specifies whether the RMS UEM AppCenter should create inventory event logs.
Inventory file	<code>\$(UserName) on \$(MachineId).ndi</code>	Specifies the file name of a local copy of the inventory file.



Setting	Default Value	Description
Machine inventory directory	<code>\$ (CommonAppDataFolder) \ManageSoft Corp \ManageSoft \Tracker \Inventories</code>	Specifies the location for machine inventories.
Minimum inventory interval	0	Specifies the minimum interval (in hours) between the collection of inventories.
Permit temporary execution of console mode application	No	Specifies whether to permit the execution of console mode applications on locked down Windows 9x desktops for zero-touch hardware inventory collection.
Progress depth	10	Specifies the number of directory levels to search at the initialization to approximate the number of directories searched during tracking.
SMBIOS command-line	<code>conspawn smbios2.exe /I /G</code>	Specifies the command-line for non-WMI hardware inventory collection.

Logging

Setting	Default Value	Description
Log file	<code>\$ (TempDirectory) \ManageSoft \Tracker.log</code>	Specifies the name of the file used to store the logging information.
Log file size	4000000	Specifies the maximum size of the log file.
Log level	A-z	Specifies the logging level for the inventory agent. For detailed information on logging refer to Appendix II: Logging on Managed Devices .
Old log file	<code>\$ (TempDirectory) \ManageSoft \Tracker.old.log</code>	Specifies the name of the file in which additional logging information is stored.

Scanning Options

Setting	Default Value	Description
RMS UEM AppCenter Packages	Yes	Specifies whether information about RMS UEM AppCenter packages is included in the inventories.



Setting	Default Value	Description
Embed file content directory	<code>\$(CommonAppDataFolder); \$(ProgramFilesX64Folder); \$(ProgramFilesX86Folder)</code>	Specifies the folders that will be scanned for embedding file content into the inventory. This option is Windows only!
Embed file content extension	<code>swidtag</code>	Specifies the file extensions that will have content embedded into the inventory.
Embed file content max size	<code>1000000</code>	Specifies the maximum file size to consider when embedding file contents into the inventory.
Exclude directories	<code>{empty}</code>	Specifies the folders to exclude from the inventory.
Exclude embed file content directory	<code>{empty}</code>	Specifies the folders that will be excluded from the scan for embedding file content into the inventory.
Exclude extension	<code>{empty}</code>	Specifies the file extensions to exclude from the inventory. This may include a leading dot and can be only a dot to specify files without extension.
Exclude file	<code>{empty}</code>	Specifies the files to exclude from the inventory.
Exclude file system types	<code>{empty}</code>	Specifies the types of file systems for which files will never be included in the inventory. This option is non-windows only!
Exclude MD5	<code>{empty}</code>	Specifies the MD5 for files that are excluded from the inventory.
Exclude permissions mask	<code>{empty}</code>	Specifies which files should not be scanned during a RMS UEM AppCenter inventory. The value should be an octal mask for file permissions in the format used by the <code>chmod</code> command. Files which match the mask will be excluded from the scan. If an exclamation is added before the mask, the files which do not match this mask will be excluded from the scan. This option is non-windows only!
Generate MD5	<code>No</code>	Specifies whether to generate MD5 checksums for files that are reported in the inventory.



Setting	Default Value	Description
Hardware	Yes	Specifies whether to track the hardware inventory when generating a machine inventory.
Include directory	{empty}	Specifies the folders to include into the inventory.
Include executable files	Yes	Include files that are executables. An executable on Windows is defined as a file which ends in .exe. On Unix, an executable is a file without an extension and with one or more of its executable bits being set.
Include extension	{empty}	Specifies the file extensions to include in the inventory. This may include a leading dot and can be only a dot to specify files without extensions.
Include file	{empty}	Specifies the files to be included in the inventory.
Include file system types	ufs, zfs, lofs	Specifies the types of file systems for which files will always be included in the inventory. This option is non-windows only!
Include MD5	{empty}	Specifies an MD5 for files to include in the inventory.
Include MSI packages in inventory	Yes	Specifies whether the information about MSI packages is included in the inventories. This option is Windows only!
Include permissions mask	{empty}	Specifies which files should be scanned during a RMS UEM AppCenter inventory. The value should be an octal mask for file permissions in the format used by the <code>chmod</code> command. Files which match the mask will be included in the inventory. If an exclamation mark is added before the mask, the files which do not match this mask will be included in the inventory.
Include registry key	{empty}	Specifies the registry keys or values to be included in the inventory. Additionally, this setting cannot have customized values. Multiple values need to be separated by commas. This option is Windows only!



Setting	Default Value	Description
Inventory scripts	{empty}	Specifies the scripts to run during the machine inventory. Due to its nature, this setting may be available to only a subset of the environments, languages, and architectures of the package. Additionally, this setting cannot have customized values.
Inventory scripts directory	\$(ScriptDir) \ InventoryScanning OptionsInventory Scripts	Specifies the location of the inventory scripts on the endpoint. Due to its nature, this setting may be available to only a subset of environments, languages, and architectures of the package.
MSI product codes to inspect fully	{empty}	Specifies the product codes which are to be inspected fully. This involves calculating the result of all applied transforms and patches before the retrieval of the UpgradeCode and PIDKEY properties. The value * includes all products. Additionally this setting cannot have customized values. Separate values by commata. This option is Windows only!
Platform-specific packages	Yes	Specifies whether information about platform-specific packages (for example .lpp, .pkg, .rpm, and .sd-ux) is included in inventories.
Recurse	Yes	Specifies whether child folders are included in the inventory.
Run inventory scripts	No	Specifies whether to execute any custom inventory scripts found by plugins. Due to its nature, this setting may be available to only a subset of the environments, languages, and architectures of a package.
Version info	Yes	Specifies whether the file version header information is included in the inventory.
WMI	Yes	Specifies whether WMI tracking is specified as preferred option for tracking hardware. This option is Windows only!



Policy Agent

General

Setting	Default Value	Description
Policy server priority	50	Specifies the numerical priority to be assigned to the location from which policy files (.npl) were obtained when using it as a location for downloading packages.

Logging

Setting	Default Value	Description
Log file	\$(TempDirectory) \ManageSoft \policy.log	Specifies the name of the file used to store logging information.
Old log file	\$(TempDirectory) \ManageSoft \policy.old.log	Specifies the name of the file used to store additional logging information.
Log level	A-z	Specifies the logging level for the policy agent. For detailed information on logging refer to Appendix II: Logging on Managed Devices .
Log file size	4000000	Specifies the maximum size of the log file.

Merging

Setting	Default Value	Description
Apply local policy	No	Specifies whether to use the locally cached copy of a policy if a new policy cannot be generated.
Auto detect DC	Yes	Specifies how the RMS UEM AppCenter selects a domain controller for client side policy merging.
Disable package filtering	No	Specifies whether bypassing package-level filtering is allowed during a policy merge if filtering is not required.
Enable policy failover	No	Specifies if the failover to the server side policy merging should happen or not.
GP Client side Extension enabled	No	Specifies whether the Group Policy Client Side Extension should be executed.



Setting	Default Value	Description
Launcher command-line	{empty}	Specifies the installation agent command-line options to pass to the RMS UEM AppCenter when applying policy information.
Machine policy command	"\$(ProgramFiles)\ManageSoft\nPolicy Client\mgspolicy.exe" -t Machine	The command to execute to perform an application of the machine policy on the managed device.
Minimum DC speed	0	Specifies the minimum network speed (in bits per second) between the managed device and the domain controller that is required to apply a policy. This setting only applies for client-side policy merging when <code>AutoDetectDC</code> is set to <code>False</code> .
Report compliance	No	Specifies whether endpoints will report policy compliance.  Note: This setting should not be changed from the default value of <code>False</code> as policy compliance logs are currently not imported by the RMS UEM AppC
Retry policy	Yes	Specifies whether the RMS UEM AppCenter will attempt to retrieve a policy when the endpoint boots if no machine schedule exists on the endpoint.
Retry policy command	mgspolicy.exe -t Machine -o UserInteraction Level=Quiet	Specifies the command that is used if <code>RetryPolicy</code> is set to <code>True</code> .

Locations

Setting	Default Value	Description
Machine policy package directory	\$(CommonAppDataFolder)\ManageSoft Corp\ManageSoft\nPolicy client\Packages	Specifies the location where the package information associated with the machine policy is cached.



Setting	Default Value	Description
Machine policy directory	<code>\$ (CommonAppDataFolder) \ManageSoft Corp \ManageSoft \Policy Client \Policies\Merged \Machine</code>	Specifies the location where the active machine policies will be saved.

AppCenter

General

Setting	Default Value	Description
Refresh period	5	Specifies the number of minutes between the automatic refresh of the data displayed by the RMS UEM AppCenter user interface on a managed device.
Locale	<code>\$ (UserLocale)</code>	Specifies the locale setting used by the RMS UEM AppCenter.
Default locale	EN	Specifies the default locale setting used by the RMS UEM AppCenter.
Default configuration file	<code>\$ (SkinsDirectory) \Default \\$ (Locale) \\$ (ConfigName)</code>	Specifies the name of the default configuration file used by the RMS UEM AppCenter user interface on the endpoint.
Configuration file	<code>\$ (Config FileDefault)</code>	Specifies the name of the configuration file used by the RMS UEM AppCenter user interface on managed devices.
Application verify command	<code>ndlaunch -a "{1}" -o SaveAllUser Symbols=False -o MsiRepair=True -o CachedVersion =True -o SelfHeal=True -o CheckRegistry =True -o NoExec=True {2}</code>	Specifies the template command-line to be used to verify/repair an application package through the RMS UEM AppCenter package selection agent.
Application uninstall command	<code>ndlaunch -d "{1}" -o SaveAllUser Symbols=False {2}</code>	Specifies the template command-line to be used to uninstall an application package through the RMS UEM AppCenter package selection agent.



Setting	Default Value	Description
Application install command	<code>ndlaunch -r "{1}" -o SaveAllUser Symbols=False {2}</code>	Specifies the template command-line to be used to install an application package through the RMS UEM AppCenter package selection agent.

Logging

Setting	Default Value	Description
Log file	<code>\$(TempDirectory) \ManageSoft \selector.log</code>	Specifies the name of the file to store logging information.
Old log file	<code>\$(TempDirectory) \ManageSoft \selector.old.log</code>	Specifies the name of the file to store additional logging information.
Log level	A-z	Specifies the logging information level for the policy agent. For detailed information on logging refer to Appendix II: Logging on Managed Devices .
Log file size	4000000	Specifies the maximum log file size.

Upload Agent

General

Setting	Default Value	Description
Upload inventory files	Yes	Specifies whether the RMS UEM AppCenter should upload inventory files immediately after generation.
Policy compliance log	<code>\$(ServerLocation) \PolicyCompliance Logs\\$(UserId) on \$(MachineId) at \$(DateTime).plc</code>	Specifies the location where the RMS UEM AppCenter uploads policy compliance log files from the endpoint.
Log	<code>\$(ServerLocation) \Logs\\$(MachineId) at \$(DateTime)_ \$(GUID).log</code>	Specifies the location where the RMS UEM AppCenter uploads logging files from the endpoint.



Setting	Default Value	Description
Inventory	<code>\$(ServerLocation)\Inventories\\$(UserId) on \$(MachineId) at \$(DateTime) (\$(Generation)).ndi</code>	Specifies the location where the RMS UEM AppCenter uploads inventory files.

Bandwidth Settings

Setting	Default Value	Description
Network timeout	600	Specifies the length of time in seconds of inactivity after which a network operation will time out.
Network min speed	0	Specifies the minimum network speed (bits per second) for the RMS UEM AppCenter to initiate a check for updates.
Network max rate	0	Specifies the bytes per second at which the endpoint uploads data over the network. This setting is not used if the <code>NetworkSpeed</code> setting can be determined and the <code>NetworkHighSpeed</code> is set to a non-zero value.
Network low usage lower limit	100	Specifies the minimum <code>NetworkLowUsage</code> value that can be set for an endpoint by an end-user moving the bandwidth usage slider control in the upload agent.
Network low usage	100	Specifies the maximum percentage of bandwidth that the RMS UEM AppCenter uses for uploads on a low-speed connection.
Network high usage upper limit	100	Specifies the maximum <code>NetworkHighUsage</code> value that can be set for an endpoint by the end-user moving the bandwidth usage slider control in the upload agent.
Network high usage	100	Specifies the maximum percentage of bandwidth that the RMS UEM AppCenter uses for uploads on a high-speed connection.
Network high speed	0	Specifies the lowest network speed (in bits per second) that the RMS UEM



Setting	Default Value	Description
		AppCenter will consider to be a high speed network connection to a server.

Logging

Setting	Default Value	Description
Log file	<code>\$(TempDirectory)\ManageSoft\Uploader.log</code>	Specifies the name of the file in which to store the logging information.
Old log file	<code>\$(TempDirectory)\ManageSoft\uploader.old.log</code>	Specifies the name of the file in which to store additional logging information.
Log level	A-z	Specifies the logging level for the upload agent. For detailed information on logging refer to Appendix II: Logging on Managed Devices .
Log file size	4000000	Specifies the maximum log file size.

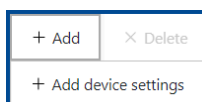
Contact

General

Setting	Default Value	Description
Support URL	{empty}	Specifies the support URL displayed to end-users within the RMS UEM AppCenter.
Support Telephone	{empty}	Specifies the support telephone number displayed to end-users within the RMS UEM AppCenter.
Contact person	{empty}	Specifies the contact person displayed to end-users within the RMS UEM AppCenter.

Add Device Settings

Click on the **Add** button in the **Device Settings** section and select the **Add device settings** option to open the **Add device settings** dialog.





In the **Add device settings** dialog it is possible to define some general information regarding the set of device settings that is being added.

ADD device settings

IMAGE

NAME *

Example Device Settings

VERSION *

1 0 0 0

i The version number is used by the Deployment Manager on the managed devices to coordinate application updates. Increase this number whenever you want to distribute a revised version of your application.

COMMENT

Enter a comment here!

Add Discard

The following options are available in the dialog.

- **IMAGE:** Clicking on the image will open a file browser. Browse for an image to customize the image for the set of device settings (the following file formats are supported: .gif, .jpg, .jpeg, and .png).
- **NAME:** The name for the set of device settings.
- **VERSION:** The version number of the settings which is further divided into:
 - Major
 - Minor
 - Build
 - RevisionSince the fields have already been separated, no further separators are allowed.
- **COMMENT:** A comment or a short description of the device settings can be added into the **COMMENT** field. Entering a comment is optional.

After clicking on the **Add** button the new set of device settings will be created using the default setting for each of the specific settings. The specific settings can now be edited in order to customize the new set of settings.



Edit Device Settings

Go on the details of a device setting package in order to edit the settings. A specific device setting can be edited by clicking on the setting. When moving the mouse pointer over a specific setting, an **Edit** symbol will appear at the right side of the setting.

A description of the options for editing the different device settings can be found in the following. All device settings have the option to revert the setting to its default value.

Common

The **Common** section of the **Device Settings** is divided into the following subcategories:

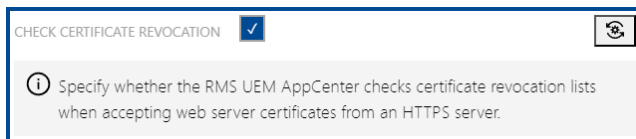
- [Security](#)

Security

All settings which affect security related functions are found in this subcategory.

- [Check Certificate Revocation](#)
- [Check Web Server Certificate](#)

Check Certificate Revocation



This setting specifies whether the RMS UEM AppCenter checks the certificate revocation list when accepting web server certificates from an HTTPS server.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Detailed information about this setting and its usage on endpoints can be found [here](#).



Check Web Server Certificate

This setting specifies whether the RMS UEM AppCenter validates the web server certificates when connecting to an HTTPS server.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Installation Agent

The **Installation Agent** section of the **Device Settings** is divided into the following subcategories:

- [General](#)
- [Logging](#)
- [Bandwidth Settings](#)
- [File Handling](#)
- [Msi Package Processing](#)
- [Reboot](#)
- [Self-heal](#)

General

All general settings for the installation agent are found in this subcategory.

- [Connection Attempts](#)
- [Detect Application Version Conflicts](#)
- [HTTP Proxy](#)

Connection Attempts

This setting specifies the number of times the installation agent should try to connect to the



distribution server.

Possible values:	Integer
Default value:	2
Example value:	10

Detailed information about this setting and its usage on endpoints can be found [here](#).

Detect Application Version Conflicts

This setting specifies whether the installation agent detects and fails differing versions of an application.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

HTTP Proxy

This setting specifies the proxy URL that is to be used by the installation agent.

Possible values:	A valid URL
Default value:	{empty}
Example value:	raynet-proxy.de

Detailed information about this setting and its usage on endpoints can be found [here](#).

Logging

All settings which affect the logging functions of the installation agent are found in this subcategory.



- [Log File](#)
- [Log File Size](#)
- [Log Level](#)
- [Old Log File](#)



Log File

LOG FILE

Specify the name of the file to store logging information.

This setting specifies the path and filename where RayManageSoft Unified Endpoint Manager stores the logging information.

Possible values:	A local or a UNC network file
Default value:	<code>\$ (TempDirectory) \ManageSoft \installation.log</code>
Example value:	<code>C:\temp\Installation.log</code>

Detailed information about this setting and its usage on endpoints can be found [here](#).

Log File Size

LOG FILE SIZE

Specify the maximum log file size.

This setting specifies the maximum size of the log file (in bytes).

Possible values:	Integer (bytes)
Default value:	4000000
Example value:	3126000 (3 MB)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Log Level

LOG LEVEL

Specify the logging level for the install agent.

This setting specifies the level of logging for the installation agent.

Possible values:	One or more logging levels
Default value:	A-z (logs everything)
Example value:	G0, 4



Detailed information about this setting and its usage on endpoints can be found [here](#).
More information regarding logging and levels of logging can be found in the [Appendix II: Logging on Managed Devices](#).

Old Log File

This setting specifies the path and filename where RayManageSoft Unified Endpoint Manager stores additional logging information.

Possible values:	A local or UNC network file
Default value:	<code>\$(TempDirectory)\ManageSoft\installation.old.log</code>
Example value:	<code>C:\temp\Installation_old.log</code>

Detailed information about this setting and its usage on endpoints can be found [here](#).

Bandwidth Settings

All settings which affect the level bandwidth usage of the installation agent are found in this subcategory.

- [Network High Speed](#)
- [Network High Usage](#)
- [Network High Usage Lower Limit](#)
- [Network High Usage Upper Limit](#)
- [Network Low Usage](#)
- [Network Low Usage Lower Limit](#)
- [Network Low Usage Upper Limit](#)
- [Network Max Rate](#)
- [Network Min Speed](#)
- [Network Retries](#)
- [Network Timeout](#)

Network High Speed



This setting specifies the lowest network speed (in bits per second) that the RMS UEM AppCenter will consider to be a high speed network connection to a server.

Possible values:	Integer (bits in seconds)
Default value:	0 (not limited)
Example value:	1 0

Detailed information about this setting and its usage on endpoints can be found [here](#).

Network High Usage

This setting specifies the maximum percentage of bandwidth that the RMS UEM AppCenter uses for uploads and downloads on a high-speed connection.

Possible values:	Integer between 0 - 100
Default value:	1 0 0
Example value:	1 0 0

Detailed information about this setting and its usage on endpoints can be found [here](#).

Network High Usage Lower Limit

This setting specifies the minimum Network High Usage value that can be set for a managed device by the end-user moving the bandwidth usage slider control in the installation agent.

Possible values:	Integer between 0 - 100
Default value:	1 0 0
Example value:	1 0 0



Detailed information about this setting and its usage on endpoints can be found [here](#).

Network High Usage Upper Limit

This setting specifies the minimum Network Low Usage value that can be set for a managed device by an end-user moving the bandwidth usage slider control in the installation agent.

Possible values:	Integer between 0 - 100
Default value:	100
Example value:	100

Detailed information about this setting and its usage on endpoints can be found [here](#).

Network Low Usage

This setting specifies the maximum percentage of bandwidth that the RMS UEM AppCenter uses for uploads and downloads on a low-speed connection.

Possible values:	Integer between 0 - 100
Default value:	100
Example value:	100

Detailed information about this setting and its usage on endpoints can be found [here](#).

Network Low Usage Lower Limit

This setting specifies the minimum Network Low Usage that can be set for a managed device by



an end-user moving the bandwidth usage slider control in the installation agent.

Possible values:	Integer between 0 - 100
Default value:	100
Example value:	100

Detailed information about this setting and its usage on endpoints can be found [here](#).

Network Low Usage Upper Limit

This setting specifies the maximum Network Low Usage that can be set for a managed device by an end-user moving the bandwidth usage slider control in the installation agent.

Possible values:	Integer between 0 - 100
Default value:	100
Example value:	100

Detailed information about this setting and its usage on endpoints can be found [here](#).

Network Max Rate

This setting specifies the bytes per second at which the managed device accesses data over the network. The setting is not used if the network speed setting can be determined and the network high speed is set to a non-zero value.

Possible values:	Integer (bytes per second)
Default value:	0 (unlimited)
Example value:	0

Detailed information about this setting and its usage on endpoints can be found [here](#).



Network Min Speed

NETWORK MIN SPEED

Specify the minimum network speed (bits per second) for the RMS UEM AppCenter to initiate a check for updates.

This setting specifies the minimum network speed in bits per second for the RMS UEM AppCenter to initiate a check for updates.

Possible values:	Integer
Default value:	0
Example value:	0

Detailed information about this setting and its usage on endpoints can be found [here](#).

Network Retries

NETWORK RETRIES

Specify the number of times a failed network operation is retried before an alternative download location is attempted.

This setting specifies the number of times a failed network operation is retried before an alternative download location is attempted.

Possible values:	Integer
Default value:	1
Example value:	1

Detailed information about this setting and its usage on endpoints can be found [here](#).

Network Timeout

NETWORK TIMEOUT

Specify the length of time in seconds of inactivity after which a network operation will time out.

This settings specifies the length of time in seconds of inactivity after which a network operation will time out.



Possible values:	Integer
Default value:	30
Example value:	30

Detailed information about this setting and its usage on endpoints can be found [here](#).

File Handling

All settings which affect how the installation agent handles files are found in this subcategory.

- [No Stage](#)
- [Force Shared File Remove](#)
- [Stage Inactive Packages](#)

No Stage

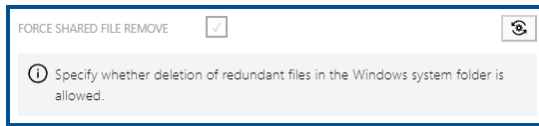
This setting specifies whether files are downloaded directly to their destination folder (Yes) or if they are first downloaded to a staging area (No). By default, the files are downloaded to the staging area first.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).



Force Shared File Remove

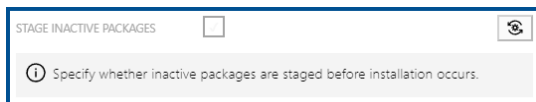


This setting specifies whether the deletion of redundant files in the Windows system folder is allowed. By default, the deletion of redundant files in the Windows system folder is prohibited.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Stage Inactive Packages



This setting specifies whether inactive packages are staged before the installation occurs. By default, inactive packages are not downloaded to the staging area until the policy is activated.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Msi Package Processing

All settings which affect the processing of MSI packages are found in this subcategory.

- [Msi Reinstall Features](#)
- [Msi Reinstall Mode Level](#)
- [Msi Repair](#)
- [Msi Repair Level](#)
- [Msi Source Location](#)
- [Msi UI Level](#)



- [Msi Uninstall Args](#)

Msi Reinstall Features

This option is Windows only!

This setting specifies which MSI components will be installed.

Possible values:	The features that are to be installed.
Default value:	ALL
Example value:	ALL

Detailed information about this setting and its usage on endpoints can be found [here](#).

Msi Reinstall Mode Level

This option is Windows only!

This setting specifies what will be reinstalled.

Possible values:	Any combination of the following letters: a, c, d, e, m, p, o, s, u, v.
Default value:	osmu
Example value:	vomus (complete reinstall)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Msi Repair

This option is Windows only!



This setting specifies whether repairs are performed at the same time as RMS UEM AppCenter self-healing operations.



Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Msi Repair Level

This option is Windows only!

This setting specifies what will be repaired.

Possible values:	Any combination of the following letters: a, c, d, e, m, p, o, s, u, v.
Default value:	vomus
Example value:	omus

Detailed information about this setting and its usage on endpoints can be found [here](#).

Msi Source Location

This option is Windows only!

This setting specifies whether Windows Installer packages are installed from the Windows Installer cache of the endpoint or from a distribution location.

Possible values:	• Windows Installer cache • Distribution location
Default value:	Windows Installer cache
Example value:	Windows Installer cache



Detailed information about this setting and its usage on endpoints can be found [here](#).

Msi UI Level

This option is Windows only!

This setting specifies the user interaction level for the end-user for MSI.

Possible values:	/q, /qn, /qb, /qr, /qf, /qn+, /qb+, /qb+!, /qb-, /qb-!
Default value:	/qb
Example value:	/qb

Detailed information about this setting and its usage on endpoints can be found [here](#).

Msi Uninstall Args

This option is Windows only!

This setting specifies the arguments to include in the MSI command-line for uninstall operations.

Possible values:	See the documentation for Microsoft Windows Installer
Default value:	{empty}
Example value:	/l*v c:\temp\msi.log (A command-line argument to turn on logging)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Reboot

All settings which affect the reboot behavior of an endpoint are found in this subcategory.

- [Allow Reboot If Locked](#)



- [Allow Reboot If Server](#)
- [Allow Timeout If Locked](#)
- [Always Display Reboot](#)
- [Continue After Command Failure](#)
- [Display the Shutdown Button](#)
- [Force Reboot](#)
- [Force Reboot If Locked](#)
- [Force Reboot Window to Top](#)
- [Post Reboot Command](#)
- [Pre Reboot Command](#)
- [Prompt Cycle Wait Time](#)
- [Reboot Command-Line](#)
- [Reboot If Required](#)
- [Reboot Log File](#)
- [Reboot Path](#)
- [Reboot Prompt Cycles](#)
- [Security Patch Reboot If Required](#)
- [Unlimited Reboot Prompting](#)

Allow Reboot If Locked

This setting specifies whether the RMS UEM AppCenter reboots the managed device if the package being installed requires it even if the machine is locked.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Allow Reboot If Server



This setting specifies whether the RMS UEM AppCenter reboots the managed device if it is a server. This setting is only used by the adoption agent.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Allow Timeout If Locked

ALLOW TIMEOUT IF LOCKED ☒

Specify whether the RMS UEM AppCenter reboot events wait for the machine to become unlocked before proceeding with a reboot.

This setting specifies whether RMS UEM AppCenter reboot events wait for the machine to become unlocked before proceeding with a reboot.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Always Display Reboot

ALWAYS DISPLAY REBOOT ☐

Specify whether the RMS UEM AppCenter displays a warning to the user before performing any reboot required by a package installation.

This setting specifies whether the RMS UEM AppCenter displays a warning to the user before performing any reboot required by a package installation.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)



Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Continue After Command Failure

This setting specifies whether to proceed with the requested reboot if the prereboot command returns a non-zero exit code.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Display the Shutdown Button

This setting specifies whether the **Shutdown** button as well as the **Reboot** button will be displayed to users on the reboot dialog. If set to **No**, only the **Reboot** button will be available.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)



Force Reboot

FORCE REBOOT

☐

Specify whether the RMS UEM AppCenter forces reboot if the package being installed requires it. This setting suppresses any user interaction required to close other applications that may be running.

This setting specifies whether the RMS UEM AppCenter forces a reboot if the package being installed requires it. This setting suppresses any user interaction required to close other applications that may be running.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).



Force Reboot If Locked

FORCE REBOOT IF LOCKED ☒

Specify whether the RMS UEM AppCenter performs a forced reboot if the machine is locked.

This setting specifies whether the RMS UEM AppCenter performs a forced reboot if the machine is locked.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Force Reboot Window to Top

FORCE REBOOT WINDOW TO TOP ☐

Force the reboot dialog to be the top window during the final stage of user prompting.

This setting specifies whether the reboot dialog is forced to be the top window during the final stage of the user prompting.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Post Reboot Command

POST REBOOT COMMAND

Specify the command to be run after an RMS UEM AppCenter requested reboot occurs.

This setting specifies the command to be run after a reboot requested by the RMS UEM AppCenter occurs.



Possible values:	A valid command
Default value:	{empty}
Example value:	chkdsk /f

Detailed information about this setting and its usage on endpoints can be found [here](#).

Pre Reboot Command

PRE-REBOOT COMMAND

Specify the command to be run before an RMS UEM AppCenter requested reboot occurs.

This setting specifies the command to be run before a reboot requested by the RMS UEM AppCenter occurs.

Possible values:	A valid command
Default value:	{empty}
Example value:	cleanmgr

Detailed information about this setting and its usage on endpoints can be found [here](#).

Prompt Cycle Wait Time

PROMPT CYCLE WAIT TIME

Specify the length of reboot prompt cycles, in seconds.

This setting specifies the length of the reboot prompt cycles in seconds.

Possible values:	Integer (seconds)
Default value:	600
Example value:	600

Detailed information about this setting and its usage on endpoints can be found [here](#).



Reboot Command-Line

REBOOT COMMAND LINE

Specify the command used to perform reboot on the managed devices.

This setting specifies the command used to perform a reboot on the managed device.

Possible values:	Name of the executable in the command path
Default value:	\$ (RebootPath)
Example value:	\$ (RebootPath)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Reboot If Required

REBOOT IF REQUIRED ☐

Specify the default response to dialogs that prompt the user to allow a reboot.

This setting specifies the default response to dialogs that prompt the user to allow a reboot.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Reboot Log File

REBOOT LOG FILE

Specify the name of the file to store logging information.

This setting specifies the name of the file to store the logging information into.

Possible values:	A local or a UNC network file
Default value:	\$ (TempDirectory) \ManageSoft\RMSReboot.log



Example value:	C:\temp\RMSReboot.log

Reboot Path

REBOOT PATH

Specify the full path to the command line used to reboot managed devices.

This setting specifies the full path to the command used to reboot managed devices.

Possible values:	A valid local directory path and executable program name
Default value:	\$ (ProgamPath) \RMSReboot.exe
Example value:	\$ (ProgamPath) \RMSReboot.exe



Reboot Prompt Cycles

This setting specifies the number of times the user is prompted to reboot. The user is given the option to reboot or to postpone until these cycles are complete.

Possible values:	Integer
Default value:	0
Example value:	2

Detailed information about this setting and its usage on endpoints can be found [here](#).

Security Patch Reboot If Required

This setting specifies the default response to the dialogs displayed during security patch installation that prompt the user to allow a reboot.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Unlimited Reboot Prompting

This setting specifies whether there will be an infinite number of **Reboot Prompt Cycles**.



Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Self-heal

All settings which affect the self-healing behavior of an endpoint are found in this subcategory.

- [Self-heal](#)

Self-heal

SELF-HEAL



 Specify whether self-healing should occur. `True` means that all packages on this managed device should self-heal. `False` means that no packages on this managed device should self-heal. Any other value means that self-healing attempted only on packages with a custom property whose name matches the value of `SelfHeal`. Note: The custom property value is not used, but it must have a non empty value to take effect.

This setting specifies whether self-healing should occur. `True` means that all packages on this managed device should self-heal. `False` means that no packages on this managed device should self-heal. Any other value means that self-healing is only attempted on packages with a custom property whose name matches the value of `SelfHeal`.

**Note:**

The custom property value is not used, but it must have a non-empty value to take effect.

Possible values:	A string. Valid entries include: • <code>True</code> means that all packages on this managed device should self-heal. • <code>False</code> means that no packages on this managed device should self-heal. • Any other value means that self-healing should be attempted only on packages with a <code>SelfHeal</code> property whose value matches this string. For example, if a package has a <code>SelfHeal</code> value of <code>AlwaysHealMe</code>, and <code>SelfHeal</code> on a device is also set to <code>AlwaysHealMe</code>, self-healing of that package will occur on that device.
Default value:	<code>True</code>
Example value:	<code>AlwaysHealMe</code>



Detailed information about this setting and its usage on endpoints can be found [here](#).

Inventory Agent

The **Inventory Agent** section of the **Device Settings** is divided into the following subcategories:

- [General](#)
- [Logging](#)
- [Scanning Options](#)

General

All general settings for the inventory agent are found in this subcategory.

- [Create Inventory Event Logs](#)
- [Inventory File](#)
- [Machine Inventory Directory](#)
- [Minimum Inventory Interval](#)
- [Permit Temporary Execution of Console Mode Application](#)
- [Progress Depth](#)
- [SMBIOS Command-Line](#)

Create Inventory Event Logs

Specifies whether the RMS UEM AppCenter should create inventory event logs.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Inventory File



This setting specifies the name of a local copy of the inventory file.

Possible values:	*.ndi
Default value:	\$(UserName) on \$(MachineId).ndi
Example value:	myComputer.ndi

Detailed information about this setting and its usage on endpoints can be found [here](#).

Machine Inventory Directory

MACHINE INVENTORY DIRECTORY

\$(CommonAppDataFolder)\ManageSoft Corp\ManageSoft\Tracker\Inv

Specify the location for machine inventories.

This setting specifies the location for machine inventories.

Possible values:	A valid local directory path
Default value:	\$(CommonAppDataFolder)\ManageSoft Corp \ManageSoft\Tracker\Inventories
Example value:	\$(CommonAppDataFolder)\ManageSoft Corp \ManageSoft\Tracker\Inventories

Detailed information about this setting and its usage on endpoints can be found [here](#).

Minimum Inventory Interval

MINIMUM INVENTORY INTERVAL

0

Specify the minimum interval (in hours) between collections of inventory.

This setting specifies the minimum interval in hours between the collection of inventories.

Possible values:	Integer (hours)
Default value:	0
Example value:	12

Detailed information about this setting and its usage on endpoints can be found [here](#).



Permit Temporary Execution of Console Mode Application

PERMIT TEMPORARY EXECUTION OF
CONSOLE MODE APPLICATION ☐



 Specify whether to permit execution of console mode applications on locked down Windows 9X desktops for zero-touch hardware inventory collection.

This setting specifies whether to permit the execution of console mode applications on locked down Windows 9x desktops for zero-touch hardware inventory collection.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)



Progress Depth

PROGRESS DEPTH

Specify the number of directory levels to search at initialization to approximate the number of directories searched during tracking.

This setting specifies the number of directory levels to search at initialization in order to approximate the number of directories searched during tracking.

Possible values:	Integer
Default value:	10
Example value:	10

Detailed information about this setting and its usage on endpoints can be found [here](#).

SMBIOS Command-Line

SMBIOS COMMAND LINE

Specify the command line for non-WMI hardware inventory collection.

This setting specifies the command-line for non-WMI hardware inventory collection.

Possible values:	A valid command-line that will execute <code>smbios2.exe</code> that results in output being written to standard output (it should include the <code>/l</code> argument).
Default value:	<code>conspawn smbios2.exe /l /G</code>
Example value:	<code>conspawn smbios2.exe /l /a</code>

Detailed information about this setting and its usage on endpoints can be found [here](#).

Logging

All settings which affect the logging functions of the inventory agent are found in this subcategory.

- [Log File](#)
- [Log File Size](#)
- [Log Level](#)
- [Old Log File](#)



Log File

This setting specifies the path and filename where RayManageSoft Unified Endpoint Manager stores the logging information.

Possible values:	A local or a UNC network file
Default value:	<code>\$(TempDirectory)\ManageSoft\Tracker.log</code>
Example value:	<code>C:\temp\Tracker.log</code>

Log File Size

This setting specifies the maximum size of the log file (in bytes).

Possible values:	Integer (bytes)
Default value:	4000000
Example value:	3126000 (3 MB)

Log Level

This setting specifies the level of logging for the installation agent.

Possible values:	One or more logging levels
Default value:	A-z (logs everything)
Example value:	G0, 4

More information regarding logging and levels of logging can be found in the [Appendix II: Logging on Managed Devices](#).



Old Log File

OLD LOG FILE

Specify the name of the file to store additional logging information.

This setting specifies the the path and filename where RayManageSoft Unified Endpoint Manager stores additional logging information.

Possible values:	A local or UNC network file
Default value:	<code>\$ (TempDirectory) \ManageSoft \Tracker.old.log</code>
Example value:	<code>C:\temp\Tracker_old.log</code>

Scanning Options

All settings which affect the scanning options of the inventory agent are found in this subcategory.

- [RMS UEM AppCenter Packages](#)
- [Embed File Content Directory](#)
- [Embed File Content Extension](#)
- [Embed File Content Max Size](#)
- [Exclude Directories](#)
- [Exclude Embed File Content Directory](#)
- [Exclude Extension](#)
- [Exclude File](#)
- [Exclude File System Type](#)
- [Exclude MD5](#)
- [Exclude Permissions Mask](#)
- [Generate MD5](#)
- [Hardware](#)
- [Include Directory](#)
- [Include Executable Files](#)
- [Include Extension](#)
- [Include File](#)
- [Include File System Types](#)
- [Include MD5](#)
- [Include MSI Packages in Inventory](#)
- [Include Permission Mask](#)
- [Include Registry Key](#)
- [Inventory Scripts](#)



- [Inventory Scripts Directory](#)
- [MSI Product Codes to Inspect Fully](#)
- [Platform-specific Packages](#)
- [Recurse](#)
- [Run Inventory Scripts](#)
- [Version Info](#)
- [WMI](#)

RMS UEM AppCenter Packages

This setting specifies whether information about RMS UEM AppCenter packages is included in inventories.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Embed File Content Directory

This option is Windows only!

This setting specifies the folders that will be scanned for embedding file content into the inventory.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)



Detailed information about this setting and its usage on endpoints can be found [here](#).



Embed File Content Extension

EMBED FILE CONTENT EXTENSIONS

Specify the file extensions that will have content embedded into inventory.

This setting specifies the file extensions that will have content embedded into the inventory.

Possible values:	A file extension (without period)
Default value:	swidtag
Example value:	swidtag

Detailed information about this setting and its usage on endpoints can be found [here](#).

Embed File Content Max Size

EMBED FILE CONTENT MAX SIZE

Specify the maximum file size to consider when embedding file contents into inventory.

This setting specifies the maximum size in bytes to consider when embedding file contents in the inventory.

Possible values:	Integer (bytes)
Default value:	1000000
Example value:	1000000

Detailed information about this setting and its usage on endpoints can be found [here](#).

Exclude Directories

EXCLUDE DIRECTORIES

Specify the folders to exclude from inventory.

This setting specifies the folders that will be excluded from the inventory.

Possible values:	A valid folder
Default value:	{empty}



Example value:	\$ (WinDirectory)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Exclude Embed File Content Directory

This value specifies the directories to exclude from scanning for embedding file contents into the inventory.

Possible values:	A valid folder
Default value:	{empty}
Example value:	\$ (WinDirectory)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Exclude Extension

This setting specifies the file extensions to exclude from the inventory. This **may** include a leading period and can only be a period to specify files without extensions.

Possible values:	A valid file extension (no period required)
Default value:	{empty}
Example value:	DLL

Detailed information about this setting and its usage on endpoints can be found [here](#).



Exclude File

EXCLUDE FILE

Specify the files to exclude from inventory.

This settings specifies the files to be excluded from the inventory.

Possible values:	A valid file name
Default value:	{empty}
Example value:	myfile.txt

Detailed information about this setting and its usage on endpoints can be found [here](#).

Exclude File System Type

This option is non-windows only!

EXCLUDE FILE SYSTEM TYPES

Specify the types of files that should be excluded from the inventory.

This setting specifies the types of file system for which files will never be included in the inventory.

Possible values:	A valid file system type
Default value:	{empty}
Example value:	ufs

Detailed information about this setting and its usage on endpoints can be found [here](#).

Exclude MD5

EXCLUDE MD5

Specify the MD5 for files that are excluded from the inventory.

This setting specifies the MD5 for files that are excluded from the inventory.

Possible values:	A valid MD5 value



Default value:	{empty}
Example value:	7d9d2440656fdb3645f6734465678c60

Detailed information about this setting and its usage on endpoints can be found [here](#).



Exclude Permissions Mask

This option is non-windows only!

EXCLUDE PERMISSIONS MASK

① Specify which files should not be scanned during a Deployment Manager inventory. The value should be an octal mask for file permissions in the format used by the `chmod` command. Files which match this mask will be excluded from the scan. If an exclamation is added before the mask, the files which do not match this mask will be excluded from the scan.

This setting specifies which files should not be scanned during an inventory. The value should be an octal mask for file permissions in the format used by the `chmod` command. Files which match this mask will be excluded from the scan. If an exclamation mark is added before the mask, files not matching this mask will be excluded from the scan.

Possible values:	An octal value in the format used for <code>chmod</code>
Default value:	{empty}
Example value:	0777

Detailed information about this setting and its usage on endpoints can be found [here](#).

Generate MD5

GENERATE MD5

☐

① Specify whether to generate MD5 checksums for files that are reported in inventory.

This value specifies whether to generate MD5 checksums for files that are reported in the inventory.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).



Hardware

HARDWARE

☒

Specify whether to track hardware inventory when generating machine inventory.

This setting specifies whether to track hardware inventories when generating a machine inventory.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Include Directory

INCLUDE DIRECTORY

Specify the folders to include in inventory.

This setting specifies the folders to include in the inventory.

Possible values:	A valid folder
Default value:	{empty}
Example value:	C:\Program Files

Detailed information about this setting and its usage on endpoints can be found [here](#).

Include Executable Files

INCLUDE EXECUTABLE FILES

☒

Include files which are executable. An executable on Windows is defined as a file which end in '.exe'. On Unix, and executable is a file without an extension and with one or more of its executable bits being set.

This setting specifies if files that are executable will be included.

Possible values:	• Yes (checked)



	• No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Include Extension

INCLUDE EXTENSION

Specify the file extensions to include in inventory. This may include a leading dot and can be just a dot to specify files without extension.

This setting specifies the file extensions to include in the inventory. This **may** include a leading period and can only be a period to specify files without extensions.

Possible values:	A valid file extension (no period required)
Default value:	{empty}
Example value:	bat

Detailed information about this setting and its usage on endpoints can be found [here](#).

Include File

INCLUDE FILE

Specify the files to be included in inventory.

This setting specifies the files to be included in the inventory.

Possible values:	A valid file name
Default value:	{empty}
Example value:	myfile.txt

Detailed information about this setting and its usage on endpoints can be found [here](#).

Include File System Types

This option is non-windows only!



This setting specifies the types of file systems for which files will always be included in the inventory.

Possible values:	A valid file system type
Default value:	ufs,zfs,lofs
Example value:	ufs,zfs,lofs

Detailed information about this setting and its usage on endpoints can be found [here](#).

Include MD5

This setting specifies the MD5 for files to include in the inventory.

Possible values:	A valid MD5 value
Default value:	{empty}
Example value:	7d9d2440656fdb3645f6734465678c60

Detailed information about this setting and its usage on endpoints can be found [here](#).

Include MSI Packages in Inventory

This option is Windows only!

This setting specifies whether information about MSI packages is included in the inventory.

Possible values:	• Yes (checked) • No (checked)



Default value:	checked (Yes)
Example value:	checked (Yes)

Detailed information about this setting and its usage on endpoints can be found [here](#).



Include Permission Mask

INCLUDE PERMISSIONS MASK

i Specify which files should be scanned during a Deployment Manager inventory. The value should be an octal mask for file permissions in the format used by the `chmod` command. Files which match this mask will be included in the scan. If an exclamation mark is added before the mask, the files which do not match this mask will be included in the scan.

This setting specifies which files should be scanned during an inventory. The value should be an octal mask for file permissions in the format used by the `chmod` command. Files which match this mask will be included in the scan. If an exclamation mark is added before the mask, files not matching this mask will be included in the scan.

Possible values:	An octal value in the format used for <code>chmod</code>
Default value:	{empty}
Example value:	0777

Detailed information about this setting and its usage on endpoints can be found [here](#).

Include Registry Key

This option is Windows only!

INCLUDE REGISTRY KEY

i Specify the registry keys or values to be include in the inventory. Additionally, this setting cannot have customized values. Separate multiple values by comma.

This setting specifies the registry keys or values to be included in the inventory. Additionally, this setting cannot have customized values. Multiple values are separated by commata.

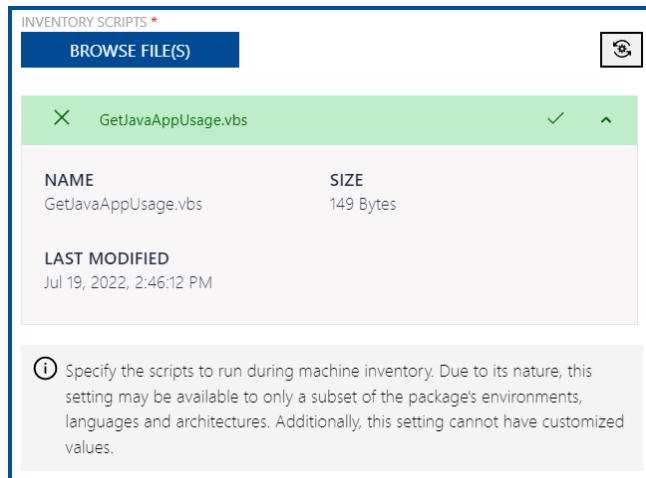
Possible values:	A valid key or registry value
Default value:	{empty}
Example value:	<pre>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\ - tracks all registry entries under this key HKEY_LOCALE_MACHINE\SOFTWARE*\ - tracks all registry keys and values under HKLM\SOFTWARE HKLM\SOFTWARE\Microsoft* - tracks all values under HKLM\SOFTWARE\Microsoft</pre>



	HKEY_LOCAL_MACHINE\SOFTWARE*\CurrentVersion*\n- illustrates the use of multiple wildcards

Detailed information about this setting and its usage on endpoints can be found [here](#).

Inventory Scripts



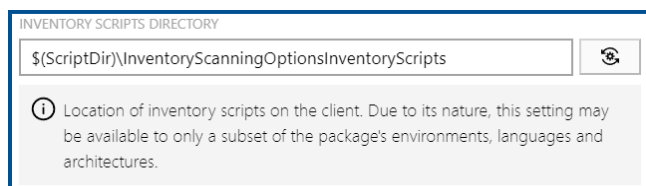
This setting specifies the scripts that are to run during a machine inventory. Due to its nature, this setting may only be available on a subset of endpoints in the environments, languages, and architectures of the package. Additionally, this setting cannot have customized values.

	Be aware: It is not possible to add more than one script file to this setting. Adding a file will replace the already existing file.

Possible values:	A valid script file
Default value:	{empty}
Example value:	GetJavaAppUsage.vbs

Detailed information about this setting and its usage on endpoints can be found [here](#).

Inventory Scripts Directory





This setting specifies the location of inventory scripts on the client. Due to its nature, this setting may only be available on a subset of endpoints in the environments, languages, and architectures of the package.

Possible values:	A valid location
Default value:	<code>\$(ScriptDir)\InventoryScanningOptionsInventoryScripts</code>
Example value:	<code>C:\LocalScripts\</code>

Detailed information about this setting and its usage on endpoints can be found [here](#).

MSI Product Codes to Inspect Fully

This option is Windows only!

MSI PRODUCT CODES TO INSPECT FULLY

Specify the product codes which are to be inspected fully, which involves calculating the result of all applied transforms and patches before retrieval of the UpgradeCode and PIDKEY properties. The value * includes all products. Additionally, this setting cannot have customized values. Separate values by comma.

This settings specifies the product codes which are to be inspected fully. This involves calculating the result of all applied transforms and patches before retrieval of the UpgradeCode and PIDKEY properties. The value * includes all products. Additionally, this setting cannot have customized values. Multiple values are separated by commata.

Possible values:	A valid product code represented as a string GUID
Default value:	{empty}
Example value:	{12345678-1234-1234-1234-123456789012}

Platform-specific Packages

PLATFORM-SPECIFIC PACKAGES ☒

Specify whether information about platform-specific packages (for example .lpp, .pkg, .rpm and .sd-ux) is included in inventories.

This setting specifies whether information about platform-specific packages (for example: .lpp, .pkg, .rpm, and .sd-ux) is included in the inventory.

Possible values:	• Yes (checked)



	• No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Detailed information about this setting and its usage on endpoints can be found [here](#).



Recurse

RECURSE ☒

 Specify whether child folders are included in inventory.

This setting specifies whether child folders are included in the inventory.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Run Inventory Scripts

RUN INVENTORY SCRIPTS ☐

 Specify whether to execute any custom inventory scripts found by plugins.
Due to its nature, this setting may be available to only a subset of the package's environments, languages and architectures.

This setting specifies whether to execute any custom inventory scripts found by plugins. Due to its nature, this setting may be available only to a subset of environments, languages, and architectures for the package.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	checked (Yes)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Version Info

VERSION INFO ☒

 Specify whether file version header information is included in inventory.

This setting defines whether file header information is included in the inventory.

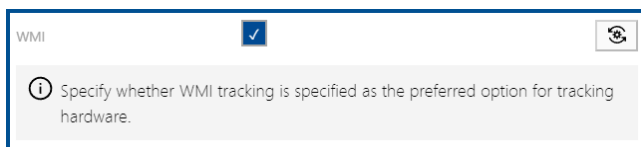


Possible values:	• Yes (checked) • No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Detailed information about this setting and its usage on endpoints can be found [here](#).

WMI

This option is Windows only!



This setting specifies whether WMI tracking is specified as the preferred option for tracking hardware.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Policy Agent

The **Policy Agent** section of the **Device Settings** is divided into the following subcategories:

- [General](#)
- [Logging](#)
- [Merging](#)
- [Locations](#)

General

All general settings for the policy agent are found in this subcategory.

- [Policy Server Priority](#)



Policy Server Priority

POLICY SERVER PRIORITY

i Specify the numerical priority (or "invalid") to be assigned to the location from which policy (.NPL) files were obtained, when using it as a location for downloading packages.

This setting specifies the numerical priority (or `invalid`) to be assigned to the location from which policy (`.nlp`) files were obtained when using it as a location for downloading packages.

Possible values:	Integer between 0 - 100, or <code>Invalid</code>
Default value:	50
Example value:	50

Detailed information about this setting and its usage on endpoints can be found [here](#).

Logging

All settings which affect the logging functions of the policy agent are found in this subcategory.

- [Log File](#)
- [Old Log File](#)
- [Log Level](#)
- [Log File Size](#)

Log File

LOG FILE

i Specify the name of the file to store logging information.

This setting specifies the the path and filename where RayManageSoft Unified Endpoint Manager stores the logging information.

Possible values:	A local or a UNC network file
Default value:	<code>\$ (TempDirectory) \ManageSoft \policy.log</code>
Example value:	<code>C:\temp\policy.log</code>



Old Log File

OLD LOG FILE

Specify the name of the file to store additional logging information.

This setting specifies the path and filename where RayManageSoft Unified Endpoint Manager stores additional logging information.

Possible values:	A local or UNC network file
Default value:	\$ (TempDirectory) \ManageSoft \policy.old.log
Example value:	C:\temp\policy_old.log

Log Level

LOG LEVEL

Specify the logging level for the policy agent.

This setting specifies the level of logging for the policy agent.

Possible values:	One or more logging levels
Default value:	A-z (logs everything)
Example value:	G0, 4

More information regarding logging and levels of logging can be found in the [Appendix II: Logging on Managed Devices](#).

Log File Size

LOG FILE SIZE

Specify the maximum log file size.

This setting specifies the maximum size of the log file (in bytes).

Possible values:	Integer (bytes)
Default value:	4000000
Example value:	3126000 (3 MB)



Merging

All settings which affect the merging in regard of the policy agent are found in this subcategory.

- [Apply Local Policy](#)
- [Auto Detect DC](#)
- [Disable Package Filtering](#)
- [Enable Policy Failover](#)
- [GP Client Side Extension Enabled](#)
- [Launcher Command-Line](#)
- [Machine Policy Command](#)
- [Minimum DC Speed](#)
- [Report Compliance](#)
- [Retry Policy](#)
- [Retry Policy Command](#)

Apply Local Policy

This setting specifies whether to use the locally cached copy of a policy if a new policy cannot be generated.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Disable Package Filtering

This setting specifies whether bypassing package-level filtering is allowed during a policy merge if filtering is not required.



Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Enable Policy Failover

ENABLE POLICY FAIL OVER

☐

Specify if fail over to server side policy merging should happen or not.

This setting specifies whether the failover to server side policy merging should happen.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).

GP Client Side Extension Enabled

GP CLIENT SIDE EXTENSION
ENABLED

☐

Specifies whether the Group Policy Client Side Extension should be executed.

This setting specifies whether the Group Policy Client Side Extension should be executed.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)



Launcher Command Line

LAUNCHER COMMAND LINE

Specify the installation agent command line options to pass to RMS UEM AppCenter when applying policy information.

This setting specifies the installation agent command-line options to pass to the RMS UEM AppCenter when applying policy information.

Possible values:	Valid command-line options
Default value:	{empty}
Example value:	/Lx C:\temp\policy.log

Detailed information about this setting and its usage on endpoints can be found [here](#).

Machine Policy Command

"\$(ProgramFiles)\ManageSoft\Policy Client\mgspolicy.exe" -t Machine

The command to execute to perform an application of machine policy on the managed device.

This setting specifies the command to execute to perform an application of the machine policy on the managed device.

Possible values:	A valid command-line for the mgspolicy.exe
Default value:	"\$(ProgramFiles)\ManageSoft\Policy Client\mgspolicy.exe" -t Machine
Example value:	"\$(ProgramFiles)\ManageSoft\Policy Client\mgspolicy.exe" -t Machine

Detailed information about this setting and its usage on endpoints can be found [here](#).

Minimum DC Speed

MINIMUM DC SPEED

0

Specify the minimum network speed (in bits per second) between the managed device and the domain controller that is required to apply policy. This setting only applies for client-side policy merging when Auto Detect DC is set to False.



This setting specifies the minimum network speed in bits per second between the managed device and the domain controller that is required to apply the policy. This setting only applies for client-side policy merging when `AutoDetectDC` is set to `False`.

Possible values:	Integer (bits per second)
Default value:	0
Example value:	3500

Detailed information about this setting and its usage on endpoints can be found [here](#).

Report Compliance

REPORT COMPLIANCE ☐


 Specify whether managed devices will report policy compliance. Note: This setting should not be changed from the default value of `false` as policy compliance logs are not currently imported by RMS UEM AppCenter.

This setting specifies whether managed devices will report policy compliance.

 **Note:**
This setting should not be changed from the default value of `False` as policy compliance logs are currently not imported by the RMS UEM AppCenter.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	unchecked (No)
Example value:	unchecked (No)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Retry Policy

RETRY POLICY ☒


 Specify whether the RMS UEM AppCenter will attempt to retrieve policy when the managed device boots, if no machine schedule exists on managed device.

This setting specifies whether the RMS UEM AppCenter will attempt to retrieve a policy when the managed device boots if no machine schedule exists on the managed device.

Possible values:	• Yes (checked)



	• No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Detailed information about this setting and its usage on endpoints can be found [here](#).

Retry Policy Command

RETRY POLICY COMMAND

mgspolicy.exe -t Machine -o UserInteractionLevel=Quiet



 Specify the command used to retrieve policy if Retry Policy is set to true.

This setting specifies the command used to retrieve the policy if `RetryPolicy` is set to `True`.

Possible values:	A valid policy agent command-line
Default value:	<code>mgspolicy.exe -t Machine</code> <code>-o UserInteractionLevel=Quiet</code>
Example value:	<code>mgspolicy.exe -t Machine</code>

Detailed information about this setting and its usage on endpoints can be found [here](#).

Locations

All settings regarding locations relevant for the policy agent are found in this subcategory.

- [Machine Policy Package Directory](#)
- [Machine Policy Directory](#)

Machine Policy Package Directory

MACHINE POLICY PACKAGE DIRECTORY

\$(CommonAppDataFolder)\ManageSoft Corp\ManageSoft\Policy Client



 Specify the location where package information associated with machine policy is cached.

This setting specifies the location where package information associated with a machine policy is cached.

Possible values:	A valid folder and path
Default value:	<code>\$(CommonAppDataFolder)\ManageSoft Corp\</code> <code>ManageSoft\Policy Client\Packages</code>



Example value:	C:\Temp\MachinePolicies\PackageInfo

Detailed information about this setting and its usage on endpoints can be found [here](#).

Machine Policy Directory

This setting specifies the location in which to save the current machine policy.

Possible values:	A valid folder and path
Default value:	\$(CommonAppDataFolder)\ManageSoft Corp\ ManageSoft\Policy Client\Policies\Merged\Machine
Example value:	C:\Temp\MachinePolicies

Detailed information about this setting and its usage on endpoints can be found [here](#).

AppCenter

The **AppCenter** section of the **Device Settings** is divided into the following subcategories:

- [General](#)
- [Logging](#)

General

All general settings for the RMS UEM AppCenter are found in this subcategory.

- [Refresh Period](#)
- [Locale](#)
- [Default Locale](#)
- [Default Configuration File](#)
- [Configuration File](#)
- [Application Verify Command](#)
- [Application Uninstall Command](#)
- [Application Install Command](#)



Refresh Period

REFRESH PERIOD

Specify the number of minutes between automatic refresh of data displayed by the RMS UEM AppCenter user interface on a managed device.

This setting specifies the number of minutes between the automatic refresh of data displayed by the RMS UEM AppCenter user interface on a managed device.

Possible values:	Integer (minutes)
Default value:	5
Example value:	5

Detailed information about this setting and its usage on endpoints can be found [here](#).



Locale

LOCALE

Specify the locale setting used by the AppCenter.

This setting specifies the locale setting used by the AppCenter.

Possible values:	A two-character abbreviation that is valid for <code>locale</code> . For the currently valid values, check ISO 3166-1-alpha-2 code .
Default value:	<code>\$(UserLocale)</code>
Example value:	DE

Detailed information about this setting and its usage on endpoints can be found [here](#).

Default Locale

DEFAULT LOCALE

Specify the default locale setting used by the AppCenter.

This setting specifies the default locale setting used by the AppCenter.

Possible values:	A two-character abbreviation that is valid for <code>locale</code> . For the currently valid values, check ISO 3166-1-alpha-2 code .
Default value:	EN
Example value:	DE

Detailed information about this setting and its usage on endpoints can be found [here](#).

Default Configuration File

DEFAULT CONFIGURATION FILE

Specify the name of the default configuration file used by the RMS UEM AppCenter user interface on managed devices.

This setting specifies the name of the default configuration file used by the RMS UEM AppCenter user interface on managed devices.



Possible values:	A path and filename of a valid configuration file
Default value:	<code>\$(SkinsDirectory)\Default\\$(Locale)\\$(ConfigName)</code>
Example value:	<code>C:\Program Files\ManageSoft\Selector\ Skins\MySkin\DE\config.xml</code>

Detailed information about this setting and its usage on endpoints can be found [here](#).

Configuration File

This setting specifies the name of the configuration file used by the RMS UEM AppCenter user interface on managed devices.

Possible values:	A path to a valid configuration file
Default value:	<code>\$(ConfigFileDefault)</code>
Example value:	<code>C:\Program Files\ManageSoft\Selector\ Skins\MySkin\DE\config.xml</code>

Detailed information about this setting and its usage on endpoints can be found [here](#).

Application Verify Command

This setting specifies the command-line to be used to verify or repair an application package through the RMS UEM AppCenter package selection agent.

The value of this setting should always include the following special substrings:

- `{1}` - This substring will be replaced with the URL of the package to be verified. This value is typically passed as the value of the `-a` command-line option of the installation agent. The URL may contain space characters and therefore should be appropriately set into quotation marks in the command-line.
- `{2}` - This substring will be replaced with any installation agent command-line options that the selection agent determines may be needed to verify the package. This value should not be set into quotation marks in the command-line.



Possible values:	A valid command-line string containing the literal substrings {1} and {2}.
Default value:	<code>ndlaunch -a "{1}" -o SaveAllUserSymbols=False -o MsiRepair=True -o CachedVersion=True -o SelfHeal=True -o CheckRegistry=True -o NoExec=True {2}</code>
Example value:	To require applications to be verified against their source from an appropriate distribution location and to not self-heal registry settings: <code>ndlaunch -a "{1}" -o SaveAllUserSymbols=False -o MsiRepair=True -CheckRegistry=False -o NoExec=True {2}</code>

Detailed information about this setting and its usage on endpoints can be found [here](#).

Application Uninstall Command

APPLICATION UNINSTALL COMMAND

Specify the template command line to be used to uninstall an application package through the RMS UEM AppCenter package selection agent.

This setting specifies the template command-line to be used to uninstall an application package through the RMS UEM AppCenter package selection agent.

- {1} - This substring will be replaced with the URL of the package to be verified. This value is typically passed as the value of the `-a` command-line option of the installation agent. The URL may contain space characters and therefore should be appropriately set into quotation marks in the command-line.
- {2} - This substring will be replaced with any installation agent command-line options that the selection agent determines may be needed to verify the package. This value should not be set into quotation marks in the command-line.

Possible values:	A valid command-line string containing the literal substrings {1} and {2}.
Default value:	<code>ndlaunch -d "{1}" -o SaveAllUserSymbols=False {2}</code>
Example value:	To uninstall packages with full user interaction: <code>ndlaunch -d "{1}" -o SaveAllUserSymbols=False {2} -o UserInteractionLevel=Full</code>

Detailed information about this setting and its usage on endpoints can be found [here](#).



Application Install Command

APPLICATION INSTALL COMMAND

`ndlaunch -r "{1}" -o SaveAllUserSymbols=False {2}`

Specify the template command line to be used to install an application package through the RMS UEM AppCenter package selection agent.

This setting specifies the template command-line to be used to uninstall an application package through the RMS UEM AppCenter package selection agent.

- { 1 } - This substring will be replaced with the URL of the package to be verified. This value is typically passed as the value of the `-a` command-line option of the installation agent. The URL may contain space characters and therefore should be appropriately set into quotation marks in the command-line.
- { 2 } - This substring will be replaced with any installation agent command-line options that the selection agent determines may be needed to verify the package. This value should not be set into quotation marks in the command-line.



Possible values:	A valid command-line string containing the literal substrings {1} and {2}.
Default value:	<code>ndlaunch -r "{1}" -o SaveAllUserSymbols=False {2}</code>
Example value:	To install packages with full user interaction: <code>ndlaunch -r "{1}" -o SaveAllUserSymbols=False {2}</code> <code>-o UserInteractionLevel=Full</code>

Detailed information about this setting and its usage on endpoints can be found [here](#).

Logging

All settings which affect the logging functions of the RMS UEM AppCenter are found in this subcategory.

- [Log File](#)
- [Old Log File](#)
- [Log Level](#)
- [Log File Size](#)

Log File

LOG FILE

Specify the name of the file to store logging information.

This setting specifies the path and filename where RayManageSoft Unified Endpoint Manager stores the logging information.

Possible values:	A local or a UNC network file
Default value:	<code>\$ (TempDirectory) \ManageSoft \selector.log</code>
Example value:	<code>C:\temp\selector.log</code>

Old Log File

OLD LOG FILE

Specify the name of the file to store additional logging information.

This setting specifies the path and filename where RayManageSoft Unified Endpoint Manager stores additional logging information.



Possible values:	A local or UNC network file
Default value:	\$(TempDirectory)\ManageSoft\selector.old.log
Example value:	C:\temp\selector_old.log

Log Level

This setting specifies the level of logging for the installation agent.

Possible values:	One or more logging levels
Default value:	A-z (logs everything)
Example value:	G0, 4

More information regarding logging and levels of logging can be found in the [Appendix II: Logging on Managed Devices](#).

Log File Size

This setting specifies the maximum size of the log file (in bytes).

Possible values:	Integer (bytes)
Default value:	4000000
Example value:	3126000 (3 MB)

Upload Agent

The **Upload Agent** section of the **Device Settings** is divided into the following subcategories:

- [General](#)
- [Bandwidth Settings](#)
- [Logging](#)



General

All general settings for the upload agent are found in this subcategory.

- [Upload Inventory Files](#)
- [Policy Compliance Log](#)
- [Log](#)
- [Inventory](#)

Upload Inventory Files

This setting specifies whether the RMS UEM AppCenter should upload inventory files immediately after their generation.

Possible values:	• Yes (checked) • No (unchecked)
Default value:	checked (Yes)
Example value:	checked (Yes)

Policy Compliance Log

This setting specifies the location where the RMS UEM AppCenter uploads the policy compliance log file from the managed device.

Possible values:	A valid location
Default value:	<code>\$(ServerLocation)\PolicyComplianceLogs\\$(UserId) on \$(MachineId) at \$(DateTime).plc</code>
Example value:	<code>\$(ServerLocation)\PolicyComplianceLogs\\$(UserId) on \$(MachineId) at \$(DateTime).plc</code>

Detailed information about this setting and its usage on endpoints can be found [here](#).



Log

UPLOAD INVENTORY FILES

☒

Specify whether the RMS UEM AppCenter should upload inventory files immediately after generation.

This setting specifies the location where the RMS UEM AppCenter uploads the logging files from the managed device.

Possible values:	A valid location
Default value:	<code>\$(ServerLocation)\Logs\\$(MachineId) at \$(DateTime)_\$(GUID).log</code>
Example value:	<code>\$(ServerLocation)\Logs\\$(MachineId) at \$(DateTime).log</code>

Detailed information about this setting and its usage on endpoints can be found [here](#).

Inventory

INVENTORY

Specify the location where the RMS UEM AppCenter uploads inventory files.

This setting specifies the location where the RMS UEM AppCenter uploads inventory files.

Possible values:	A valid location
Default value:	<code>\$(ServerLocation)\Inventories\\$(UserId) on \$(MachineId) at \$(DateTime) (\$(Generation)).ndi</code>
Example value:	<code>\$(ServerLocation)\Inventories\\$(MachineId).ndi</code>

Detailed information about this setting and its usage on endpoints can be found [here](#).

Bandwidth Settings

All bandwidth settings for the upload agent are found in this subcategory.

- [Network Timeout](#)
- [Network Min Speed](#)
- [Network Max Rate](#)
- [Network Low Usage Lower Limit](#)
- [Network Low Usage](#)
- [Network High Usage Upper Limit](#)



- [Network High Usage](#)
- [Network High Speed](#)

Network Timeout

This setting specifies the length of time in seconds of inactivity after which a network operation will time out.

Possible values:	Integer (seconds)
Default value:	600
Example value:	600

Detailed information about this setting and its usage on endpoints can be found [here](#).

Network Min Speed

This setting specifies the minimum network speed in bits per second for the RMS UEM AppCenter to initiate a check for updates. If below this network speed, no check for updates will be initiated. If set to 0, the RMS UEM AppCenter will always initiate a check for updates.

Possible values:	Integer (bits per seconds)
Default value:	0
Example value:	250

Detailed information about this setting and its usage on endpoints can be found [here](#).



Network Max Rate

NETWORK MAX RATE

Specify the bytes per second at which the managed device uploads data over the network. This setting is not used if the NetworkSpeed setting can be determined and the NetworkHighSpeed is set to a non-zero value.

This setting specifies the speed in bytes per second at which the managed device uploads data over the network. This setting is not used if the `NetworkSpeed` setting can be determined and the `NetworkHighSpeed` setting is set to a non-zero value. If the setting is set to 0, it means it is not limited.

Possible values:	Integer (bytes per second)
Default value:	0
Example value:	600

Detailed information about this setting and its usage on endpoints can be found [here](#).



Network Low Usage Lower Limit

This setting specifies the minimum `NetworkLowUsage` value that can be set for a managed device by an end-user moving the bandwidth usage slider control in the installation agent.

Possible values:	Integer between 0 - 100
Default value:	100
Example value:	100

Detailed information about this setting and its usage on endpoints can be found [here](#).

Network Low Usage

This setting specifies the maximum percentage of bandwidth that the RMS UEM AppCenter uses for uploads on a low-speed connection.

Possible values:	Integer between 0 - 100
Default value:	100
Example value:	100

Detailed information about this setting and its usage on endpoints can be found [here](#).

Network High Usage Upper Limit

This setting specifies the maximum `NetworkHighUsage` value that can be set for a managed device by an end-user moving the bandwidth usage slider control in the installation agent.



Possible values:	Integer between 0 - 100
Default value:	100
Example value:	100

Detailed information about this setting and its usage on endpoints can be found [here](#).

Network High Usage

This setting specifies the maximum percentage of bandwidth that the RMS UEM AppCenter uses for uploads on a high-speed connection.

Possible values:	Integer between 0 - 100
Default value:	100
Example value:	100

Detailed information about this setting and its usage on endpoints can be found [here](#).

Network High Speed

This setting specifies the lowest network speed in bits per second that the RMS UEM AppCenter will consider to be a high speed network connection to a server. If this setting is set to 0, bandwidth usage will not be limited according to the network speed.

Possible values:	Integer (bits per second)
Default value:	0
Example value:	32

Detailed information about this setting and its usage on endpoints can be found [here](#).



Logging

All settings which affect the logging functions of the upload agent are found in this subcategory.

- [Log File](#)
- [Old Log File](#)
- [Log Level](#)
- [Log File Size](#)



Log File

LOG FILE

Specify the name of the file to store logging information.

This setting specifies the path and filename where RayManageSoft Unified Endpoint Manager stores the logging information.

Possible values:	A local or a UNC network file
Default value:	\$ (TempDirectory) \ManageSoft \Uploader.log
Example value:	C:\temp\Uploader.log

Old Log File

OLD LOG FILE

Specify the name of the file to store additional logging information.

This setting specifies the path and filename where RayManageSoft Unified Endpoint Manager stores additional logging information.

Possible values:	A local or UNC network file
Default value:	\$ (TempDirectory) \ManageSoft \uploader.old.log
Example value:	C:\temp\uploader_old.log

Log Level

LOG LEVEL

Specify the logging level for the upload agent.

This setting specifies the level of logging for the installation agent.

Possible values:	One or more logging levels
Default value:	A-z (logs everything)
Example value:	G0, 4

More information regarding logging and levels of logging can be found in the [Appendix II:](#)



[Logging on Managed Devices.](#)



Log File Size

This setting specifies the maximum size of the log file (in bytes).

Possible values:	Integer (bytes)
Default value:	4000000
Example value:	3126000 (3 MB)

Contact

The **Contact** section of the **Device Settings** is divided into the following subcategories:

- [General](#)

General

All general settings for the overall functionality of RayManageSoft Unified Endpoint Manager are found in this subcategory.

- [Support URL](#)
- [Support Telephone](#)
- [Contact Person](#)

Support URL

This setting specifies the support URL displayed to end-users within the AppCenter.

Possible values:	String
Default value:	{empty}
Example value:	https://mycompany.com/support



Support Telephone

SUPPORT TELEPHONE

Specify the support telephone number displayed to your end users within the AppCenter.

This setting specifies the telephone number that will be displayed to end-users within the RMS UEM AppCenter.

Possible values:	String
Default value:	{empty}
Example value:	+12 345 678 1234

Contact Person

CONTACT PERSON

Specify the contact person displayed to your end users within the AppCenter.

This setting specifies the contact person that will be displayed to end-users within the AppCenter.

Possible values:	String
Default value:	{empty}
Example value:	Jane Admin

Edit the Properties of the Device Settings

Clicking on the **Properties** button in the **Device Details** will open the **Properties** dialog.

Be aware:
In this dialog, it is only possible to edit the general information of a set of device settings. To edit a specific device setting, it is necessary to select the specific setting while in the set of device settings in which its value should be changed.



Properties

IMAGE

NAME *

Example Device Settings

VERSION *

1 0 0 1

The version number is used by the Deployment Manager on the managed devices to coordinate application updates. Increase this number whenever you want to distribute a revised version of your application.

COMMENT

Enter a comment here!

Save changes Discard

The following options are available in the dialog.

- **IMAGE:** Clicking on the image will open a file browser. Browse for an image to customize the image for the set of device settings (the following file formats are supported: .gif, .jpg, .jpeg, and .png).
- **NAME:** The name for the set of device settings.
- **VERSION:** The version number of the settings which is further divided into:
 - Major
 - Minor
 - Build
 - RevisionSince the fields have already been separated, no further separators are allowed.
- **COMMENT:** A comment or a short description of the device settings can be added into the **COMMENT** field. Entering a comment is optional.

After clicking on the **Save changes** button the new set of device settings will be created using the default setting for each of the specific settings. The specific settings can now be edited in order to customize the new set of settings.



Device Schedules

The **Device Schedules** section contains an overview of the sets of device settings currently available in the tenant.

Status	Name	Version	Comment
OK	Default Device Schedule	1.0.0.0	This default device schedule will be applied to every device in this tenant.

The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the screen can be used to refresh the view.
- **Add** - The **Add** button on the top left of the screen can be used to add a new device schedule to the list. For more information see [Add a Device Schedule](#).
- **Delete** - The **Delete** button on the top left of the screen can be used to delete one or more device schedules if one or more device schedules in the list have been selected.
- **Search field** - The **Search** field can be found on the top right of the screen. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.

When clicking on the name of device schedule, the specific schedule will be opened.

Device Schedule Details

When opening the details for a device schedule, these consist of two parts. The left part contains some general information.

Event	Summary
Update Follower Locations	At startup / login, When connected to network, Daily
Generate Inventory	As soon as possible, At startup / login
Upload Client Files	Daily, When connected to network
Update Machine Policy	At startup / login, Daily

The right part of the details contains a list of the events that are configured for the device schedule. The following actions are available in this section.

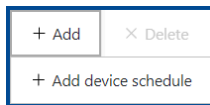
- **Refresh** - The **Refresh** button on the top left of the screen can be used to refresh the view.
- **Add** - The **Add** button on the top left of the screen can be used to add a new event to the list. For more information see [Add an Event](#).
- **Edit** - The **Edit** button on the top left of the screen can be used to edit an event if one of the events in the list have been selected. For more information see [Edit an Event](#).



- **Delete** - The **Delete** button on the top left of the screen can be used to delete one or more events if one or more device events in the list have been selected.

Add a Device Schedule

Click on the **Add** button in the **Device Schedules** section and select the **Add device schedule** option to open the **Add device schedule** dialog.



The **Add device schedule** dialog is used to add a new Device Schedule to the list of schedules available in RayManageSoft Unified Endpoint Manager.

Add device schedule [X]

IMAGE

NAME *

Example Device Schedule

VERSION *

1 0 0 0

i The version number is used by the Deployment Manager on the managed devices to coordinate application updates. Increase this number whenever you want to distribute a revised version of your application.

COMMENT

This is an example device schedule.

Add Discard

The following options are available in the dialog.

- **IMAGE**: Clicking on the image will open a file browser. Browse for an image to customize the image for the **Device Schedule** (the following file formats are supported: .gif, .jpg, .jpeg,



and .png).

- **NAME:** The name of the **Device Schedule**.
- **VERSION:** The version number of the **Device Schedule** which is further divided into:
 - Major
 - Minor
 - Build
 - RevisionSince the fields have already been separated, no further separators are allowed.
- **COMMENT:** A comment containing further information about the **Device Schedule**.

After adding a new **Device Schedule** events can now be added to the new schedule. See [Add an Event](#) for information regarding how to add a new **Event** to a **Device Schedule**.

Add an Event

Clicking on the **Add** button in the **Events** section of the **Device Schedule** details will open a dialog that can be used to add a new **Event**. The dialog is divided into the following tabs.

- [General](#)
- [Advanced](#)
- [Trigger](#)

General

In the **General** tab the type of the event and, according to the selected type, some further settings regarding the event can be determined. The following event types are available in this tab.

- [Apply a RMS UEM AppCenter policy](#)
- [Generate a RMS UEM AppCenter inventory](#)
- [Install or update RMS UEM AppCenter failover locations](#)
- [Upload RMS UEM AppCenter managed device files](#)
- [Run a Windows program, script or batch file](#)

Apply a RMS UEM AppCenter Policy

EVENT TYPE

Apply an RMS UEM AppCenter policy

INSTALL/UPDATE THE POLICY WITH THE FOLLOWING LEVEL OF USER INTERACTION LEVEL

RMS UEM AppCenter managed device's current user interaction level

DISPLAY THE CHOSEN USER INTERFACE
ONLY IF A PACKAGE CHANGES ☐

When **Apply a RMS UEM AppCenter policy** is selected as **EVENT TYPE**, the following options



for configuration are available:

- **INSTALL/UPDATE THE POLICY WITH THE FOLLOWING LEVEL OF USER INTERACTION LEVEL:**

Select one of the following (this setting will override the current setting of the device for this specific event):

- **RMS UEM AppCenter managed device's current user interaction level:** The level currently set on the device will be used.
 - **Full user interaction:** There is no limit to the user interaction regarding this event, even if the setting of the device normally limits the user interaction.
 - **No user interaction or user interface:** For this event, no user interaction is possible and no user interface will be shown, no matter the general setting of the device.
 - **Interaction only when error occur:** User interaction for this event will only be possible if an error occurs, otherwise no user interaction will be possible.
 - **A progress window, but no user interaction:** The end-user will be shown a progress window, but he will not be able to otherwise interact.
- **DISPLAY THE CHOSEN USER INTERFACE ONLY IF A PACKAGE CHANGES:** This checkbox can be used to limit the times when the user interface will be shown. If set to **Yes**, the user interface will only be shown if a package is changed and it will not be shown if no package is changed during the event.

Generate a RMS UEM AppCenter Inventory

EVENT TYPE

Generate an RMS UEM AppCenter inventory

INSTALL/UPDATE THE POLICY WITH THE FOLLOWING LEVEL OF USER INTERACTION LEVEL

RMS UEM AppCenter managed device's current user interaction level

When **Generate a RMS UEM AppCenter inventory** is selected as **EVENT TYPE**, the following options for configuration are available:

- **INSTALL/UPDATE THE POLICY WITH THE FOLLOWING LEVEL OF USER INTERACTION LEVEL:**

Select one of the following (this setting will override the current setting of the device for this specific event):

- **RMS UEM AppCenter managed device's current user interaction level:** The level currently set on the device will be used.
- **Full user interaction:** There is no limit to the user interaction regarding this event, even if the setting of the device normally limits the user interaction.
- **No user interaction or user interface:** For this event, no user interaction is possible and no user interface will be shown, no matter the general setting of the device.
- **Interaction only when error occur:** User interaction for this event will only be possible if an error occurs, otherwise no user interaction will be possible.
- **A progress window, but no user interaction:** The end-user will be shown a progress window, but he will not be able to otherwise interact.



Install or Update RMS UEM AppCenter Failover Locations

EVENT TYPE

Install or update RMS UEM AppCenter failover locations

INSTALL/UPDATE THE POLICY WITH THE FOLLOWING LEVEL OF USER INTERACTION LEVEL

RMS UEM AppCenter managed device's current user interaction level

DISPLAY THE CHOSEN USER INTERFACE
ONLY IF A PACKAGE CHANGES

☐

When **Install or update RMS UEM AppCenter failover location** is selected as **EVENT TYPE**, the following options for configuration are available:

- **INSTALL/UPDATE THE POLICY WITH THE FOLLOWING LEVEL OF USER INTERACTION LEVEL:**

Select one of the following (this setting will override the current setting of the device for this specific event):

- **RMS UEM AppCenter managed device's current user interaction level:** The level currently set on the device will be used.
- **Full user interaction:** There is no limit to the user interaction regarding this event, even if the setting of the device normally limits the user interaction.
- **No user interaction or user interface:** For this event, no user interaction is possible and no user interface will be shown, no matter the general setting of the device.
- **Interaction only when error occur:** User interaction for this event will only be possible if an error occurs, otherwise no user interaction will be possible.
- **A progress window, but no user interaction:** The end-user will be shown a progress window, but he will not be able to otherwise interact.

- **DISPLAY THE CHOSEN USER INTERFACE ONLY IF A PACKAGE CHANGES:** This checkbox can be used to limit the times when the user interface will be shown. If set to **Yes**, the user interface will only be shown if a package is changed and it will not be shown if no package is changed during the event.

Upload RMS UEM AppCenter Managed Devices Files

EVENT TYPE

Upload RMS UEM AppCenter managed device files

UPLOAD THE FOLLOWING FILES FROM THE MANAGED DEVICE

Upload all file types

When **Upload RMS UEM AppCenter managed files** is selected as **EVENT TYPE**, the following further options for configuration are available:

- **UPLOAD THE FOLLOWING FILES FROM THE MANAGED DEVICE:**

Select one of the following:

- **Upload all file types:** Select this option in order to upload all collected files.
- **Inventories:** Select this option in order to upload the inventory files.



- **Installation event logs:** Select this option in order to upload the installation event logs.

Run a Windows Program, Script, or Batch File

EVENT TYPE
Run a Windows program, script or batch file

TARGET

START IN

PARAMETERS

When **Run a Windows program, script or batch file** is selected as **EVENT TYPE**, the following options for configuration are available:

- **TARGET:** The path where the file can be found on the managed device needs to be entered here. For example: `cmd`.
- **START IN:** The path where the file will be executed on the managed device can be entered here. In most use cases this field can be left empty. An example for a path would be `$(TempDirectory)`.
- **PARAMETERS:** This field can be used to define additional parameters for the application that is about to run. For example: `/c "echo $(TempDirectory) >> C:\tmp\test.txt"`.

Advanced

In the **Advanced** tab of the dialog, some information regarding the behavior of the event can be configured.

DELAY NEXT RUN

☒ Delay next run by 1 Hour(s)

Delay the next execution of the event after a successful run.

RERUN BEHAVIOR

Ignore missed events

If the event has not been run for some reason, the managed device's task scheduler should use the selected behavior.

ONLY RUN THIS EVENT IF A NETWORK CONNECTION IS AVAILABLE ☐

ADDITIONAL PARAMETERS

In this tab, the following options are available:

- **DELAY NEXT RUN:** This option can be activated in order to delay the next run. It is possible to define the delay either by the number of minutes, hours, or days by selecting the unit of measurement in the dropdown box and entering the number in the field located on the left of the dropdown box.



- **RERUN BEHAVIOR:** This option defines how the event will behave if one or more occurrences of the event have been missed. The following behaviors are available:
 - Ignore missed events
 - Run all missed events
 - Run only the last event missed
- **ONLY RUN THIS EVENT IF A NETWORK CONNECTION IS AVAILABLE:** If set to **Yes**, the event only runs if a network is available. If set to **No**, the event will always run.
- **ADDITIONAL PARAMETERS:** This option can be used to enter additional parameters for the event.



Trigger

In the **Trigger** tab, the conditions under which the event will run can be defined. The event can be triggered either by time-related or by event-related conditions. The following categories of conditions are available in this tab.

- [Once](#)
- [Daily](#)
- [Weekly](#)
- [Monthly](#)
- [As soon as possible](#)
- [At startup / logon](#)
- [When connected to a network](#)

Furthermore there are some settings which can be activated by the [ADVANCED MODE](#) switch which can be used to fine tune those conditions.

Once

If **Once** has been chosen, a specific time when the event will trigger can be chosen. It is possible to define a time within 00:00 and 23:59. The event will be executed once at the specified time.

Daily

If **Daily** has been chosen as trigger for the event, the following can be configured:

- **AT:** This is the time at which the event will be executed. It is possible to define a time within 00:00 and 23:59.
- **RUN THE EVENT EVERY:** This specifies how often the event should run (in days). It will be run each time the given number of days has passed.

Example: If **RUN THE EVENT EVERY** is set to **3** and **13:30** has been configured in the **AT** field, the



event will run every three days at 01:30 PM.

Weekly

If **Weekly** has been selected the following options can be configured.

- **AT:** This is the time at which the event will be executed. It is possible to define a time within 00:00 and 23:59.
- **RUN THE EVENT EVERY:** This specifies how often the event should run (in weeks). It will run each time the given number of weeks has passed.
- **Weekdays:** There is a checkbox for every day of the week. If a day is checked, this day is included in the run. If it is unchecked, the event will not trigger on this day.

Example: If **AT** has been set to **14:45**, **RUN THE EVENT EVERY** has been set to **2**, and the **TUESDAY** checkbox and the **THURSDAY** checkbox have been checked, the event will be triggered at 02:45 PM every third Tuesday and every third Thursday.

Monthly

If **Monthly** has been selected the following options can be configured.

- **AT:** This is the time at which the event will be executed. It is possible to define a time within 00:00 and 23:59.
- **RUN THE EVENT:** This specifies when the event should run. There are two ways to configure



this setting.

- **On day:** If this option is chosen, choose a number between 1 - 30. The event will be executed on this day of the selected months.



Be aware:

When configuring this option, keep in mind that the days of a month vary between 28 and 31 days.

- **On the:** If this option has been chosen, there are two fields for configuration. In the first field there are the following options: **First, Second, Third, Fourth,** and **Last**. This field defines which occurrence of the weekday that can be selected in the second field will be chosen.
- **Months:** There is a checkbox for every month of the year. If a day is checked, this month is included in the run. If it is unchecked, the event will not trigger during this month.

Example: If **AT** is set to **13:00**, **RUN THE EVENT** is set to **On the** and the options **Third** and **Wednesday** have been chosen for it, and in Months **FEBRUARY** and **AUGUST** are checked, the event will be triggered at 01:00 PM on the third Wednesday of February and of August.

As Soon as Possible

If **As soon as possible** has been chosen, the event will trigger as soon as possible.

At Startup / Logon

If **At startup / logon** has been chosen the event will be triggered by the startup of the device / the logon of the user. The **START AFTER** field can be used to configure how much time will pass between the startup / logon and the execution of the event. It is possible to define a time within 00:00 and 23:59. The event will be executed once the specified amount of time has passed.



When Connected to Network

When connected to network → When connected to network

When connected to network START AFTER 00:00 Remove

ADVANCED MODE

Add

If **When connected to network** has been chosen the event will be triggered once the device has a network connection. The **START AFTER** field, can be used to configure how much time will pass between the establishment of the network connection and the execution of the event. It is possible to define a time within 00:00 and 23:59. The event will be executed once the specified amount of time has passed.



Advanced Mode

The following additional options for a trigger are available if the **ADVANCED MODE** switch has been switched to active.

The screenshot shows the 'Advanced Mode' configuration for an event trigger. At the top, it says 'Daily → Every 1 Day(s)' with a 'Remove' button. Below this, there's a dropdown set to 'Daily' and a time field set to '12:00 AM'. A section labeled 'RUN THE EVENT EVERY' has a value of '1' and the unit 'DAYS'. A toggle switch for 'ADVANCED MODE' is turned on. Below this, the 'RUN THE EVENT' section has a dropdown set to 'between', with start and end date fields both set to '11.04.2022'. Another toggle switch for 'REPEAT THE EVENT EVERY' is turned on, with two input fields for 'minutes...' and 'MINUTES, FOR' followed by another 'minutes...' and 'MINUTES.' field. At the bottom, 'THE EVENT WILL TRIGGER' has a dropdown set to 'within' and an input field for 'minutes...' followed by 'MINUTES OF THE SPECIFIED TIME.' An 'Add' button is at the very bottom.

- **RUN THE EVENT:** This option can be used to define when the first run of an event will be or a time period during which the event will run.
 - **from the following date:** This option can be selected in order to run the event from a specific date onward each time the trigger for the event will be met.
 - **between:** This option can be selected in order to select a time period during which the event will be run. It will run each time the trigger is met during this specified period but not before the start date and not after the end date specified in this option.
- **REPEAT THE EVENT:** This setting can be used to repeat the event after a specified time period for a specified time period. If activated, the event will be repeated as defined in the **REPEAT THE EVENT EVERY** and the **MINUTES, FOR ... MINUTES.** time field. The first field defines how often the event will be repeated. The second field defines the time period. For example, if the first field is set to 15 and the second field is set to 60 the event will be repeated every 15 minutes until an hour has passed since the event has been triggered. This option is only available if one of the following trigger has been chosen:
 - **Once**
 - **Daily**
 - **Weekly**
 - **Monthly**
- **THE EVENT WILL TRIGGER:** This setting defines how soon after the trigger for the event has occurred, the event will actually be executed.
 - **exactly at the specified time:** If this option has been chosen, the event will be executed exactly at the moment when the trigger has been met.
 - **within:** If this option has been chosen, it is possible to select a period of time (up to 23 hours and 59 minutes) from the moment the trigger has been met until when the event might actually be executed. The event will occur sometime within this specified time frame.

Edit an Event

Clicking on the **Edit** button in the **Events** section of the **Device Schedule** details while a specific event is selected will open a dialog that can be used to edit this **Event**. The dialog is divided into



the following tabs.

- [General](#)
- [Advanced](#)
- [Trigger](#)

General

In the **General** tab the type of the event and, according to the selected type, some further settings regarding the event can be determined. The following event types are available in this tab.

- [Apply a RMS UEM AppCenter policy](#)
- [Generate a RMS UEM AppCenter inventory](#)
- [Install or update RMS UEM AppCenter failover locations](#)
- [Upload RMS UEM AppCenter managed device files](#)
- [Run a Windows program, script or batch file](#)

Apply a RMS UEM AppCenter Policy

EVENT TYPE

Apply an RMS UEM AppCenter policy

INSTALL/UPDATE THE POLICY WITH THE FOLLOWING LEVEL OF USER INTERACTION LEVEL

RMS UEM AppCenter managed device's current user interaction level

DISPLAY THE CHOSEN USER INTERFACE
ONLY IF A PACKAGE CHANGES ☐

When **Apply a RMS UEM AppCenter policy** is selected as **EVENT TYPE**, the following further options for configuration are available:

- **INSTALL/UPDATE THE POLICY WITH THE FOLLOWING LEVEL OF USER INTERACTION LEVEL:**

Select one of the following (this setting will override the current setting of the device for this specific event):

- **RMS UEM AppCenter managed device's current user interaction level:** The level currently set on the device will be used.
- **Full user interaction:** There is no limit to the user interaction regarding this event, even if the setting of the device normally limits the user interaction.
- **No user interaction or user interface:** For this event, no user interaction is possible and no user interface will be shown, no matter the general setting of the device.
- **Interaction only when error occur:** User interaction for this event will only be possible if an error occurs, otherwise no user interaction will be possible.
- **A progress window, but no user interaction:** The end-user will be shown a progress window, but he will not be able to otherwise interact.



- **DISPLAY THE CHOSEN USER INTERFACE ONLY IF A PACKAGE CHANGES:** This checkbox can be used to limit the times when the user interface will be shown. If set to **Yes**, the user interface will only be shown if a package is changed and it will not be shown if no package is changed during the event.

Generate a RMS UEM AppCenter Inventory

The screenshot shows a configuration form with two dropdown menus. The first dropdown, labeled 'EVENT TYPE', has the option 'Generate an RMS UEM AppCenter inventory' selected. The second dropdown, labeled 'INSTALL/UPDATE THE POLICY WITH THE FOLLOWING LEVEL OF USER INTERACTION LEVEL', has the option 'RMS UEM AppCenter managed device's current user interaction level' selected.

When **Generate a RMS UEM AppCenter inventory** is selected as **EVENT TYPE**, the following further options for configuration are available:

- **INSTALL/UPDATE THE POLICY WITH THE FOLLOWING LEVEL OF USER INTERACTION LEVEL:**
Select one of the following (this setting will override the current setting of the device for this specific event):
 - **RMS UEM AppCenter managed device's current user interaction level:** The level currently set on the device will be used.
 - **Full user interaction:** There is no limit to the user interaction regarding this event, even if the setting of the device normally limits the user interaction.
 - **No user interaction or user interface:** For this event, no user interaction is possible and no user interface will be shown, no matter the general setting of the device.
 - **Interaction only when error occur:** User interaction for this event will only be possible if an error occurs, otherwise no user interaction will be possible.
 - **A progress window, but no user interaction:** The end-user will be shown a progress window, but he will not be able to otherwise interact.

Install or Update RMS UEM AppCenter Failover Locations

The screenshot shows a configuration form with two dropdown menus and a checkbox. The first dropdown, labeled 'EVENT TYPE', has the option 'Install or update RMS UEM AppCenter failover locations' selected. The second dropdown, labeled 'INSTALL/UPDATE THE POLICY WITH THE FOLLOWING LEVEL OF USER INTERACTION LEVEL', has the option 'RMS UEM AppCenter managed device's current user interaction level' selected. At the bottom, there is a checkbox labeled 'DISPLAY THE CHOSEN USER INTERFACE ONLY IF A PACKAGE CHANGES', which is currently unchecked.

When **Install or update RMS UEM AppCenter failover location** is selected as **EVENT TYPE**, the following further options for configuration are available:

- **INSTALL/UPDATE THE POLICY WITH THE FOLLOWING LEVEL OF USER INTERACTION LEVEL:**



Select one of the following (this setting will override the current setting of the device for this specific event):

- **RMS UEM AppCenter managed device's current user interaction level:** The level currently set on the device will be used.
- **Full user interaction:** There is no limit to the user interaction regarding this event, even if the setting of the device normally limits the user interaction.
- **No user interaction or user interface:** For this event, no user interaction is possible and no user interface will be shown, no matter the general setting of the device.
- **Interaction only when error occur:** User interaction for this event will only be possible if an error occurs, otherwise no user interaction will be possible.
- **A progress window, but no user interaction:** The end-user will be shown a progress window, but he will not be able to otherwise interact.
- **DISPLAY THE CHOSEN USER INTERFACE ONLY IF A PACKAGE CHANGES:** This checkbox can be used to limit the times when the user interface will be shown. If set to **Yes**, the user interface will only be shown if a package is changed and it will not be shown if no package is changed during the event.

Upload RMS UEM AppCenter Managed Device Files

EVENT TYPE

Upload RMS UEM AppCenter managed device files

UPLOAD THE FOLLOWING FILES FROM THE MANAGED DEVICE

Upload all file types

When **Upload RMS UEM AppCenter managed files** is selected as **EVENT TYPE**, the following further options for configuration are available:

- **UPLOAD THE FOLLOWING FILES FROM THE MANAGED DEVICE:**
Select one of the following:
 - **Upload all file types:** Select this option in order to upload all collected files.
 - **Inventories:** Select this option in order to upload the inventory files.
 - **Installation event logs:** Select this option in order to upload the installation event logs.

Run a Windows Program, Script, or Batch File

EVENT TYPE

Run a Windows program, script or batch file

TARGET

START IN

PARAMETERS

When **Run a Windows program, script or batch** is selected as **EVENT TYPE**, the following further options for configuration are available:



- **TARGET:** The path where the file can be found on the managed device needs to be entered here. For example: `cmd`.
- **START IN:** The path where the file will be executed on the managed device can be entered here. In most use cases this field can be left empty. An example for a path would be `$(TempDirectory)`.
- **PARAMETERS:** This field can be used to define additional parameters for the application that is about to run can be defined. For example: `/c "echo $(TempDirectory) >> C:\tmp\test.txt"`.

Advanced

In the **Advanced** tab of the dialog some information regarding the behavior of the event can be configured.

DELAY NEXT RUN

☒ Delay next run by

Delay the next execution of the event after a successful run.

RERUN BEHAVIOR

If the event has not been run for some reason, the managed device's task scheduler should use the selected behavior.

ONLY RUN THIS EVENT IF A NETWORK CONNECTION IS AVAILABLE ☐

ADDITIONAL PARAMETERS

In this tab the following options are available:

- **DELAY NEXT RUN:** This option can be activated in order to delay the next run. It is possible to define the delay either by the number of minutes, hours, or days by selecting the unit of measurement in the dropdown box and entering the number in the field located on the left of the dropdown box.
- **RERUN BEHAVIOR:** This option defines how the event will behave if one or more occurrences of the event have been missed. The following behaviors are available:
 - Ignore missed events
 - Run all missed events
 - Run only the last event missed
- **ONLY RUN THIS EVENT IF A NETWORK CONNECTION IS AVAILABLE:** If set to **Yes**, the event only runs if a network is available. If set to **No**, the event will always run.
- **ADDITIONAL PARAMETERS:** This option can be used to enter additional parameters for the event.



Trigger

In the **Trigger** tab, the conditions under which the event will run can be defined. The event can be triggered either by time-related or by event-related conditions. The following categories of conditions are available in this tab.

- [Once](#)
- [Daily](#)
- [Weekly](#)
- [Monthly](#)
- [As Soon as Possible](#)
- [At Startup / Logon](#)
- [When Connected to a Network](#)

Furthermore there are some settings which can be activated by the **Advanced Mode** switch which can be used to fine tune those conditions.

Once

If **Once** has been chosen, a specific time when the event will trigger can be chosen. It is possible to define a time within 00:00 and 23:59. The event will be executed once at the specified time.

Daily

If **Daily** has been chosen as trigger for the event, the following can be configured:

- **AT:** This is the time at which the event will be executed. It is possible to define a time within 00:00 and 23:59.
- **RUN THE EVENT EVERY:** This specifies how often the event should run. It will be run each time the given number of days has passed.

Example: If **RUN THE EVENT EVERY** is set to **3** and **13:30** has been configured in the **AT** field, the



event will run every three days at 01:30 PM.

Weekly

If **Weekly** has been selected the following options can be configured.

- **AT:** This is the time at which the event will be executed. It is possible to define a time within 00:00 and 23:59.
- **RUN THE EVENT EVERY:** This specifies how often the event should run (in weeks). It will run each time the given number of weeks has passed.
- **Weekdays:** There is a checkbox for every day of the week. If a day is checked, this day is included in the run. If it is unchecked, the event will not trigger on this day.

Example: If **AT** has been set to **14:45**, **RUN THE EVENT EVERY** has been set to **2**, and the **TUESDAY** checkbox and the **THURSDAY** checkbox have been checked, the event will be triggered at 02:45 PM every third Tuesday and every third Thursday.

Monthly

If **Monthly** has been selected, the following options can be configured.

- **AT:** This is the time at which the event will be executed. It is possible to define a time within 00:00 and 23:59.
- **RUN THE EVENT:** This specifies when the event should run. There are two ways to configure



this setting.

- **On day:** If this option is chosen, choose a number between 1 - 30. The event will be executed on this day of the selected months.



Be aware:

When configuring this option, keep in mind that the days of a month vary between 28 and 31 days.

- **On the:** If this option has been chosen, there are two fields for configuration. In the first field there are the following options: **First, Second, Third, Fourth,** and **Last**. This field defines which occurrence of the weekday that can be selected in the second field will be chosen.
- **Months:** There is a checkbox for every month of the year. If a day is checked, this month is included in the run. If it is unchecked, the event will not trigger during this month.

Example: If **AT** is set to **13:00**, **RUN THE EVENT** is set to **On the** and the options **Third** and **Wednesday** have been chosen for it, and in Months **FEBRUARY** and **AUGUST** are checked, the event will be triggered at 01:00 PM on the third Wednesday of February and of August.

As Soon as Possible

If **As soon as possible** has been chosen, the event will trigger as soon as possible.

At Startup / Logon

If **At startup / logon** has been chosen the event will be triggered by the startup of the device / the logon of the user. The **START AFTER** field can be used to configure how much time will pass between the startup / logon and the execution of the event. It is possible to define a time within 00:00 and 23:59. The event will be executed once the specified amount of time has passed.



When Connected to Network

When connected to network → When connected to network

When connected to network START AFTER 00:00 Remove

ADVANCED MODE

Add

If **When connected to network** has been chosen, the event will be triggered once the device has a network connection. The **START AFTER** field can be used to configure how much time will pass between the establishment of the network connection and the execution of the event. It is possible to define a time within 00:00 and 23:59. The event will be executed once the specified amount of time has passed.



Advanced Mode

The following additional options for a trigger are available if the **ADVANCED MODE** switch has been switched to active.

Daily → Every 1 Day(s) Remove

Daily AT 12:00 AM

RUN THE EVENT EVERY 1 DAYS

ADVANCED MODE

RUN THE EVENT between 11.04.2022 AND 11.04.2022

REPEAT THE EVENT EVERY minutes... MINUTES, FOR minutes... MINUTES.

THE EVENT WILL TRIGGER within minutes... MINUTES OF THE SPECIFIED TIME.

Add

- **RUN THE EVENT:** This option can be used to define when the first run of an event will be or a time period during which the event will run.
 - **from the following date:** This option can be selected in order to run the event from a specific date onward each time the trigger for the event will be met.
 - **between:** This option can be selected in order to select a time period during which the event will be run. It will run each time the trigger is met during this specified period but not before the start date and not after the end date specified in this option.
- **REPEAT THE EVENT:** This setting can be used to repeat the event after a specified time period for a specified time period. If activated, the event will be repeated as defined in the **REPEAT THE EVENT EVERY** and the **MINUTES, FOR ... MINUTES.** time field. The first field defines how often the event will be repeated. The second field defines the time period. For example, if the first field is set to 15 and the second field is set to 60 the event will be repeated every 15 minutes until an hour has passed since the event has been triggered. This option is only available if one of the following trigger has been chosen:
 - **Once**
 - **Daily**
 - **Weekly**
 - **Monthly**
- **THE EVENT WILL TRIGGER:** This setting defines how soon after the trigger for the event has occurred, the event will actually be executed.
 - **exactly at the specified time:** If this option has been chosen, the event will be executed exactly at the moment when the trigger has been met.
 - **within:** If this option has been chosen, it is possible to select a period of time (up to 23 hours and 59 minutes) from the moment the trigger has been met until which the event might actually be executed. The event will occur sometime within this specified time frame.



Edit a Device Schedule

The **Properties** dialog is used to edit an existing Device Schedule.

The screenshot shows a 'Properties' dialog box with a close button (X) in the top right corner. It contains the following fields and elements:

- IMAGE:** A square placeholder with a gear icon.
- NAME:** A text input field containing 'Example Device Schedule'.
- VERSION:** Four separate input fields for version components, containing '1', '0', '0', and '1' respectively.
- Information:** A grey box with an information icon and text: 'The version number is used by the Deployment Manager on the managed devices to coordinate application updates. Increase this number whenever you want to distribute a revised version of your application.'
- COMMENT:** A large text area containing 'This is an example device schedule.'
- Buttons:** 'Save changes' (blue) and 'Discard' (grey) at the bottom.

The following options are available in the dialog.

- **IMAGE:** Clicking on the image will open a file browser. Browse for an image to customize the image for the **Device Schedule** (the following file formats are supported: .gif, .jpg, .jpeg, and .png).
- **NAME:** The name for the **Device Schedule**.
- **VERSION:** The version number of the **Device Schedule** which is further divided into:
 - Major
 - Minor
 - Build
 - RevisionSince the fields have already been separated, no further separators are allowed.
- **COMMENT:** A comment containing further information about the **Device Schedule**.

This option only edits the information about the **Device Schedule**. How to add or edit events



assigned to the **Device Schedule** is described in the [Add an Event](#) and an [Edit an Event](#) sections.



Scheduled Tasks

The **Scheduled Tasks** section contains an overview of the scheduled tasks that are currently configured.

Name	Interval
Hourly Azure Import	Every hour
Security Groups	At 10:00 AM, only on Monday

The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the screen can be used to refresh the view.
- **Add** - The **Add** button on the top left of the screen can be used to add a new scheduled task to the list. For more information see [Add a Scheduled Task](#).
- **Edit** - The **Edit** button on the top left of the screen can be used to edit a scheduled task if one of the tasks in the list has been selected. For more information see [Edit a Scheduled Task](#).
- **Delete** - The **Delete** button on the top left of the screen can be used to delete one or more scheduled tasks if one or more tasks in the list have been selected.
- **Search field** - The **Search** field can be found on the top right of the screen. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.

When clicking on the name of a scheduled task, the task will be opened.

Scheduled Task Details

The details for a specific scheduled task are divided into two parts. On the left side, the general information about the scheduled task can be found. This part contains the name, the type, the interval for which the task is scheduled, as well as the settings that have been defined for the scheduled task.



The screenshot shows the 'SCHEDULED TASKS' section in the Raymanagesoft interface. On the left, a task named 'Test' is listed with details: TYPE: Azure AD Import, INTERVAL: At 10:00 AM, on day 1 of the month, and various group and device settings. On the right, the 'Task executions' table lists two successful runs. The first run on May 5, 2021, at 9:30:41 AM, lasted 00:00:29 and was triggered by 'root'. The second run on May 1, 2021, at 10:00:00 AM, lasted 00:00:46 and was triggered by 'System'. A 'Refresh' button is located above the table.

Status	Start Date	Duration	Trigger
●	May 5, 2021, 9:30:41 AM	00:00:29	root
●	May 1, 2021, 10:00:00 AM	00:00:46	System

On the right side of the section, the executions of the tasks are listed. If clicking on one of the items of the list, all information regarding this specific run of the scheduled task are found and listed in the **Scheduled Task Execution Details** dialog. In this dialog the duration of the task, how the task was triggered, the start and end date, the state as well as detailed results for the task can be found.

In addition to the general information regarding the task and the list of the executions of the task, the following actions are available in this section.

- **Run** - The **Run** button on the top left of the screen can be used to manually run the scheduled task despite of its schedule.
- **Edit** - The **Edit** button on the top left of the screen can be used to edit this scheduled task. For more information see [Edit a Scheduled Task](#).
- **Delete** - The **Delete** button on the top left of the screen can be used to delete this scheduled task.

Add a Scheduled Task

The **Add scheduled task** dialog contains the following tabs which are used to configure the necessary information for the scheduled task.

- [General](#)
- [Schedule](#)
- [Configurations](#)

General

In the **General** tab some of the general information is defined. All of the fields in this tab are mandatory information for the creation of a scheduled task.



Add scheduled task

General Schedule Configurations

NAME *

Example

TYPE *

Azure AD Import

Add Discard

The following information can be configured in this tab.

- **NAME:** The name for the scheduled task that will be shown.
- **TYPE:** A dropdown menu from which to choose the type of the scheduled task. The available task types depend on the the integrations that have been configured.

Schedule

In the **Schedule** tab the frequency of how often a scheduled task is executed is defined. It is possible to select between different intervals which than can be configured in order to best suit the scheduled task.

The following intervals can be selected for the schedule:

- [Hourly](#)
- [Daily](#)
- [Weekly](#)
- [Monthly](#)
- [Advanced](#)

Hourly

When the **Hourly** interval has been selected, the hours and minutes between the execution of the scheduled task can be selected using the **HOUR(S)** and the **MINUTE(S)** dropdown box.



Add scheduled task

General Schedule Configurations

INTERVAL: *
Hourly

HOUR(S) MINUTE(S)
1 0

Add Discard

In the **HOUR(S)** dropdown box the number of hours in between the execution of the scheduled task (up to 23 hours) can be selected. In the **MINUTE(S)** dropdown menu the number of minutes (up to 59 minutes) can be selected.

The shortest time period to be configured for the scheduled task to be executed using this option is every hour. The longest period that can be configured for the execution of the scheduled task is every 23 hours and 59 minutes.

Daily

If a task is scheduled to be executed on a daily base, there are still some more options to consider for the configuration.

Add scheduled task

General Schedule Configurations

INTERVAL: *
Daily

DAY SELECTION
Every week day

HOUR(S) MINUTE(S)
10 0

Add Discard

Selecting **Every day** in the **DAY SELECTION** dropdown box will lead to the task being executed every day, selecting **Every week day** will lead to the task only being executed from Monday to Friday.

DAY SELECTION

Every week day

Every day

Every week day



The **HOUR(S)** and the **MINUTE(S)** dropdown menus are used to define the exact time (in a 24 hours format) the scheduled task is started. For example, if **14** is selected for **HOUR(S)** and **30** is selected for **MINUTE(S)** the scheduled task will be started at 02:30 PM on the defined day.

Weekly

If **Weekly** has been chosen as interval for the execution of the scheduled task, one or more days of the week can be selected by selecting the respective checkbox for the day.

The screenshot shows a window titled "Add scheduled task" with a close button (X) in the top right corner. It has three tabs: "General", "Schedule" (which is active), and "Configurations". Under the "Schedule" tab, there is a section labeled "INTERVAL:" with a dropdown menu currently showing "Weekly". Below this, there are seven checkboxes for the days of the week: MONDAY (checked), TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, and SUNDAY. At the bottom of the form, there are two dropdown menus: "HOUR(S)" with the value "10" and "MINUTE(S)" with the value "0". At the very bottom are two buttons: "Add" (in blue) and "Discard" (in grey).

The **HOUR(S)** and the **MINUTE(S)** dropdown menus are used to define the exact time (in a 24 hours format) the scheduled task is started. For example, if **14** is selected for **HOUR(S)** and **30** is selected for **MINUTE(S)** the scheduled task will be started at 02:30 PM on the defined day.

Monthly

There are two different options how to use monthly scheduling.

- [By Date](#)
- [By Occurrence](#)



By Date

If a scheduled task is set to **Monthly** and **By date**, the task can be configured to occur on a specific weekday. The task will then be executed on this specific day every month or every configured period of months.

The screenshot shows the 'Add scheduled task' dialog box with the 'Schedule' tab selected. The 'INTERVAL' dropdown is set to 'Monthly'. The 'By date' dropdown is selected. Under 'OCCURRENCE', the first dropdown is set to 'First' and the second to 'Monday'. The 'EVERY MONTH(S)' dropdown is set to '1'. The 'HOUR(S)' dropdown is set to '10', 'MINUTE(S)' is set to '0', and 'START MONTH' is set to 'January'. At the bottom are 'Add' and 'Discard' buttons.

OCCURRENCE consists of two different dropdown menus. In the first dropdown menu it is possible to choose between **First**, **Second**, **Third**, **Fourth**, or **Fifth**. The second one is a list of the days of the week. For example, if **Second** is selected in the first dropdown menu and **Friday** is selected for the second dropdown menu, the scheduled task would always be executed on the second Friday of each month or the specified interval of months.

The **EVERY MONTH(S)** dropdown menu contains numbers from **1** to **12**. This defines the exact number of months between the occurrences of the scheduled task. For example, if set to **4**, the scheduled task will be executed every four months.

The **HOUR(S)** and the **MINUTE(S)** dropdown menus are used to define the exact time (in a 24 hours format) the scheduled task is started. For example, if **14** is selected for **HOUR(S)** and **30** is selected for **MINUTE(S)** the scheduled task will be started at 02:30 PM on the defined day.

The last thing to define when using this option is the month the execution of the scheduled task is about to start. This can be done using the **START MONTH** dropdown menu. In this dropdown menu it is possible to choose from each month of the year. For example, if **May** is selected, the scheduled task will first be executed in the month of May and from that point on follow the configured interval.

By Occurrence

If a scheduled task is set to **Monthly** and **By first occurrence**, the task can be configured to occur on a specific day of the month. The task will then be executed on this specific day every month or every configured period of months.



The **DAY OF MONTH** dropdown menu is used to configure the specific day of the month. The given options are **1st day** to **31st day** or **Last day**. For example, if choosing **15th day**, the scheduled task will be executed on the 15th of each month or the interval of months configured in the **EVERY MONTH(S)** dropdown menu.



Be aware:

When configuring this option, keep in mind that the days of a month vary between 28 and 31 days. To configure the execution for the last day of the month, the **Last day** option should be used.

The **EVERY MONTH(S)** dropdown menu contains numbers from **1** to **12**. This defines the exact number of months between the occurrences of the scheduled task. For example, if set to **4**, the scheduled task will be executed every four months.

The **HOUR(S)** and the **MINUTE(S)** dropdown menus are used to define the exact time (in a 24 hours format) the scheduled task is started. For example, if **14** is selected for **HOUR(S)** and **30** is selected for **MINUTE(S)** the scheduled task will be started at 02:30 PM on the defined day.

This option also has a checkbox labeled **DURING THE NEAREST WEEKDAY**. If this checkbox is checked, RayManageSoft Unified Endpoint Manager will execute the scheduled task on the closest weekday (Monday to Friday) to the configured date. For example, if the task is scheduled for execution for the 15th of a month, but the 15th is a Sunday, the task will only be executed on the 15th if the checkbox is unchecked. If it is checked, the task will be executed on the 16th instead.

Advanced

The option **Advanced** enables for a more customized schedule for the scheduled task.



Add scheduled task

General Schedule Configurations

INTERVAL: *
Advanced

CRON EXPRESSION
0 15 10 L-2 * ?

Add Discard

When **Advanced** has been selected, the schedule can be defined using CRON expression.

An introduction into CRON expressions can be found at <https://www.quartz-scheduler.net>.

Configurations

In the **Configurations** tab the filters for the scheduled task can be defined. This tab is not available for all scheduled tasks. The following represents the settings that will be available for the AAD import tasks. The settings for other scheduled tasks vary.

Add scheduled task

General Schedule Configurations

GROUP FILTER

MICROSOFT 365 GROUPS	☒
DISTRIBUTION GROUPS	☒
SECURITY GROUPS	☒
EMAIL ENABLED SECURITY GROUPS	☒

SENSITIVE DATA FILTER

DEVICE OWNER NAME	☒

ADVANCED FILTER

ALLOW NEW DEVICES	☒

Add Discard

The filters are divided into different groups for which one or more filters are available. The different filters can be activated by checking the checkbox next to the filter name. If the checkbox is not checked, the filter is deactivated.

- **GROUP FILTER**



- **MICROSOFT 365 GROUPS:** If checked, all **Microsoft Office 365** groups will be gathered.
- **DISTRIBUTION GROUPS:** If checked, all **Distribution** groups will be gathered.
- **SECURITY GROUPS:** If checked, all **Security** groups will be gathered.
- **E-MAIL ENABLED SECURITY GROUPS:** If checked, all **E-mail enabled security** groups will be gathered.
- **SENSITIVE DATA FILTER**
 - **DEVICE OWNER NAME:** If checked, the device owners will be imported.
- **ADVANCED FILTER**
 - **ALLOW NEW DEVICES:** If checked, devices which are not already managed by RayManageSoft Unified Endpoint Manager will be imported.

Edit a Scheduled Task

The **Edit scheduled task** dialog contains the following tabs which are used to configure the necessary information for the scheduled task.

- [General](#)
- [Schedule](#)
- [Configurations](#)

General

In the **General** tab some of the general information is defined.

The screenshot shows a dialog box titled "Edit scheduled task" with a close button (X) in the top right corner. Below the title bar are three tabs: "General", "Schedule", and "Configurations". The "General" tab is selected. Inside the "General" tab, there is a "NAME" field with a red asterisk indicating it is mandatory, containing the text "ASD". Below it is a "TYPE" dropdown menu showing the value "1". At the bottom of the dialog are two buttons: "Save changes" and "Discard".

The following information is available in this tab.

- **NAME:** The name for the scheduled task that will be shown. This field is mandatory and cannot be empty.
- **TYPE:** This value cannot be configured when editing an already existing scheduled task.

Schedule

In the **Schedule** tab of the **Edit scheduled task** dialog, the schedule for the scheduled task can be changed.



The configuration of the schedule when editing a scheduled task is identical to configuring the schedule when adding a scheduled task. For detailed information refer to the [Schedule](#) chapter for the **Add scheduled task** dialog.

Configurations

In the **Configurations** tab the filters for the scheduled task can be defined. This tab is only available for AAD import tasks, therefore, if no Active Directory integration has been configured, this tab will not be available.

The filters are divided into different groups for which one or more filters are available. The different filters can be activated by checking the checkbox next to the filter name. If the checkbox is not checked, the filter is deactivated.

- **GROUP FILTER**
 - **MICROSOFT 365 GROUPS:** If checked, all **Microsoft Office 365** groups will be gathered.
 - **DISTRIBUTION GROUPS:** If checked, all **Distribution** groups will be gathered.
 - **SECURITY GROUPS:** If checked, all **Security** groups will be gathered.
 - **E-MAIL ENABLED SECURITY GROUPS:** If checked, all **E-mail enabled security** groups will

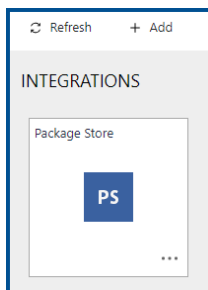


be gathered.

- **SENSITIVE DATA FILTER**
 - **DEVICE OWNER NAME:** If checked, the device owners will be imported.
- **ADVANCED FILTER**
 - **ALLOW NEW DEVICES:** If checked, devices which are not already managed by RayManageSoft Unified Endpoint Manager will be imported.

Integrations

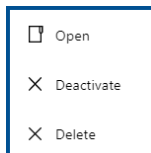
In this section integrations of other applications into RayManageSoft Unified Endpoint Manager can be added and existing integrations are managed. Each integration that has been added is shown as a separate tile.



The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the screen can be used to refresh the view.
- **Add** - The **Add** button on the top left of the screen can be used to add a new integration. For more information see [Add an Integration](#).

In order to edit an integration, it is necessary to open it. An integration can be opened by first clicking on the ... button at the right bottom of the tile. This will open the context menu for the integration.



In the context menu the following options are available:

- **Open:** This option will open a dialog for the integration. For more information see [Edit an Integration](#).
- **Deactivate:** This option can be used to deactivate the integration without deleting it.
- **Delete:** This option can be used to delete the integration.



Add an Integration

In this dialog the following integrations types are available for selection.

- [Azure Active Directory](#)
- [RayVentory Server](#)
- [RayMobile](#)
- [Package Store](#)
- [Local Active Directory](#)
- [Catalog](#)

Azure Active Directory

TYPE *

Azure Active Directory

ACTIVE DIRECTORY SYNCED:
☐

CLIENT / APPLICATION ID: *

CLIENT / APPLICATION SECRET: *

TENANT: *

API URL: *

<https://graph.microsoft.com/>

INSTANCE: *

<https://login.microsoftonline.com/{0}>



The following information is needed if an integration of an Azure Active Directory should be added:

- **ACTIVE DIRECTORY SYNCED:** This switch is used in order to specify if the Active Directory sync is enabled or not.



Be aware:

If the Active Directory sync is enabled, this will prevent users from creating device group assignments manually. While an import process is running unmanaged devices, device group assignments, group child assignments, and groups which are no longer present in the Azure Active Directory will be deleted from RayManageSoft Unified Endpoint Manager. This ensures the synchronicity between the Azure Active Directory and RayManageSoft Unified Endpoint Manager.

- **CLIENT / APPLICATION ID:** Enter the application ID for the Azure Active Directory. Information on how to create / where to find the ID can be found in the [Microsoft Documentation](#).
- **CLIENT / APPLICATION SECRET:** Enter the application secret for the Azure Active Directory. Information on where to find the secret can be found in the [Microsoft Documentation](#).
- **TENANT:** Enter the tenant for the Azure Active Directory integration. Information on how to create a tenant in Azure Active Directory can be found in the [Microsoft Documentation](#).
- **API URL:** This field contains the API URL. By default, this is `http://graph.microsoft.com/`.
- **INSTANCE:** This field contains the URL of the instance. By default, this is `https://login.microsoftonline.com/{0}`.

RayVentory Server

TYPE *

RayVentory Server

NDI FORWARDING:

☐

i The forwarding of NDI files ensures that the inventory data of the managed devices is not only available in RMS UEM, but also on the specified RayVentory server.

URL: *

USERNAME: *

PASSWORD: *

The following information is needed if an integration of a RayVentory Server should be added.

- **NDI FORWARDING:** This switch controls if NDI files will be forwarded or not.



Be aware:



	The forwarding of NDI files ensures that the inventory data of managed devices is not only available in RayManageSoft Unified Endpoint Manager but also on the specified RayVentory Server.

- **URL:** Enter the URL of the RayVentory Server.
- **USERNAME:** Enter the username of the user account that is used for the integration.
- **PASSWORD:** Enter the password for the user account that is used for the integration.

RayMobile

TYPE *

RayMobile

ENDPOINT: *

http://188.99.08.240:8800/

HELP

To integrate RayMobile into RayManageSoft Unified Endpoint Management, please download this Docker image:

Docker image

When starting up the container, please provide **PROTOCOL**, **HOST** and **PORT** environment variables of your RayMobile instance. Please also expose the container on some port. Detailed instruction can be found at the link above.

When the container is running, provide the address of the container in the endpoint field above.

The following information is needed if a RayMobile integration should be added.

- **ENDPOINT:** The IP or URL and the portnumber of the running Docker container created using the Docker image provided in this dialog.

In order to integrate RayMobile into RayManageSoft Unified Endpoint Manager it is necessary to create a Docker container.

After starting up the container, the **PROTOCOL**, **HOST**, and **PORT** environment variables of the RayMobile proxy need to be provided. It is also necessary that one port of the container is accessible.

To create the Docker container and gain the necessary information execute the following steps:

1. Download the provided Docker image by clicking on the green button labeled Docker image.
2. Create a DOMAIN which will serve as RayMobile proxy.
3. Obtain an SSL certificate for the domain and place both (certificate and private key) in the certs folder. Take note of the file names.
4. Edit the `default.conf` file by replacing all the placeholders (marked <<PLACEHOLDER>>). The following placeholders can be found in the file:

- o `server_name` - the selected DOMAIN name
- o `ssl_certificate` - name of the certificate file placed in the certs folder (for example: `certificate.crt`)



- `ssl_certificate_key` - the name of the key file placed in the certs folder (for example: `key.key`)
 - `proxy_pass` - URL of the RayMobile instance (for example: `https://raymobile.company.org:443` [This is not the DOMAIN that has been selected])
 - `proxy_set_header` - the hostname of the URL that can be found in the `proxy_pass` (for example: `raymobile.company.org`)
5. The proxy is based on nginx server.
For further customizations refer to <https://nginx.org/en/docs/>.
 6. Start the proxy using the following command:
`docker-compose up -d`
 7. The proxy should now be up and running at:
`https://DOMAIN:8800`
 8. Copy the URL of the proxy and paste this URL into the Endpoint field in RayManageSoft Unified Endpoint Manager.

Package Store

The following information is needed if a Package Store integration should be added.

- **API KEY:** Enter the API key that is used for the Package Store. The API key can be found in the delivery documents. In case your API key is missing, contact your Raynet representative.



Local Active Directory

TYPE *

Local Active Directory

DOMAIN: *

USER: *

PASSWORD: *

Add Discard

The following information is needed if a Local Active Directory integration should be added.

- **DOMAIN:** The name of the local AD domain.
- **USER:** The username of the AD account that will be used.
- **PASSWORD:** The password of the AD account that will be used.

Catalog

TYPE *

Catalog

API KEY: *

Add Discard

The following information is needed if a Catalog integration should be added.

- **API KEY:** Enter the API key that is used for the connection with RayVentory Catalog. To learn how to create an API key for RayVentory Catalog read the [Create an API key for RayVentory Catalog](#) chapter.

After the API key has been entered, it is necessary to execute the scheduled task for the Catalog integration. This task needs to be created first. Information on how to create the scheduled task for the Catalog integration can be found [here](#).



Note:

A detailed description of the functionality of the RayVentory Catalog can be found in the RayVentory Catalog documentation.

Create an API Key for RayVentory Catalog

To receive an API key, log into RayVentory Catalog and continue with the following steps.

1. Go to the User Profile by hovering the mouse pointer over the logged in user on the top right of the screen.
2. Select **Profile** from the context menu.
3. Click on the **+ Add...** button.
4. In the **Add Token** dialog, enter a descriptive name for the token (for example: *RayManageSoft UEM Integration*).
5. Copy the API key from the **API KEY** field and save it to a secure location.



Be aware:

The API key will only be shown this one time. If the API key gets lost, it will be necessary to create a new key.

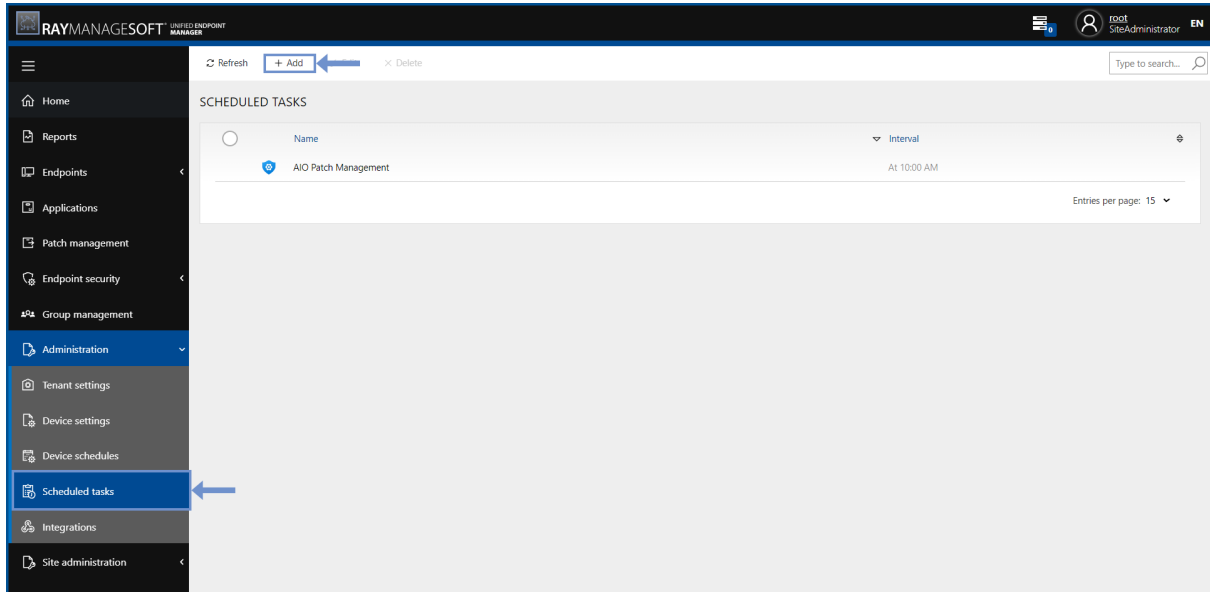
6. Click on the **Save changes** button in order to finalize the process.

The newly created API key can now be used to create the integration.



Create a Scheduled Task for the Catalog Integration

To create a scheduled task for the Catalog integrations go to **Administration > Scheduled tasks**.



In the Scheduled tasks section, click on the **+ Add** button in order to open the **Add scheduled task** dialog. The **Add scheduled task** dialog is divided into three different tabs:

- [General](#)
- [Schedule](#)
- [Configurations](#)

After the scheduled task has been created accordingly, run it manually to ensure that it is active. To run the task manually, click on the task and click on the **Run** button located at the top left above the scheduled tasks details.

General

In the **General** tab, enter a name for the Catalog task into the **NAME** field. The name should be descriptive (for example: *Catalog Integration*).



Add scheduled task [X]

General | Schedule | Configurations

NAME *
Catalog Integration

TYPE *
Catalog

Add Discard

In the **TYPE** dropdown menu, select **Catalog** as type.

Schedule

In the **Schedule** tab, define how often the Catalog task will be executed.

Add scheduled task [X]

General | Schedule | Configurations

INTERVAL *
Hourly

HOUR(S) MINUTE(S)
1 0

Add Discard

It is recommended to use the default settings for the Catalog task:

- **INTERVAL:** Hourly
- **HOUR(S):** 1
- **MINUTE(S):** 0

Configurations

In the **Schedule** tab, define the further settings for the Catalog task.



Add scheduled task

General Schedule Configurations

DEVICE FILTER

NEW INVENTORY AVAILABLE ☒

REFRESH INTERVAL EXCEEDED

Add **Discard**

It is recommended to use the default settings for the Catalog task:

- **NEW INVENTORY AVAILABLE:** checked
- **REFRESH INTERVAL EXCEEDED:** 1

Edit an Integration

The dialog depends on the integration that has been selected for editing. Currently, the following types are available.

- [Azure Active Directory](#)
- [RayVentory Server](#)
- [RayMobile](#)
- [Package Store](#)
- [Local Active Directory](#)
- [Catalog](#)

Azure Active Directory

ACTIVE DIRECTORY SYNCED: ☐

CLIENT / APPLICATION ID: *

CLIENT / APPLICATION SECRET: *

TENANT: *

API URL: *

INSTANCE: *

The following information can be edited if the chosen integration is of the type Azure Active Directory:



- **ACTIVE DIRECTORY SYNCED:** This switch is used in order to specify if the Active Directory sync is enabled or not.



Be aware:

If the Active Directory sync is enabled, this will prevent users from creating device group assignments manually. While an import process is running unmanaged devices, device group assignments, group child assignments, and groups which are no longer present in the Azure Active Directory will be deleted from RayManageSoft Unified Endpoint Manager. This ensures the synchronicity between the Azure Active Directory and RayManageSoft Unified Endpoint Manager.

- **CLIENT / APPLICATION ID:** Enter the application ID for the Azure Active Directory. Information on how to create / where to find the ID can be found in the [Microsoft Documentation](#).
- **CLIENT / APPLICATION SECRET:** Enter the application secret for the Azure Active Directory. Information on where to find the secret can be found in the [Microsoft Documentation](#).
- **TENANT:** Enter the tenant for the Azure Active Directory integration. Information on how to create a tenant in Azure Active Directory can be found in the [Microsoft Documentation](#).
- **API URL:** This field contains the API URL. By default, this is `http://graph.microsoft.com/`.
- **INSTANCE:** This field contains the URL of the instance. By default, this is `https://login.microsoftonline.com/{0}`.

RayVentory Server

NDI FORWARDING:

☐

The forwarding of NDI files ensures that the inventory data of the managed devices is not only available in RMS UEM, but also on the specified RayVentory server.

URL: *

USERNAME: *

PASSWORD: *

The following information can be edited if the integration is of the type RayVentory Server:

- **NDI FORWARDING:** This switch controls if NDI files will be forwarded or not.



Be aware:

The forwarding of NDI files ensures that the inventory data of managed devices is not only available in RayManageSoft Unified Endpoint Manager but also on the specified RayVentory Server.

- **URL:** Enter the URL of the RayVentory Server.



- **USERNAME:** Enter the username of the user account that is used for the integration.
- **PASSWORD:** Enter the password for the user account that is used for the integration.

RayMobile

The following information can be edited if the integration is of the type RayMobile.

- **ENDPOINT:** The IP or URL and the portnumber of the running Docker container created using the Docker image provided in this dialog.

In order to integrate RayMobile into RayManageSoft Unified Endpoint Manager it is necessary to create a Docker container. In order to create this container, download the provided Docker image by clicking on the green button labeled Docker image and follow the instructions given in the installation dialog. After starting up the container, the **PROTOCOL, HOST, and PORT** environment variables of the RayMobile instance need to be provided. It is also necessary that one port of the container is accessible.

Package Store

The following information can be edited if the integration is of the type Package Store.

- **API KEY:** Enter the API key that is used for the Package Store. The API key can be found in the delivery documents. In case your API key is missing, contact your Raynet representative.



Local Active Directory

TYPE *	Local Active Directory
DOMAIN: *	MyDomain
USER: *	MyUsername
PASSWORD: *	*****

The following information can be edited if the integration is of the type Local Active Directory.

- **DOMAIN:** The name of the local AD domain.
- **USER:** The username of the AD account that will be used.
- **PASSWORD:** The password of the AD account that will be used.

Catalog

API KEY: *	ABC0DEF-G12HIJ3-K4LM56N-7PQR89S

The following information can be edited if the integration is of the type RayVentory Catalog.

- **API KEY:** Enter the API key that is used for the connection with RayVentory Catalog.

Information on how to create an API key for the RayVentory Catalog integration can be found [here](#).



Site-Administration

The **Site-Administration** category of the sidebar contains the following subcategories.

- [All Users](#)
- [Tenants](#)
- [System Settings](#)

All Users

This section contains a list of all users that exist in the RayManageSoft Unified Endpoint Manager instance.

Name	E-mail	Company	Site Administrator
example.user	example.user@raynet.de	-	✓
root	root@raynet.de	-	✓
System	support@raynet.de	-	✓

The following actions are available in this section.

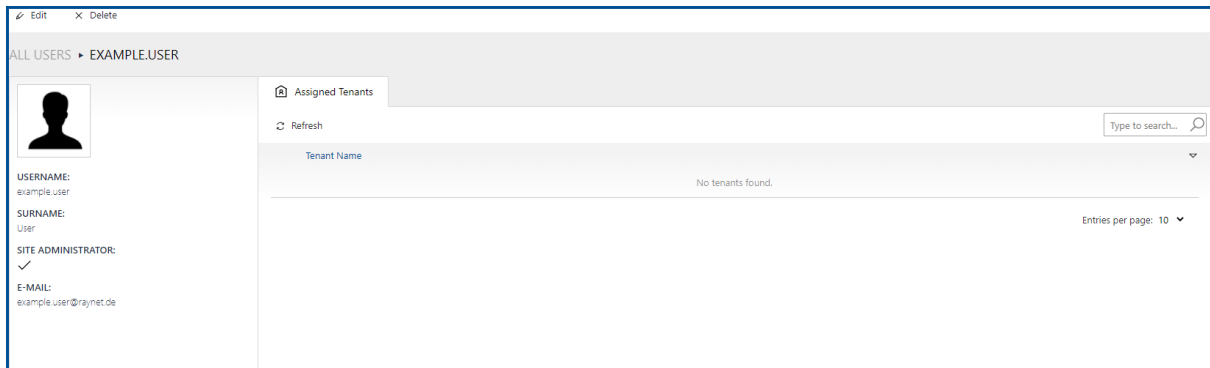
- **Refresh** - The **Refresh** button on the top left of the screen can be used to refresh the view.
- **Add** - The **Add** button on the top left of the screen can be used to add a new user to the RayManageSoft Unified Endpoint Manager instance. For more information see [Add a User](#).
- **Search field** - The **Search** field can be found on the top right of the screen. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.

When clicking on a specific user, the details for this user will be opened.

User Details

The detail page of a user is divided into two different areas. The first part located on the left contains the details of the user. This includes the username, the information if the user is site administrator, and the e-mail of the user. The information shown here depend on the information given for the user when it was created / last edited.

The second part of the right side contains a list of the tenants which are assigned to the user.



The following actions are available in this section.

- **Refresh** - The **Refresh** button on the top left of the **Assigned Tenants** list can be used to refresh the list.
- **Edit** - The **Edit** button on the top left of the screen can be used to edit the user. For more information see [Edit a User](#).
- **Delete** - The **Delete** button on the top left of the screen can be used to delete the user.
- **Search field** - The **Search** field can be found on the top right of the **Assigned Tenants** list. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.

When clicking on a tenant in the list, the detail page for the tenant will be opened.



Add a User

USERNAME *

SURNAME

PASSWORD *

E-MAIL *

PICTURE

SITE ADMINISTRATOR ☐

TELEPHONE

COMPANY

DEPARTMENT

OFFICE

POSITION

The following options are available in the **Add User** dialog:

- **USERNAME:** Enter the username of the user. This field is mandatory.
- **SURNAME:** Enter the surname of the user.
- **PASSWORD:** Enter the password for the user. The password will be encrypted. In order to view the password in a not encrypted form, click on the eye button at the left side of the password field. While entering the password, the password will be measured for its security. The current security level of the password will be shown as a color-coded beam right below the field. When the beam is filled completely and has turned from red to green the password is considered to be save. A password is considered to be save if it contains at least 11 characters and consists of random numbers, special characters, and upper and lowercase letters. The password field is mandatory.
- **E-MAIL:** Enter the e-mail of the user. This field is mandatory.
- **PICTURE:** A picture for the user can be uploaded by clicking the **Image** button and opening an image from the browser (the following file formats are supported: .gif, .jpg, .jpeg, and .png).
- **SITE ADMINISTRATOR:** The checkbox is used to determine if the user is a site administrator.
- **TELEPHONE:** Enter the phone number of the user.
- **COMPANY:** Enter the company of the user.
- **DEPARTMENT:** Enter the department of the user.
- **OFFICE:** Enter the office of the user.



- **POSITION:** Enter the position of the user.

Edit a User

USERNAME *
example.user

SURNAME
User

NEW PASSWORD
[toggle icon]

E-MAIL *
example.user@raynet.de

PICTURE
[silhouette icon] SITE ADMINISTRATOR ☒

TELEPHONE
[empty field]

COMPANY
[empty field]

DEPARTMENT
[empty field]

OFFICE
[empty field]

POSITION
[empty field]

The following options are available in the **Add User** dialog:

- **USERNAME:** This field contains the username of the user. This field is mandatory.
- **SURNAME:** This field can contain the surname of the user.
- **NEW PASSWORD:** A new password for the user can be entered here. The password will be encrypted. In order to view the password in a not encrypted form, click on the eye button at the left side of the password field. While entering the password, the password will be measured for its security. The current security level of the password will be shown as a color-coded beam right below the field. When the beam is filled completely and has turned from red to green it is considered to be save. A password is considered to be save if it contains at least 11 characters and consists of random numbers, special characters, and upper and lowercase letters.
- **E-MAIL:** This field contains the e-mail of the user. This field is mandatory.
- **PICTURE:** A picture that will be used for the user can be uploaded by clicking the **Image** button and opening an image from the browser (the following file formats are supported: .gif, .jpg, .jpeg, and .png).
- **SITE ADMINISTRATOR:** The checkbox is used to determine if the user is a site administrator.
- **TELEPHONE:** This field can contain a phone number of the user.



- **COMPANY:** This field can contain the company of the user.
- **DEPARTMENT:** This field can contain the department of the user.
- **OFFICE:** This field can contain the office of the user.
- **POSITION:** This field can contain the position of the user.

Tenants

RayManageSoft Unified Endpoint Manager is able to manage multiple tenants located on different storages hosted by different storage providers. This category contains a list of the tenants that are currently part of the RayManageSoft Unified Endpoint Manager instance.

Tenant name	Database name	Active
Default	RMSC_Default	✓
tests	RMSC_tests	✓
test123	RMSC_test123	✓
testAWS	RMSC_testAWS	✓

The following options are available in this category:

- **Refresh** - The **Refresh** button on the top left of the screen can be used to refresh the view.
- **Add** - The **Add** button on the top left of the screen can be used to add a tenant. For more information see [Add a Tenant](#).
- **Edit** - The **Edit** button on the top left of the screen can be used to edit a tenant if one tenant in the list has been selected. For more information see [Edit a Tenant](#).
- **Activate** - The **Activate** button on the top left of the screen can be used to activate a tenant if a deactivated tenant in the list has been selected.
- **Deactivate** - The **Deactivate** button on the top left of the screen can be used to deactivate a tenant if an active tenant in the list has been selected.
- **Search field** - The **Search** field can be found on the top right of the screen. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.

If clicking on a specific tenant, the **Tenant Details** for the tenant will be opened.

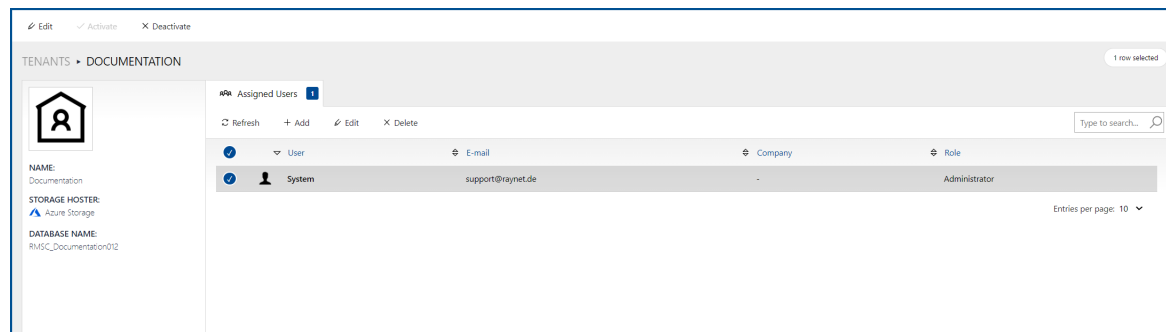


Tenant Details

The **Tenant Details** are divided into two different areas. The first area on the left side contains general information about the tenant. This includes the name of the tenant, the storage hoster, and the name of the database.

The following options are available for the tenant overall:

- **Edit** - The **Edit** button on the top left of the screen can be used to edit the tenant. For more information see [Edit a Tenant](#).
- **Activate** - The **Activate** button on the top left of the screen can be used to activate the tenant if the tenant is deactivated.
- **Deactivate** - The **Deactivate** button on the top left of the screen can be used to deactivate the tenant if the tenant is active.



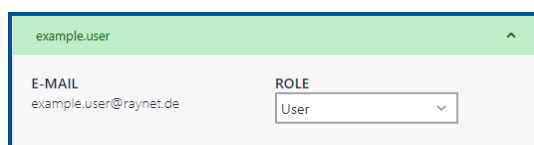
The second area on the right side contains the **Assigned Users** tab. There the list of users that are assigned to the tenant can be found. In the tab header, the number of users assigned to the tenant is shown. For the **Assigned Users** tab, the following options are available:

- **Refresh** - The **Refresh** button on the top left of the list can be used to refresh the view.
- **Add** - The **Add** button on the top left of the list can be used to add a tenant.



Add an existing user to the users assigned from the tenant. A list of available users will automatically open when clicking into the field. By entering letters into the field, the list can be shortened.

- **Edit** - The **Edit** button on the top left of the list can be used to edit the assignment of a user if one user in the list has been selected.



Select the role (either **User** or **Administrator**) for the user.



- **Delete** - The **Delete** button on the top left of the list can be used to delete a selected user from the **Assigned Users** list.
- **Search field** - The **Search** field can be found on the top right of the list. More information on how the search field works can be found in the [Using Sorting, Filter, and Search Options](#) section.

Add a Tenant

The **Add Tenant** dialog is divided into the following tabs:

- [General](#)
- [Details](#)
- [Storage](#)

General

In the **General** tab of the **Add Tenant** dialog the following details for the tenant are defined:

- **NAME:** Enter a name for the new tenant. This field is mandatory.
- **PICTURE:** A custom picture for the tenant can be uploaded by clicking the **Image** button and opening an image from the browser (the following file formats are supported: .gif, .jpg, .jpeg, and .png).
- **IS ACTIVE:** This checkbox defines if the tenant is active or deactivated.



- **CREATE DATABASE:** If this checkbox is checked, a database for the new tenant will be created automatically when the tenant is created. If this checkbox is unchecked, a new mandatory field will appear. Enter the connection string for the database that is to be used into this field. The connection string should look like the following examples:

- In order to connect to a SQL Server instance

```
Server=myServerAddress\myInstanceName;Database=myDataBase;User  
Id=myUsername;Password=myPassword;
```

- In order to use a trusted connection

```
Server=myServerAddress;Database=myDataBase;Trusted_Connection=True;
```

Details

In the **Details** tab of the **Add Tenant** dialog the following details for the tenant are defined:

The screenshot shows the 'Add Tenant' dialog box with the 'Details' tab selected. The dialog has a title bar with a close button. Below the title bar are three tabs: 'General', 'Details' (which is underlined), and 'Storage'. The 'Details' tab contains six text input fields, each with a label above it: 'CONTACT PERSON', 'COUNTRY', 'CITY', 'ZIP CODE', 'STREET', and 'STREET NUMBER'. At the bottom of the dialog, there are two buttons: 'Add' and 'Discard'.

- **CONTACT PERSON:** Enter a contact person for the tenant.
- **COUNTRY:** Enter a country.
- **CITY:** Enter a city.
- **ZIP CODE:** Enter a zip code for the city.
- **STREET:** Enter a street.
- **STREET NUMBER:** Enter a specific street number for the street.

All information in the **Details** tab are optional.

Storage

The options in the **Storage** tab depend on the selected storage hoster. The following storage hosters are available.



- [Azure](#)
- [Amazon S3](#)
- [MinIO](#)



Azure

If **Azure** is selected as the **STORAGE HOSTER**, the following details for the tenant can be defined:

The screenshot shows a window titled "Add Tenant" with a close button (X) in the top right corner. Inside the window, there are three tabs: "General", "Details", and "Storage". The "Storage" tab is currently selected. Under the "Storage" tab, there is a section labeled "STORAGE HOSTER" with a dropdown menu showing "Azure". Below this, there are three text input fields labeled "AZURE STORAGE ENDPOINT", "AZURE ENDPOINT URL", and "AZURE TOKEN TIMEOUT". At the bottom of the window, there are two buttons: "Add" (in blue) and "Discard" (in grey).

- **AZURE STORAGE ENDPOINT:** Enter the connection string properties for the Azure Storage. It should contain the following properties divided by semicolon:
 - DefaultEndpointsProtocol=https
 - AccountName=youraccount
 - AccountKey=YourAzureAccountKey==
 - EndpointSuffix=core.windows.net
- **AZURE ENDPOINT URL:** Enter the primary endpoint property of the Azure Storage.
- **AZURE TOKEN TIMEOUT:** The time after which the token will expire.

For more information regarding the configuration of the storage for a tenant refer to the *Installation Guide* for RayManageSoft Unified Endpoint Manager.

Amazon S3

If **Amazon S3** is selected as the **STORAGE HOSTER**, the following details for the tenant can be defined:



Add Tenant

General

Details

Storage

STORAGE HOSTER *

Amazon S3

REGION *

Europe (Frankfurt)

AWS ACCESS KEY *

AWS SECRET KEY *

CUSTOM BUCKET NAME

In case of no custom name provided the tenant ID will be used.

Add

Discard

- **REGION:** This is the region that should be used to host the storage. A full list of regions can be found at: <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html>.
- **AWS ACCESS KEY:** This is the access key received during the setup of the AWS IAM user.
- **AWS SECRET KEY:** This is the secret key received during the setup of the AWS IAM user.
- **CUSTOM BUCKET NAME:** Enter a custom name for the bucket. If no custom name is provided, the tenant ID will be used.

For more information regarding the configuration of the storage for a tenant refer to the *Installation Guide* for RayManageSoft Unified Endpoint Manager.

MinIO

If **MinIO** is selected as the **STORAGE HOSTER**, the following details for the tenant can be defined:



Add Tenant [X]

General Details Storage

STORAGE HOSTER *
MinIO

MINIO ENDPOINT *
[]

MINIO ACCESS KEY *
[]

MINIO SECRET KEY *
[]

MINIO USE SSL ☒

Add Discard

- **MINIO ENDPOINT:** The endpoint of the used MinIO instance. Either as `ip:port` or `fqdn:port`.
- **MINIO ACCESS KEY:** The access key that has been configured during the setup of the MinIO instance.
- **MINIO SECRET KEY:** The secret key that has been configured during the setup of the MinIO instance.
- **MINIO USE SSL:** This checkbox defines if MinIO will use SSL.

For more information regarding the configuration of the storage for a tenant refer to the *Installation Guide* for RayManageSoft Unified Endpoint Manager.

Edit a Tenant

The **Edit Tenant** dialog is divided into the following tabs:

- [General](#)
- [Details](#)
- [Storage](#)



General

In the **General** tab of the **Edit Tenant** dialog the following details for the tenant are defined:

- **NAME:** This field contains the name of the tenant. This field is mandatory.
- **PICTURE:** A custom picture for the tenant can be uploaded by clicking the **Image** button and opening an image from the browser (the following file formats are supported: .gif, .jpg, .jpeg, and .png).
- **IS ACTIVE:** This checkbox defines if the tenant is active or deactivated.
- **CONNECTION STRING:** This field contains the connection string to the database the tenant is using. The connection string should look like the following examples:
 - In order to connect to a SQL Server instance
Server=myServerAddress\myInstanceName;Database=myDataBase;User
Id=myUsername;Password=myPassword;
 - In order to use a trusted connection
Server=myServerAddress;Database=myDataBase;Trusted_Connection=True;

Details

In the **Details** tab of the **Edit Tenant** dialog the following details for the tenant are defined:



Edit Tenant

General Details Storage

CONTACT PERSON

COUNTRY

CITY

ZIP CODE

STREET

STREET NUMBER

Save changes Discard

- **CONTACT PERSON:** Enter a contact person for the tenant.
- **COUNTRY:** Enter a country.
- **CITY:** Enter a city.
- **ZIP CODE:** Enter a zip code for the city.
- **STREET:** Enter a street.
- **STREET NUMBER:** Enter a specific street number for the street.

All information in the **Details** tab are optional.

Storage

The options in the **Storage** tab depend on the selected storage hoster. The following storage hosters are available.

- [Azure](#)
- [Amazon S3](#)
- [MinIO](#)



WARNING:

Raynet does not recommend to change the storage details for an existing tenant. Doing so will remove all existing packages before switching to the new storage hoster. Currently, there is no automated migration of packages implemented.



Azure

If **Azure** is selected as the **STORAGE HOSTER**, the following details for the tenant can be defined:

Edit Tenant

General Details Storage

STORAGE HOSTER *
Azure

AZURE STORAGE ENDPOINT *

AZURE ENDPOINT URL *

AZURE TOKEN TIMEOUT *

⚠ If you change the storage hoster or the storage hoster endpoints the packages will be lost.

Save changes Discard

- **AZURE STORAGE ENDPOINT:** Enter the connection string property for the Azure Storage. It should contain the following properties divided by semicolon:
 - o DefaultEndpointsProtocol=https
 - o AccountName=youraccount
 - o AccountKey=YourAzureAccountKey==
 - o EndpointSuffix=core.windows.net
- **AZURE ENDPOINT URL:** Enter the primary endpoint property of the Azure Storage.
- **AZURE TOKEN TIMEOUT:** The time after which the token will expire.

For more information regarding the configuration of the storage for a tenant refer to the *Installation Guide* for RayManageSoft Unified Endpoint Manager.

Amazon S3

If **Amazon S3** is selected as the **STORAGE HOSTER**, the following details for the tenant can be defined:



Edit Tenant

General

Details

Storage

STORAGE HOSTER *

Amazon S3

REGION *

US East (N. Virginia)

AWS ACCESS KEY *

AWS SECRET KEY *

CUSTOM BUCKET NAME

In case of no custom name provided the tenant ID will be used.

⚠ If you change the storage hoster or the storage hoster endpoints the packages will be lost.

Save changes

Discard

- **REGION:** This is the region that should be used to host the storage. A full list of regions can be found at: <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html>.
- **AWS ACCESS KEY:** This is the access key received during the setup of the AWS IAM user.
- **AWS SECRET KEY:** This is the secret key received during the setup of the AWS IAM user.
- **CUSTOM BUCKET NAME:** Enter a custom name for the bucket. If no custom name is provided, the tenant ID will be used.

For more information regarding the configuration of the storage for a tenant refer to the *Installation Guide* for RayManageSoft Unified Endpoint Manager.

MinIO

If **MinIO** is selected as the **STORAGE HOSTER**, the following details for the tenant can be defined:



Edit Tenant

General Details Storage

STORAGE HOSTER *
MinIO

MINIO ENDPOINT *

MINIO ACCESS KEY *

MINIO SECRET KEY *

MINIO USE SSL ☐

⚠ If you change the storage hoster or the storage hoster endpoints the packages will be lost.

Save changes Discard

- **MINIO ENDPOINT:** The endpoint of the used MinIO instance. Either as `ip:port` or `fqdn:port`.
- **MINIO ACCESS KEY:** The access key that has been configured during the setup of the MinIO instance.
- **MINIO SECRET KEY:** The secret key that has been configured during the setup of the MinIO instance.
- **MINIO USE SSL:** This checkbox defines if MinIO will use SSL.

For more information regarding the configuration of the storage for a tenant refer to the *Installation Guide* for RayManageSoft Unified Endpoint Manager.

System Settings

This section contains the system settings for the RayManageSoft Unified Endpoint Manager instance. Furthermore, the system log can be found here.



Edit Download log

SYSTEM SETTINGS

SYSTEM SETTINGS

LOG LEVEL: Warning

The log level determines the verbosity with which actions are logged. Note that higher levels of verbosity may have an impact on performance, size and usability of the log.

LOG STORAGE PERIOD: 3 days

The number of days log entries will be preserved.

DEFAULT STORAGE HOST: Amazon S3

The default storage hoster which will be used when creating new tenants.

BACKEND SETTINGS

BACKEND URL: rmscloud.yourcloud.corp

The URL by which the managed device backend is reachable.

BACKEND PORT: 8080

The port by which the managed device backend is reachable.

BACKEND PROTOCOL: http

The protocol by which the managed device backend is reachable.

HEALTHY - SYSTEM IS PRESENT AND CAN RESPOND.

SYSTEM LOG

```
X [May 7, 2021, 4:47:14:287 PM]: Could not parse database entry: [Raynet.RayManageSoft.Cloud.Persistence.Models.Tenant.EFTenantConfigurationEntry] for property defaultDeviceSettingsPackageId of type System.Guid
X [May 7, 2021, 4:47:14:293 PM]: Value cannot be null. (Parameter 'input')
X [May 7, 2021, 4:47:14:297 PM]: Could not parse database entry: [Raynet.RayManageSoft.Cloud.Persistence.Models.Tenant.EFTenantConfigurationEntry] for property defaultDeviceSchedulePackageId of type System.Guid
X [May 7, 2021, 4:47:14:300 PM]: Value cannot be null. (Parameter 'input')
X [May 7, 2021, 4:51:11:150 PM]: Received a request from a managed device without a valid tenant id. Returning Bad Request. Tenant Claim contains an invalid tenant id.
X [May 7, 2021, 4:56:06:060 PM]: Could not parse database entry: [Raynet.RayManageSoft.Cloud.Persistence.Models.Tenant.EFTenantConfigurationEntry] for property defaultDeviceSettingsPackageId of type System.Guid
X [May 7, 2021, 4:56:06:077 PM]: Value cannot be null. (Parameter 'input')
X [May 7, 2021, 4:56:06:080 PM]: Could not parse database entry: [Raynet.RayManageSoft.Cloud.Persistence.Models.Tenant.EFTenantConfigurationEntry] for property defaultDeviceSchedulePackageId of type System.Guid
X [May 7, 2021, 4:56:06:083 PM]: Value cannot be null. (Parameter 'input')
X [May 7, 2021, 4:56:11:137 PM]: Received a request from a managed device without a valid tenant id. Returning Bad Request. Tenant Claim contains an invalid tenant id.
```

The following options are available in this category:

- **Edit** - The **Edit** button on the top left of the screen can be used to edit the system settings. For more information see [Edit System Settings](#).
- **Download log** - The **Download log** button on the top left of the screen can be used to download the complete RayManageSoft Unified Endpoint Manager log.



Edit System Settings

The following tabs are available in the **Edit Settings** dialog:

- [General](#)
- [Storage](#)

General

In the **General** tab of the **Edit Settings** dialog, the following options are available:

The screenshot shows the 'General' tab of the 'Edit Settings' dialog. It contains the following fields and information:

- LOG LEVEL:** A dropdown menu set to 'Warn'. Below it, an information icon and text state: 'The log level determines the verbosity with which actions are logged. Note that higher levels of verbosity may have an impact on performance, size and usability of the log.'
- LOG STORAGE PERIOD:** A text input field containing '3'. Below it, an information icon and text state: 'According to the specified log storage period the log entries of the last day(s) will be preserved and are ready to be downloaded.'
- BACKEND ENDPOINT:** A text input field containing 'rmscloud.yourcloud.corp'. Below it, an information icon and text state: 'The url by which the managed device backend is reachable.'
- ENDPOINT PORT:** A text input field containing '8080'. Below it, an information icon and text state: 'The port by which the managed device backend is reachable.'
- BACKEND PROTOCOL:** A dropdown menu set to 'HTTP'. Below it, an information icon and text state: 'The protocol by which the managed device backend is reachable.'

- **LOG LEVEL:** The log level determines the verbosity with which actions are logged. The following level are available: **Finer**, **Finest**, **Info**, **Log4net_debug**, **Notice**, **Off**, **Severe**, **Trace**, **Verbose**, and **Warn**.



Note:
Higher levels of verbosity may have an impact on performance, size, and usability of the log file.

- **LOG STORAGE PERIOD:** According to the specified log storage period in days, the log entries of the last days will be preserved and are ready to be downloaded.
- **BACKEND ENDPOINT:** The URL by which the managed device backend is reachable.
- **ENDPOINT PORT:** The port by which the managed device backend is reachable.
- **BACKED PROTOCOL:** The protocol by which the managed device backend is reachable. The following protocols are available: HTTP and HTTPS.



Storage

In the **Storage** tab, the default storage hoster that will be used when a new tenant is created is defined. The settings in the **Storage** tab depend on the selected **STORAGE HOSTER**. The following **STORAGE HOSTER** are available:

- [Amazon S3](#)
- [Azure](#)
- [MinIO](#)

Amazon S3

If **Amazon S3** is selected as **STORAGE HOSTER**, the following options are available:

- **REGION:** This is the region that should be used to host the storage. A full list of regions can be found at: <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html>.
- **AWS ACCESS KEY:** This is the access key received during the setup of the AWS IAM user.
- **AWS SECRET KEY:** This is the secret key received during the setup of the AWS IAM user.

For more information regarding the configuration of the storage for a tenant refer to the *Installation Guide* for RayManageSoft Unified Endpoint Manager.

Azure

If **Azure** is selected as **STORAGE HOSTER**, the following options are available:



The screenshot shows the 'Storage' tab of the configuration interface. It includes the following fields and descriptions:

- STORAGE HOSTER ***: A dropdown menu with 'Azure' selected. Description: 'The default storage hoster which will be used when creating new tenants.'
- AZURE HOST ENDPOINT ***: A text field containing 'DefaultEndpointsProtocol=https;AccountName=rmscloudtest;AccountKey=+dM'. Description: 'The Azure storage endpoint, which will be used to connect to the network storage.'
- AZURE ENDPOINT URL ***: A text field containing 'https://rmscloud.yourcloud.corp'. Description: 'The Azure endpoint url which will be used during upload.'
- AZURE TOKEN TIMEOUT ***: A text field containing '60'. Description: 'The Azure token timeout (how long an upload token is valid).'

- **AZURE STORAGE ENDPOINT:** Enter the connection string property for the Azure Storage.
- **AZURE ENDPOINT URL:** Enter the primary endpoint property of the Azure Storage.
- **AZURE TOKEN TIMEOUT:** The number for the token timeout.

For more information regarding the configuration of the storage for a tenant refer to the *Installation Guide* for RayManageSoft Unified Endpoint Manager.

MinIO

If **MinIO** is selected as **STORAGE HOSTER**, the following options are available:

The screenshot shows the 'Storage' tab of the configuration interface with 'MinIO' selected as the storage hoster. It includes the following fields and descriptions:

- STORAGE HOSTER ***: A dropdown menu with 'MinIO' selected. Description: 'The default storage hoster which will be used when creating new tenants.'
- MINIO ENDPOINT ***: An empty text field.
- MINIO ACCESS KEY ***: An empty text field.
- MINIO SECRET KEY ***: An empty text field.
- MINIO USE SSL**: A checkbox that is checked.

- **MINIO ENDPOINT:** The endpoint of the used MinIO instance. Either as `ip:port` or `fqdn:port`.
- **MINIO ACCESS KEY:** The access key that has been configured during the setup of the MinIO instance.
- **MINIO SECRET KEY:** The secret key that has been configured during the setup of the MinIO instance.
- **MINIO USE SSL:** This checkbox defines if MinIO will use SSL.



For more information regarding the configuration of the storage for a tenant refer to the *Installation Guide* for RayManageSoft Unified Endpoint Manager.



Using Sorting, Filter, and Search Options

The following chapter describes the different ways of sorting and filtering that are available in RayManageSoft Unified Endpoint Manager. Furthermore, the functionality of the search field will be described in this chapter.

Sorting Options

It is possible to sort the tables in lists in RayManageSoft Unified Endpoint Manager by specific columns. A column that can be used for sorting a list is identified by the following icon:



If this symbol is shown in front of the title of a column, the column can be used for sorting, but is currently not actively used.

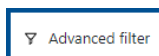
A column which is currently used for sorting is marked by one of two icons.

- ▼ : If a column is marked by this icon, the list is currently sorted according to this column from 0-9 and A-Z.
- ▲ : If a column is marked by this icon, the list is currently sorted according to this column from Z-A and 9-0.

In order to change the currently active sorting, click on the sorting icon. Switching to another column is done by clicking on the sorting icon of the target column.

Filtering Options

Depending on the selected category, different filtering options are available. The filtering options for the selected category can be found at the upper right corner.



Select the **Advanced filter** option and the different filtering options for the category will be shown. If the **Advanced filter** option is not available, there are no filtering options for this category.

The following filtering options are currently available:



- [Computer devices](#)
- [Applications](#)
- [Device details - Device logs](#)
- [Group management](#)

Computer Devices

☐	Only locked devices
Only managed devices ▼	Managed
All ▼	Operating system

The advanced filtering for **Computer Devices** contains the following options for filtering:

- [Locked devices checkbox](#)
- [Managed](#)
- [Operating systems](#)

Locked Devices Checkbox

If this checkbox is checked, it will only show those devices which are currently locked.

Managed

The **Managed** filter option can be used to filter after managed and unmanaged devices.

Only managed devices ^
Only managed devices
Only unmanaged devices
All

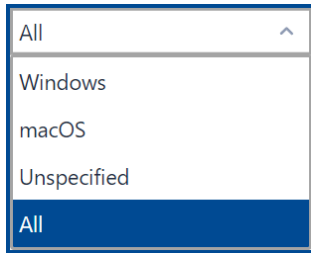
It contains the following filtering options:

- **Only managed devices:** If this option is chosen, only the devices under management by RayManageSoft Unified Endpoint Manager will be shown.
- **Only unmanaged devices:** If this option is chosen, only those devices which are not yet managed by RayManageSoft Unified Endpoint Manager will be shown.
- **All:** If this option is chosen, all devices (both managed and unmanaged) will be shown. This is the default setting.

Operating System



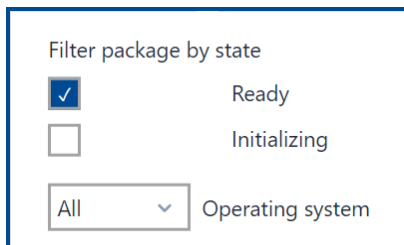
The **Operating system** filter option can be used to filter after the different OS of the devices.



It contains the following filtering options:

- **Windows:** If this option is chosen, only Windows devices will be shown.
- **macOS:** If this option is chosen, only macOS devices will be shown.
- **Unspecified:** If this option is chosen, only those devices for which the OS has not been specified will be shown.
- **All:** If this option is chosen, all devices regardless of their OS will be shown.

Applications



The advanced filtering for **Applications** contains the following options for filtering:

- [Ready](#)
- [Initializing](#)
- [Operating system](#)

Ready

If this checkbox is checked, packages that are currently in the **Ok** state will be shown, otherwise packages in the **Ok** state will not be shown.

Initializing

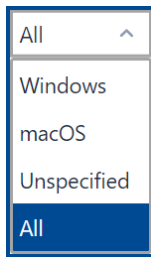
If this checkbox is checked, packages that are currently initializing will be shown, otherwise packages that are initializing will not be shown.

Operating System

The **Operating system** filter option can be used to filter after the different OS dependencies of



the applications.

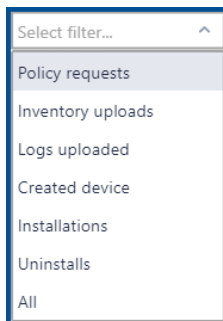


It contains the following filtering options:

- **Windows:** If this option is chosen, only Windows applications will be shown.
- **macOS:** If this option is chosen, only macOS applications will be shown.
- **Unspecified:** If this option is chosen, only those applications for which the OS has not been specified will be shown.
- **All:** If this option is chosen, all applications regardless of their defined OS will be shown.

Device Details - Device Logs

The advanced filtering for the **Device log** tab offers a dropdown box which can be used to filter the Device Logs in regard of the actions.



- **Policy requests:** If this option is selected, only logging data for policy requests will be shown.
- **Inventory uploads:** If this option is selected, only logging data for inventory uploads is shown.
- **Log uploaded:** If this options is selected, only logging data for log uploads is shown.
- **Created device:** If this option is selected, only logging data for created devices is shown.
- **Installations:** If this option is selected, only logging data for installation actions is shown.
- **Uninstalls:** If this option is selected, only logging data for uninstallation actions is shown.
- **All:** If this options is selected, all logging data for the device will be shown.



Group Management

A screenshot of the Group Management interface showing two filter controls. The first control is labeled 'Deployment relevance' and has a dropdown menu with 'All groups' selected. The second control is labeled 'Operating system' and has a dropdown menu with 'All' selected.

The advanced filtering for **Group Management** contains the following options for filtering:

- [Deployment relevance](#)
- [Operating system](#)

Deployment Relevance

The **Deployment relevance** filter option can be used to filter after groups that are relevant for deployment.

A screenshot of the 'Deployment relevance' dropdown menu. It shows three options: 'All groups' (selected), 'Deployment relevant groups', and 'All groups'.

It contains the following filtering options:

- **Deployment relevant groups:** If this option is chosen, only groups that have been flagged as deployment relevant will be shown.
- **All groups:** If this option is chosen, all groups regardless of their deployment relevance will be shown.

Operating System

The **Operating system** filter option can be used to filter after the different OS defined for the groups.

A screenshot of the 'Operating system' dropdown menu. It shows four options: 'All' (selected), 'Windows', 'macOS', and 'Unspecified'.

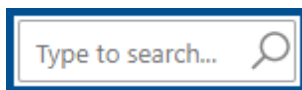
It contains the following filtering options:



- **Windows:** If this option is chosen, only Windows groups will be shown.
- **macOS:** If this option is chosen, only macOS groups will be shown.
- **Unspecified:** If this option is chosen, only those groups for which the OS has not been specified will be shown.
- **All:** If this option is chosen, all groups regardless of their defined OS will be shown.

Search Options

For many tables and lists in RayManageSoft Unified Endpoint Manager a search field is available. The search field is generally located above the upper right corner of the related list.



The search field in RayManageSoft Unified Endpoint Manager works in real time. When entering a letter or sign into the search field, RayManageSoft Unified Endpoint Manager will instantly reduce the related list or table to only contain those entries which contain the letter or sign that have been entered. If more than one letter or sign has been entered, the items in the list are an exact match of the string that has been entered in the search field. It is possible to enter more than one string if separating them by a space character.

Example:

If the string "**rea**" has been entered into the search field, all entries which contain exactly this string will be shown. Entries which contain a "**re_a**" string would not be shown. If the entry in the search field is "**re a**", both strings will be shown. Furthermore, all entries which contain "**re**" and an "**a**" somewhere would be shown.



Troubleshooting

Where to Find Log Files.

Application logs are available in the **Site-Administration / System Settings** section or in the Azure container details page (**Container instances > Details > Settings > Containers > Logs**).

One or More Pages Do Not Load or Do Not Open.

Please delete the cache of the browser that is being used to access RayManageSoft Unified Endpoint Manager and restart the browser. If the problem persists, try to contact the support representative that is specified in the RayManageSoft Unified Endpoint Manager instance.



Appendix I: Preference Settings for Managed Devices

This chapter describes the settings for the configuration of RayManageSoft Unified Endpoint Manager for an environment. The following points will be covered:

- The setup of the RayManageSoft Unified Endpoint Manager preference settings.
- The usage of managed device settings packages
 - in the Windows registry.
 - in command-line tools.
 - in packages, as registry entries, or project variables.
 - in configuration files.
- The identification of settings associated with particular RayManageSoft Unified Endpoint Manager behavior.
- Details of the individual settings.

RayManageSoft Unified Endpoint Manager Managed Device Settings

RayManageSoft Unified Endpoint Manager provides a large selection of settings which can be used to control the behavior of RayManageSoft Unified Endpoint Manager. Most of these are used for the managed devices and can either be configured on the individual managed device or can be embedded in a package in order to control the behavior of the package on all managed devices using it.

There are also settings which can be configured directly in RayManageSoft Unified Endpoint Manager. This chapter describes the settings configured on the managed devices.



Be aware:

Since each environment is unique, the examples in this manual may not suit your specific implementation. If in doubt, Raynet strongly recommends to speak with your Raynet Support representative before starting to change your settings.

Installation Defaults

When RayManageSoft Unified Endpoint Manager is installed, it configures default values for many settings. This chapter includes details about the installation defaults for all settings on the managed device.

Learning More About Managed Device Preference Settings

The remainder of this chapter contains:

- An overview of how settings are configured, evaluated, and locked.



- Details on how RayManageSoft Unified Endpoint Manager uses the Windows registry for configuring and reading settings.
- An explanation of using packaging project variables to configure settings.
- Details about settings with command-line tools.
- An introduction to the global configuration file.
- Lists of settings according to the behavior that they modify.
- An alphabetical list of settings which outlines:
 - the purpose of the setting.
 - defaults, values or ranges, and example values.
 - the methods by which the setting can be configured.
 - details applicable to each definition method relevant for the setting.

Configuration, Fixing, and Evaluation

The following section shows:

- the range of methods available for configuring settings.
- how to lock a setting to stop it from being overridden.
- the evaluation order of the various methods of configuring settings.
- the relationship between settings and environment variables.

Ways of Configuring Settings

There are different ways to configure settings. Settings can be:

- defined in the managed device settings packages that are assigned to a policy and distributed and installed using the same methods as standard packages.
- set in the Windows registry under the Computer or User hives.
- set as arguments in the RayManageSoft Unified Endpoint Manager command-line tools.
- defined as project variables in packages.
- set directly in the global configuration file allowing for the specification of the settings in a central location.

All of these methods are referenced in this chapter.

Fixing Managed Device Settings

It is possible to define fixed settings that cannot be modified by users who do not have administrator permissions.

This can be done for any RayManageSoft Unified Endpoint Manager registry setting on a managed device by creating another entry in the registry with the same name as the setting, suffixed with `Fixed` or `Fxd` and assigning the value `True` to the new entry.



Example

All packages installed by RayManageSoft Unified Endpoint Manager have to create an entry in the **Add/Remove Programs** control panel applet. First, the `AddRemove` registry entry needs to be set to `Create`, then an entry in the same location needs to be created called `AddRemoveFixed` (or `AddRemoveFxd`). The entry then needs to be set to `True`.



Be aware:

Fixed settings can be overridden by command-line options if the `CmdLineOverrides` installation setting is set to `True` in the registry. See [CmdLineOverrides](#) within the [Alphabetical Listing of Settings](#).

Evaluating Settings

RayManageSoft Unified Endpoint Manager refers to a number of locations when evaluating preference settings on a managed device. The order of precedence is as follows (highest to lowest):

1. Command-line arguments.
2. Any preference settings read from [UserAlternateRegistryHive](#).
3. User settings taken from:
`HKEY_CURRENT_USER\Software\ManageSoft Corp\ManageSoft\...`
4. Any settings read from [MachineAlternateRegistryHive](#).
5. Computer preferences, taken from one of the locations described in `[Registry]`.
6. Network preferences taken from the file on the network specified by URL or UNC in the registry setting [GlobalConfigSource](#).
7. The RayManageSoft Unified Endpoint Manager factory defaults.



Be aware:

If preferences are defined as "fixed entries" (see above for details), higher precedence settings are ignored. For example, if a setting is fixed through network preferences, then user settings, computer settings, and command-line arguments are ignored.



Be aware:

The fact that the system environment does not appear in this list is significant. Preference setting values are **not** retrieved from the system environment for the purposes of controlling product behavior or package behavior. In some cases, the system environment is queried when no other value can be determined for a project variable. Do not rely on this behavior, but instead ensure that values are set for all project variables in use.

Alternative Registry Hives

In order to enable handy registry setting evaluation, RayManageSoft Unified Endpoint Manager



uses the registry entries `UserAlternateRegistryHive` and [`MachineAlternateRegistryHive`](#). For registry testing, copy the registry content from the default `[Registry]` hive to a separate test hive and update the value of the respective alternate registry hive entry. The changes that are applied to the alternate path will have no effect on the productive set of registry settings and it is possible to switch back to them by simply setting the default values for `UserAlternateRegistryHive` and `MachineAlternateRegistryHive`. As mentioned above, the alternate hive is always evaluated with a higher precedence than the standard hive.

Preference Settings in Managed Device Settings Packages

When a managed device updates a policy, any new or updated managed device settings packages that apply to the managed device are installed. These packages modify the computer preferences set in the registry. The precedence order listed earlier applies.

If multiple managed device settings packages are included in the merged policy for a managed device, these packages are installed in the sequence in which they appear in the merged policy (`.npl`) file. Each new managed device settings package overrides the settings applied from the previous managed device settings package.

Preference Settings in Software Packages

Some preference settings can also be defined as project variables in RayManageSoft Unified Endpoint Manager software packages. These project variables can be assigned special behaviors that control whether they override other settings.

Because of these controls packages are not included in the above list, as RayManageSoft Unified Endpoint Manager must evaluate the precedence of preference settings in each package individually.

Managed Device Settings Packages

The most common method for managing managed device preferences is through the use of managed device settings packages. These settings packages identify specific preference values to be applied to managed devices. They are applicable across all supported platforms.

About Settings Packages

Settings packages are used to manage and distribute preference settings to managed devices across an enterprise.

Creating Settings Packages

It is possible to create a series of settings packages using the RayManageSoft Unified Endpoint Manager console on the administration server. The settings packages are stored on the administration server and distributed to the distribution locations for the retrieval by managed devices. Settings packages can be updated and redistributed as often as required.



Targeting Users and Computers

To target settings packages to users and computers, it is necessary to assign the settings packages to a group policy. This is done from:

- The **Devices** node in the RayManageSoft Unified Endpoint Manager console tree.
- The RayManageSoft Unified Endpoint Manager Software Management snap-in to the **Group Policy Object** editor, in the same way that software packages and schedules are assigned to policy.

When the policy is merged and the RayManageSoft Unified Endpoint Manager agent calculates the set of packages that should apply to each computer or user, it includes the settings packages in the calculation.

When each managed device performs its scheduled policy update, the managed device retrieves the appropriate settings package from the closest distribution location and installs it. The installation process sets the `HKEY_LOCAL_MACHINE` registry keys for the preferences included in the settings package.

Preference Settings in the Registry

Settings for RayManageSoft Unified Endpoint Manager on managed devices are stored in the Windows registry. While some settings are configured during the installation process and should not be altered, many others can be changed to suit the specific needs of an organization.

Where are Preference Settings Stored in the Registry?

By default, registry entries for each setting are stored as described in **Registry**.

Settings under this location affect the operation of RayManageSoft Unified Endpoint Manager for all users with accounts on the managed device. It is, however, possible to customize registry entries on a user by user basis by creating equivalent entries in the following location on each Windows managed device:

`HKEY_CURRENT_USER\Software\ManageSoft Corp\ManageSoft\`

See also the preferences `MachineAlternateRegistryHive` and `UserAlternateRegistryHive` in the [Alphabetical Listing of Preferences](#) section for a fuller description.

Values for most preference settings can be configured in the registry under a key that ends with something like

`...ManageSoft Corp\ManageSoft\<component>\CurrentVersion.`

Each of these settings is specific to the particular component. Such settings can generally also have default values for all or multiple components configured under

`...ManageSoft Corp\ManageSoft\Common.`

For example, the `MachineId` preference can be set for specific components in the following entries:



```
...\\ManageSoft Corp\\ManageSoft\\Launcher\\CurrentVersion\\MachineId
...\\ManageSoft Corp\\ManageSoft\\Selector\\CurrentVersion\\MachineId
...\\ManageSoft Corp\\ManageSoft\\Usage Agent\\CurrentVersion\\MachineId
...\\ManageSoft Corp\\ManageSoft\\Policy Client\\CurrentVersion\\MachineId
...\\ManageSoft Corp\\ManageSoft\\Schedule Agent\\CurrentVersion\\MachineId.
```

MachineId can also be set in the following location to provide a default value for any component that does not explicitly have a value configured:

```
...\\ManageSoft Corp\\ManageSoft\\Common\\MachineId.
```

How are Managed Device Registry Entries Set?

Most registry entries are automatically created during the installation of RayManageSoft Unified Endpoint Manager on the managed device (either prior to or when the RayManageSoft Unified Endpoint Manager installation agent runs for the first time on the managed device).

However, some entries can be manually configured:

- By a RayManageSoft Unified Endpoint Manager package.
- By the `mgssetup.ini` configuration file used in automatic adoption of managed devices.
- By any other mechanism that affects the registry.

The reference section at the end of this chapter lists each preference and also indicates whether the entry is automatically created during RayManageSoft Unified Endpoint Manager installation or only set manually.

How Does RMS UEM Use the Registry?

When RayManageSoft Unified Endpoint Manager performs an action on a managed device that has preferences associated with it, it checks the registry when evaluating the value of a setting. The registry can also be altered by setting values in a package. It is possible to define registry keys and values in a package. If a registry value, the key under which it is located needs to be defined first. It is possible to define new registry key and values or to recreate (override) RayManageSoft Unified Endpoint Manager registry entries.

It is also possible to retrieve a value from the registry and place it into a project variable. This offers the possibility to build a custom logic in order to determine actions based on the value in the registry.

Preference Settings in Command Line Tools

RayManageSoft Unified Endpoint Manager command-line features allow for the automation of RayManageSoft Unified Endpoint Manager related activities through scripts or batch files.

What do command-line tools do?

command-line tools allow for the direct interaction with a RayManageSoft Unified Endpoint Manager smart agent. Some of the ways to use command-line tools include:



- the creation of batch files to run behind the scenes.
- the inclusion of the command in a user logon script in order for the command to run when the user logs in.
- entering a command using the MS-DOS command-line in order to run the command immediately.



Persistent Managed Device Preference Settings

When configuring a preference setting on the installation agent command-line, the setting is saved in a RayManageSoft Unified Endpoint Manager symbol file (.sym) in the same folder as any details for the installation being installed. These settings are then used as the default next time an action occurs for the same package including packages installed using policies. This is referred to as being a *persistent* setting.

This behavior is controlled by the value in the `SaveAllUserSymbols` setting.

- If `True`, then the setting is saved.
- If `False`, the setting is used for the particular action but it is not saved.

Therefore, when configuring a setting on the command-line, consideration whether the setting should be persistent for future actions or only be used for the current action is needed. If the setting is only to be used for the current action, ensure that `SaveAllUserSymbols` is set to `False` before configuring the setting. See [SaveAllUserSymbols](#) in the [Alphabetical Listing of Preferences](#) section for more details about this setting and its configuration.



Be aware:

When configuring settings on the command-line, `SaveAllUserSymbols` must precede all other settings.

To Configure Settings Using the Command Line Tools

When using a command-line tool, settings can be configured in the command-line using command-line arguments. For some smart agents, all of the settings associated with the smart agent can be set in the command-line. For other agents only selected settings are available on the command-line.

Listing of Command Line Tools

The following command-line tools make use of RayManageSoft Unified Endpoint Manager settings as command-line arguments:

- **Adoption agent** (on computers being brought under management)
- **Application usage agent** (on managed devices)
- **Distribution agent** (on administration servers and distribution servers)
- **Installation agent** (on managed devices)
- **Inventory agent** (on managed devices)
- **Peer download agent** (on managed devices)
- **Policy agent** (on managed devices)
- **Reboot agent** (on managed devices)



- **Scheduling agent** (on managed devices)
- **Selection agent** (on managed devices)
- **Upload agent** (on managed devices)

The syntax for the different tools is as follows:

Adoption agent	ndinstlr
Application usage agent	mgsmislist
Distribution agent	nddistrb
Installation agent	ndlaunch
Inventory agent	ndtrack
Peer download agent	mgddl
Policy agent	mgspolicy
Reboot agent	reboot
Scheduling agent	ndschedag
Upload agent	ndupload

Adoption Agent Settings Configured Using the Command Line

The following settings can be configured using the adoption agent command-line:

- [AllowRebootIfServer](#) -determines whether or not a computer being brought under management should be rebooted if it is a server.
- [CheckCertificateRevocation](#) - determines whether RayManageSoft Unified Endpoint Manager checks the certificate revocation list when accepting web server signatures from an HTTPS server.
- [ForceReboot](#) - determines whether RayManageSoft Unified Endpoint Manager forces a reboot if the package being installed requires it. A forced reboot suppresses any user interaction required to close other applications that may be running.
- [ForceRebootIfLocked](#) - determines whether RayManageSoft Unified Endpoint Manager performs a forced reboot if the desktop of the user is locked. A forced reboot suppresses any user interaction required to close other applications that may be running.
- [RebootIfRequired](#) - controls whether RayManageSoft Unified Endpoint Manager reboots the managed device if the package being installed requires it and the desktop of the user is not locked.



Application Usage Agent Settings Configured Using the Command Line

The following settings can be configured using the application usage agent command-line:

- [CheckCertificateRevocation](#) - determines whether RayManageSoft Unified Endpoint Manager checks the certificate revocation list when accepting web server signatures from an HTTPS server.
- [Compress](#) ([Application Usage Agent](#)) - determines whether application usage files are compressed for the upload.
- [Disabled](#) ([Application Usage Agent](#)) - specifies whether the application usage agent is inactive on this managed device.
- [ExcludedMGSSs](#) - determines if applications are excluded from having usage data recorded.
- [ExcludedMSIs](#) - determines if MSI applications are excluded from having usage data recorded.
- [MinRunTime](#) - specifies the minimum time (in seconds) that an application must run before usage data for it will be recorded.
- [PreferenceUpdatePeriod](#) - specifies how often (in seconds) the application usage agent will refresh its settings from the registry.
- [ProcessUpdatePeriod](#) - specifies how often (in seconds) the application usage agent will check for newly started or exited applications.
- [ProductUpdatePeriod](#) - specifies how often (in seconds) the application usage agent will check for newly installed applications.
- [SessionBackupPeriod](#) - specifies how often (in seconds) the application usage agent will cache already recorded application usage data.
- [UploadPeriod](#) - specifies how often (in seconds) the application usage agent will upload recorded application usage data to the specified server.
- [UseAddRemove](#) - specifies if usage data for applications detected from **Add/Remove Programs** is recorded.
- [UseManualMapper](#) - specifies if usage data for applications detected from the Manual Mapper registry keys is recorded.
- [UseMGS](#) - specifies whether the application usage agent should monitor applications found in the RayManageSoft Unified Endpoint Manager application cache.
- [UseMSI](#) - specifies if usage data for applications that are detected in the native package format (MSI, RPM, or PKG) is recorded.
- [UserProcessesOnly](#) - specifies whether data for `SYSTEM` (or `root`) is recorded or only data



from other users.

Installation Agent Settings Configured Using the Command Line

The following settings can be configured using the installation agent command-line:

- [AddRemove](#) - determines whether installed packages create an entry in **Add/Remove Programs**.
- [AllowRebootIfLocked](#) - controls whether RayManageSoft Unified Endpoint Manager reboots the managed device if the package being installed requires it even if the machine is locked.
- [AlwaysDisplayReboot](#) - controls whether RayManageSoft Unified Endpoint Manager displays a warning to the user before performing any reboot required by a package installation (overrides `UserInteractionLevel`).
- [ApplyPolicy](#) - used on managed devices configured for peer-to-peer file sharing, in conjunction with `DownloadPolicy`, to distinguish between the *Apply a RMS UEM AppCenter Policy* and *Update Policy and Package Definitions in Peer Cache* events.
- [AutoDetectDC](#) - determines how RayManageSoft Unified Endpoint Manager selects a domain controller for client-side policy merging.
- [BrandARP](#) - provides the ability to exclude the name "RayManageSoft Unified Endpoint Manager" from the **Add/Remove** entries for installed applications.
- [CheckCatalogDigest](#) - determines whether RayManageSoft Unified Endpoint Manager performs a check on file-level MD5 digests during self-healing operations.
- [CheckCertificateRevocation](#) - determines whether RayManageSoft Unified Endpoint Manager checks the certificate revocation list when accepting web server signatures from an HTTPS server.
- [CheckFileDigest](#) - determines whether RayManageSoft Unified Endpoint Manager performs a check on file-level MD5 digests during self-healing operations.
- [CheckRegistry](#) (or [Reg on the command-line](#)) - determines if RayManageSoft Unified Endpoint Manager performs self-healing on registry keys and preference files.
- [ConfirmSharedFileRemoval](#) - determines whether RayManageSoft Unified Endpoint Manager displays a dialog when removing a file.
- [ConnectionAttempts](#) - the number of times that a **no connection is available** error can be reported while trying to connect to a particular distribution location as a file share.
- [DiskReservedKB](#) - the amount of disk space reserved on each drive.
- [DisplayAllAuthcode](#) - determines the subsequent behavior after RayManageSoft Unified



Endpoint Manager encounters an invalid signature when performing an Authenticode check.

- [EnablePolicyFailOver](#) - specifies whether a server-side policy file should be applied if a client-side policy file is unavailable.
- [ForceReboot](#) - determines whether RayManageSoft Unified Endpoint Manager forces a reboot if the package being installed requires it. A forced reboot suppresses any user interaction required to close other applications that may be running.
- [ForceRebootIfLocked](#) - determines whether RayManageSoft Unified Endpoint Manager performs a forced reboot if the machine is locked. A forced reboot suppresses any user interaction required to close other applications that may be running.
- [ForceSharedFileRemove](#) - allows for the deletion of redundant files in the Windows system folder.
- [ForceValidSignature](#) - determines whether RayManageSoft Unified Endpoint Manager prompts the user before installing a package when Authenticode signatures are valid.
- [http_proxy](#) - proxy settings for the RayManageSoft Unified Endpoint Manager installation agent.
- [IgnoreConnectionWindows](#) - specifies whether to use or ignore the download time periods specified by `ParentConnectionWindows` and `PeerConnectionWindows`.
- [InstallationStatusRefreshPeriod](#) - specifies how frequently (in seconds) RayManageSoft Unified Endpoint Manager should recreate installation events for packages that are installed, or flagged as not required.
- [InstallerARPMModify](#) - determines whether the external installer package details can be modified in **Add/Remove Programs**.
- [InstallerARPRemove](#) - determines whether external installer packages can be uninstalled using **Add/Remove Programs**.
- [LogFile](#) (**Installation Agent**) - the name of the file which is used to store the logging information.
- [LogFileOld](#) (**Installation Agent**) - name of the file which is used to store additional logging information.
- [LogFileSize](#) (**Installation Agent**) - maximum log file size.
- [LogInstallCheck](#) - specifies whether RayManageSoft Unified Endpoint Manager should recreate installation events while checking packages for installation or upgrade.
- [LogInstallFail](#) - specifies whether RayManageSoft Unified Endpoint Manager should log failed installation attempts.
- [LogInstallPass](#) - specifies whether RayManageSoft Unified Endpoint Manager should log successful installation events.
- [LogLevel](#) (**Installation Agent**) - level of logging returned by the smart-agent.



- [LogUninstallFail](#) - specifies whether RayManageSoft Unified Endpoint Manager should log failed uninstallation attempts.
- [LogUninstallPass](#) - specifies whether RayManageSoft Unified Endpoint Manager should log successful uninstallation events.
- [LowProfile](#) ([Installation Agent, Inventory Agent](#)) - the processing priority used for RayManageSoft Unified Endpoint Manager processes.
- [MinimumDCSpeed](#) - determines the minimum speed between the managed device and the domain controller that is required to apply the client-side policy.
- [MsiSourceLocation](#) - determines whether Windows Installer packages are installed from the local Windows Installer cache of the managed device or from a distribution location.
- [NetworkHighSpeed](#) ([Installation Agent](#)) - the lowest network speed that is considered to be a high-speed network connection.
- [NetworkHighUsage](#) - the maximum percentage of bandwidth to use for high-speed connections.
- [NetworkHighUsageLowerLimit](#) - the minimum `NetworkHighUsage` value that can be set for a managed device.
- [NetworkHighUsageUpperLimit](#) - the maximum `NetworkHighUsage` value that can be set for a managed device.
- [NetworkLowUsage](#) - the maximum percentage of bandwidth to use for low-speed connections.
- [NetworkLowUsageLowerLimit](#) - the minimum `NetworkLowUsage` value that can be set for a managed device.
- [NetworkLowUsageUpperLimit](#) - the maximum `NetworkLowUsage` value that can be set for a managed device.
- [NetworkMaxRate](#) ([Installation Agent](#)) - the rate at which the managed device accesses data over the network.
- [NetworkMinSpeed](#) ([Installation Agent](#)) - the minimum network speed at which RayManageSoft Unified Endpoint Manager will install or update a package.
- [NetworkRetries](#) - the number of times failed network operations are retried before an alternative distribution location is attempted.
- [NetworkSense](#) ([Installation Agent](#)) - determines whether network checks are bypassed.
- [NetworkTimeout](#) ([Installation Agent](#)) - the number of seconds of inactivity before a network operation will time out.
- [NoStage](#) - determines whether files are downloaded directly to their destination folder or to a staging area.



- [PolicyServerPriority](#) - specifies the priority to apply to the distribution location identified by the `PolicyServerURL` (internal-only) preference.
- [PromptOnCOMRegFailures](#) - determines whether RayManageSoft Unified Endpoint Manager prompts the user if it fails to register a COM server.
- [PromptOnInstallCompletion](#) - when the `UserInteractionLevel` (installation agent) is set to `Full`, this preference determines whether RayManageSoft Unified Endpoint Manager informs the user when the package installation is complete.
- [PromptOnUninstallCompletion](#) - when the `UserInteractionLevel` (installation agent) is set to `Full`, this preference determines whether RayManageSoft Unified Endpoint Manager informs the user when package uninstallation is complete.
- [PropagatePkgChanged](#) - reinstalls the base package if the prerequisite package has changed for Third party installer packages.
- [PublicAppAccess](#) - determines the access of RayManageSoft Unified Endpoint Manager to the **Common** folders on Windows.
- [QuietUntilUpdate](#) - controls whether the RayManageSoft Unified Endpoint Manager user interface is hidden if no user interaction is necessary.
- [RebootCmdLine](#) - used on the managed device to reboot from the command-line.
- [RebootIfRequired](#) - sets the default response to dialogs that prompt the user to allow a reboot.
- [ReInstallRequiresVersionChange](#) - determines when packages will be upgraded, downgraded, or reinstalled, based on the type of changes made to the package.
- [RenotifyTimeout](#) - the number of seconds that the installation agent waits before once again showing a user any hidden dialogs that have not yet timed out.
- [SaveAllUserSymbols](#) - determines whether RayManageSoft Unified Endpoint Manager retains installation preferences set by a top-level or prerequisite package.
- [SelfHeal](#) - determines whether self-healing should take place for an individual package.
- [StageInactivePackages](#) - determines whether the managed device can download files for packages within policies that have future activation times.
- [StrictInstall](#) - if `True`, the policy agent returns a non-zero exit code if any package fails to install.
- [SupplyWorstCaseReturnValue](#) - determines whether RayManageSoft Unified Endpoint Manager returns an error only when an installation agent operation fails or also when upgrades or self-heal operations fail.
- [UITimeoutWait](#) - the number of seconds that the installation agent dialogs display before timing out.
- [UseTrustDatabase](#) - determines whether the installation agent takes account of the



distribution location from which files are collected when determining whether a package is to be installed.

- [VerifyCatalogSigned](#) - determines whether Authenticode digital signatures are checked in the RayManageSoft Unified Endpoint Manager catalog (.ndc) file before packages are installed.
- [VerifyFilesSigned](#) - determines whether executable files downloaded by RayManageSoft Unified Endpoint Manager are checked for a valid Authenticode digital signature before being installed.
- [VirusScan](#) - determines whether files downloaded by RayManageSoft Unified Endpoint Manager are scanned for viruses before installation.
- [VirusScanCommand](#) - determines how files downloaded by RayManageSoft Unified Endpoint Manager are scanned for viruses before installation.

Inventory Agent Settings Configured Using the Command Line

The following settings can be configured using the inventory agent command-line:

- [CheckCertificateRevocation](#) - determines whether RayManageSoft Unified Endpoint Manager checks the certificate revocation list when accepting web server signatures from an HTTPS server.
- [Compress](#) ([inventory agent](#)) - determines whether inventory files are compressed for the upload.
- [Difference](#) - determines whether differential inventories are performed on the managed device.
- [ExcludeDirectory](#) - folders that are to be excluded from the inventory.
- [ExcludeExtension](#) - file extensions that are to be excluded from the inventory.
- [ExcludeFile](#) - files that are to be excluded from the inventory.
- [ExcludeMD5](#) - files matching this MD5 checksum are to be excluded from the inventory.
- [ExcludePermissionsMask](#) - files that match the defined octal mask will be excluded from the scan.
- [GenerateMD5](#) - generate an MD5 for every file being tracked.
- [GenerationMax](#) - the number of differential inventories being performed between full inventories.
- [Hardware](#) - determines whether to track hardware (in the machine context).
- [IncludeDirectory](#) - folders to be included in the inventory.



- [IncludeExtension](#) - file extensions to be included in the inventory.
- [IncludeFile](#) - files to be included in inventory.
- [IncludeMD5](#) - files matching this MD5 checksum are to be included in the inventory.
- [IncludeRegistryKey](#) - registry keys or values to be included in the inventory.
- [IncrementalDiff](#) - determines what differences RayManageSoft Unified Endpoint Manager will collect if differential inventories are performed.
- [InventoryDirectory](#) - determines a custom directory used for the storage of inventory data.
- [InventoryFile](#) - identifies the name of a local copy of the inventory file.
- [IncludePermissionsMask](#) - files that match the defined octal mask will be included into the inventory.
- [InventoryScriptsDir](#) - the location of scripts to be run immediately before inventory data is uploaded through the distribution hierarchy.
- [LowProfile](#) ([Installation Agent](#), [Inventory Agent](#)) - the processing priority used for RayManageSoft Unified Endpoint Manager processes.
- [MachineInventoryDirectory](#) - the location for machine inventories.
- [MachineZeroTouchDirectory](#) - the location for machine inventories in case of a remote call.
- [ManageSoftPackages](#) - determines the installed software packages.
- [MinInventoryInterval](#) - specifies the minimum interval (in hours) between the collection of inventories.
- [MSI](#) - specifies if MSI package information is being added to the inventories.
- [NetworkSense](#) ([Inventory Agent](#)) - determines whether network checks are bypassed.
- [PlatformSpecificPackages](#) - specifies whether the information about non-Windows, platform-specific packages is included in the inventory.
- [RunInventoryScripts](#) - specifies whether or not to run inventory scripts after gathering inventory data.
- [SMBIOSCmdLine](#) - specifies a command-line for non-WMI hardware inventory collection.
- [VersionInfo](#) - determines whether file version header information is included in inventory.

Peer Download Agent Settings Configured Using the Command Line

The following settings can be configured using the peer download agent command-line (only



when using it in debugging mode (-debug)):

- [CacheDir](#) - the location of the peer cache.
- [CatalogName](#) - the name of the peer downloads file (located in the parent of the `CacheDir` directory) listing files required by the peer cache.
- [CheckpointSeconds](#) - the frequency (in seconds) with which the peer downloads file is written to disk.
- [DiskAveragingTime](#) - the time period used to smooth the disk I/O traffic estimate. Used in conjunction with `DiskMaxRate`.
- [DiskMaxRate](#) - the maximum allowable averaged rate (in bytes per second) of all reads from and writes to disks caused by peer-to-peer file sharing. Used in conjunction with `DiskAveragingTime`.
- [GCDiskSlice](#) - the maximum percentage of `DiskMaxRate` that can be used for peer cache cleanup operations.
- [GCMaxInterval](#) - the maximum number of minutes the peer download agent should pause between examining files in the peer cache as part of cleanup operations.
- [GCMinInterval](#) - the minimum number of minutes the peer download agent should pause between examining files in the peer cache as part of cleanup operations.
- [GCPeriod](#) - the time period (in hours) over which peer cache cleanup operations are conducted.
- [MinFreeDisk](#) - the amount of disk space (in MB) that must be free for the peer download agent to download files to the peer cache.
- [PeerAveragingTime](#) - the time period to use to smooth the peer file sharing traffic estimate. Used in conjunction with `PeerMaxRate`.
- [PeerListenQueue](#) - the number of connection requests to queue before refusing additional connections.
- [PeerMaxRate](#) - the maximum allowable averaged rate (in bytes per second) of file transfers between peer managed devices. Used in conjunction with `PeerAveragingTime`.
- [PeerPullPort](#) - the TCP port on which file transfers from managed devices can be received.
- [PeerPush](#) - specifies whether peer managed devices can immediately transfer (push) requested files (`True`) or whether they must wait for a request.
- [PeerSearchDuration](#) - the time period during which to search for a file from peer managed devices.
- [PeerSearchPort](#) - the UDP port on which file transfer requests are broadcast.
- [PeerTransferLimit](#) - the number of simultaneous peer-to-peer search and file transfer



operations allowed.

- [PipeName](#) ([Peer Download Agent](#)) - the name of the pipe used to communicate with the peer download agent.
- [SearchFrequency](#) - the number of seconds between issuing peer-to-peer file sharing requests.
- [SearchMaxOffer](#) - the maximum number of offers of a file from peer managed devices to accept before terminating the search.
- [SearchMinimum](#) - the minimum number of search requests to issue for a file being sought from peer managed devices.
- [SearchRetry](#) - the number of seconds to wait after a failed file search attempt before reissuing the request.
- [UnusedFilePersistence](#) - specifies how long (in minutes) to wait after receiving the first request from the installation agent before starting to look for and delete unused files.
- [UnusedFileUptime](#) - files in the peer cache that have not been accessed within this number of seconds are removed during cleanup operations.
- [WANAveragingTime](#) - the time period to use to smooth the estimate of traffic transferred between the managed device and a distribution server across a wide area network. Used in conjunction with `WANMaxRate`.
- [WANMaxRate](#) - the maximum allowable averaged rate (in bytes per second) of file transfers between managed devices and a distribution server across a wide area network. Used in conjunction with `WANAveragingTime`.
- [WANProgressInterval](#) - the frequency (in seconds) with which to update peer managed devices with progress about file downloads from a distribution server.
- [WANRetryInterval](#) - the length of time (in seconds) after a failed WAN download to retry the download.
- [WANSearchCurrency](#) - the length of time of how recently (in seconds) a peer search for a file must have occurred before the file should be downloaded from the closest distribution server.
- [WANTimeout](#) - the time (in seconds) after which to abort stalled transfers of files from distribution servers.
- [WANTransferLimit](#) - the maximum number of managed devices that may simultaneously download from a distribution location.



Policy Agent Settings Configured Using the Command Line

The following settings can be configured using the policy agent command-line. It is also possible to configure any installation agent settings that can be configured on the command-line using the policy agent command-line:

- [BootstrappedPolicy](#) - the location of the policy to be applied to managed devices that do not use a policy attached to Active Directory domains.

Reboot Agent Settings Configured Using the Command Line

While the reboot agent is typically called by the installation agent, the following settings can be configured individually on the reboot agent command-line:

- [RebootContinueAfterCmdFailure](#) - specifies whether or not to continue with rebooting a managed device if execution of a prereboot command returns a non-zero exit code.
- [RebootPostCommand](#) - a command to run immediately after a managed device is rebooted.
- [RebootPreCommand](#) - a command to run immediately before a managed device is rebooted.
- [RebootPromptCycles](#) - the number of times an end-user can postpone the reboot of a managed device.
- [RebootPromptUnlimited](#) - specifies if prompting to reboot will continue until the managed device has rebooted.
- [RebootPromptWait](#) - the time interval (in seconds) to wait before redisplaying the dialog that prompts the end-user to reboot.

Scheduling Agent Settings Configured Using the Command Line

The following settings can be configured using the scheduling agent command-line:

- [ApplyPolicyIfLoggedOn](#) - specifies whether or not a computer policy is applied at the scheduled time if a user is logged on.
- [CheckCertificateRevocation](#) - determines whether RayManageSoft Unified Endpoint Manager checks the certificate revocation list when accepting web server signatures from an HTTPS server.
- [DisablePeriod](#) - determines the number of seconds for which RayManageSoft Unified Endpoint Manager user schedules remain disabled when the end-user disables them in the



schedule agent of the managed device.

- [EventNetType](#) - determines the type of network connections that are required to start events with an **OnConnect** trigger.
- [HideMachineUI](#) - determines if the user interface is being displayed when applying a machine policy.
- [NativeScheduler](#) - determines whether the Microsoft Task Scheduler or RayManageSoft Unified Endpoint Manager Task Scheduler is in use.
- [ndsensNetType](#) - determines what type of network connections are monitored.
- [RetryPolicy](#) - determines whether RayManageSoft Unified Endpoint Manager will attempt to retrieve RayManageSoft Unified Endpoint Manager policy when the managed device boots if no computer schedule exists on the managed device.
- [RetryPolicyCommand](#) - the command used to retrieve policy if `RetryPolicy` is set to `True`.

Selection Agent Settings Configured Using the Command Line

The following settings can be configured using the selection agent command-line:

- [ApplicationInstallCommand](#) - a template command-line to be used to install an application package through the RayManageSoft Unified Endpoint Manager package selection agent.
- [ApplicationUninstallCommand](#) - a template command-line to be used to uninstall an application package through the RayManageSoft Unified Endpoint Manager package selection agent.
- [ApplicationVerifyCommand](#) - a template command-line to be used to verify / repair an application package through the RayManageSoft Unified Endpoint Manager package selection agent.
- [CheckCertificateRevocation](#) - determines whether RayManageSoft Unified Endpoint Manager checks the certificate revocation list when accepting web server signatures from an HTTPS server.
- [ConfigFile](#) - the name of the system copy of the configuration file used by the selection agent.
- [ConfigFileDefault](#) - the name of the default configuration file to use when other settings fail.
- [Locale](#) - the locale to use for the selection agent localization.
- [LocaleDefault](#) - the locale to use in the absence of other settings.
- [RefreshPeriod](#) - the number of minutes between the automatic refresh of data held by the



package selection agent.



Upload Agent Settings Configured Using the Command Line

The following settings can be configured using the upload agent command-line:

- [CheckCertificateRevocation](#) - determines whether RayManageSoft Unified Endpoint Manager checks the certificate revocation list when accepting web server signatures from an HTTPS server.
- [NetworkHighSpeed](#) ([Upload Agent](#)) - the lowest network speed that is considered to be a high-speed network connection.
- [NetworkMaxRate](#) ([Upload Agent](#)) - the rate at which the managed device accesses data over the network.
- [NetworkMinSpeed](#) ([Upload Agent](#)) - the minimum network speed at which RayManageSoft Unified Endpoint Manager will initiate a check for updates.
- [NetworkSense](#) ([Upload Agent](#)) - determines whether network checks are bypassed.
- [NetworkTimeout](#) ([Upload Agent](#)) - determines the length of time of inactivity after which a network operation will time out.

Preference Settings in the Global Configuration File

The RayManageSoft Unified Endpoint Manager global configuration file can be used to configure preference settings in a central location.

What is the Global Configuration File?

The global configuration file can be any `.ini` file and it can be configured to apply to RayManageSoft Unified Endpoint Manager on all managed devices. Its location is specified by the `GlobalConfigSource` setting in:

```
[Registry]\ManageSoft\Launcher\CurrentVersion.
```

Where Can this File Be Kept?

The configuration file can be stored anywhere. It can be located in a local network or the corporate intranet.

The value can be a URL (`http://...`) or a UNC path such as `\\server\share\`.



Be aware:

Ensure that:

- all URL paths use forward slashes //



Example: `http://myserver/mypath/mgsconfig.ini`

- all UNC paths use backward slashes `\\`

Example: `\\my server\mypath\mgsconfig.ini`

Preferences set in the `config` file cannot be:

- Set as project variables because they are processed when the installation agent is first initialized, before any package files are read.
- Set on the command-line as they are intended to be under administrative, not user, control.

Why Configure Settings Using the Global Configuration File

A direct configuration in the configuration file allows to specify the settings under which the RayManageSoft Unified Endpoint Manager installation agent runs in a central location.

Typically, RayManageSoft Unified Endpoint Manager administrators make use of the more intuitive Active Directory and Group Policy to achieve the same result (see

[MachineAlternateRegistryHive](#) of the [Alphabetical Listing of Preference Settings for Managed Devices](#) chapter).

Raynet GmbH recommends to use this `GlobalConfigSource` functionality only on computers that do not interact with Active Directory environments. Depending on the number of managed devices referencing this file and how often each one does so, the load on the server may be an issue.

Is It Possible to Configure Any Preference Settings in the Configuration File?

It is possible to configure all settings that are normally read from:

`[Registry]\ManageSoft\Launcher\CurrentVersion.`

How to Configure Settings in the Global Configuration File

The file is in the standard Windows `.ini` file format and can be edited with any text editor. For example, WordPad.

Any settings configured in this file are set in the format: `name=value`

Each name/value is configured inside a section named (in square brackets) for the agent being configured, such as `[Launcher]`.

Example

```
[Launcher]
ForceValidSignature=True
ForceValidSignatureFixed=True
VerifyCatalogSigned=True
VerifyCatalogSignedFixed=True
```

RayManageSoft Unified Endpoint Manager refers to a number of locations when evaluating the precedence of preference settings on a managed device. The order of the settings is as follows (highest to lowest):



1. command-line arguments.
2. Any settings read from the *UserAlternateRegistryHive*.
3. User preferences, taken from:
HKEY_CURRENT_USER\Software\ManageSoft Corp\ManageSoft\...
4. Any settings read from [MachineAlternateRegistryHive](#).
5. Computer settings, taken from:
[Registry]\ManageSoft\...
6. Network settings taken from the file on the network specified by URL or UNC in the registry setting [GlobalConfigSource](#).
7. RayManageSoft Unified Endpoint Manager factory defaults.

Settings That Can Be Configured in the Global Configuration File

The following settings can be configured using the global configuration file:

- [AddRemove](#) - determines whether installed packages create an entry in **Add/Remove Programs**.
- [AllowedGroups](#) - specifies if the membership of a user is checked.
- [AllowPeerToPeer](#) - specifies whether or not managed devices can obtain downloaded files from other managed devices on the same LAN.
- [AllowRebootIfLocked](#) - controls whether RayManageSoft Unified Endpoint Manager reboots the managed device if the package being installed requires it even if the machine is locked.
- [AllowTimeoutIfLocked](#) - controls whether the time interval for prompting the end-user commences immediately if the desktop is locked or commences when the desktop is unlocked.
- [CheckCatalogDigest](#) - determines whether RayManageSoft Unified Endpoint Manager performs a check on package-level MD5 digests during self-heal operations.
- [CheckCertificateRevocation](#) - determines whether RayManageSoft Unified Endpoint Manager checks the certificate revocation list when accepting web server signatures from an HTTPS server.
- [CheckFileDigest](#) - determines whether RayManageSoft Unified Endpoint Manager performs a check on file-level MD5 digests during self-heal operations.
- [CheckRegistry](#) (or [Reg on command-line](#)) - determines if RayManageSoft Unified Endpoint Manager performs self-healing on registry keys and configuration files.
- [CmdLineOverrides](#) - determines whether options set on the command-line override fixed settings in the registry or network configuration files.
- [ConfirmSharedFileRemoval](#) - determines whether RayManageSoft Unified Endpoint Manager displays a dialog when removing a file.



- [ConnectionAttempts](#) - the number of times that a **no connection is available** error can be reported while trying to connect to a particular distribution location as a file share.
- [DisplayAllAuthcode](#) - determines the subsequent behavior after RayManageSoft Unified Endpoint Manager encounters an invalid signature when performing an Authenticode check.
- [EnablePolicyFailOver](#) - determines if a server-side policy file is used if no client-side policy file can be accessed.
- [ForceReboot](#) - determines whether RayManageSoft Unified Endpoint Manager forces a reboot if the package being installed requires it. A forced reboot suppresses any user interaction required to close other applications that may be running.
- [ForceRebootIfLocked](#) - determines whether RayManageSoft Unified Endpoint Manager performs a forced reboot if the machine is locked. A forced reboot suppresses any user interaction required to close other applications that may be running.
- [ForceSharedFileRemove](#) - allows for the deletion of redundant files in the Windows system folder.
- [ForceValidSignature](#) - determines whether RayManageSoft Unified Endpoint Manager prompts the user before installing a package when the Authenticode signatures are valid.
- [GlobalConfigSource](#) - identifies a URL that contains installation settings.
- [http_proxy](#) - contains the proxy settings for the RayManageSoft Unified Endpoint Manager installation agent.
- [InstallationStatusRefreshPeriod](#) - specifies how frequently (in seconds) RayManageSoft Unified Endpoint Manager recreates installation events for packages that are installed or flagged as not required.
- [InstallerARPModify](#) - determines whether external installer package details can be modified in **Add/Remove Programs**.
- [InstallerARPRemove](#) - determines whether external installer packages can be uninstalled using **Add/Remove Programs**.
- [LogFile \(Installation Agent\)](#) - specifies the name of the file used to store the logging information.
- [LogFileOld \(Installation Agent\)](#) - specifies the name of the file used to store additional logging information.
- [LogFileSize \(Installation Agent\)](#) - specifies the maximum size of the log file.
- [LogInstallCheck](#) - specifies whether RayManageSoft Unified Endpoint Manager should recreate installation events while checking packages for an installation or upgrade.
- [LogInstallFail](#) - specifies whether RayManageSoft Unified Endpoint Manager should log failed installation attempts.
- [LogInstallPass](#) - specifies whether RayManageSoft Unified Endpoint Manager should log



successful installation attempts.

- [LogLevel](#) ([Installation Agent](#)) - specifies the level of logging returned by the smart agent.
- [LogUninstallFail](#) - specifies whether RayManageSoft Unified Endpoint Manager should log failed uninstallation attempts.
- [LogUninstallPass](#) - specifies whether RayManageSoft Unified Endpoint Manager should log successful uninstallation events.
- [LowProfile](#) ([Installation Agent](#), [Inventory Agent](#)) - specifies the processing priority used for RayManageSoft Unified Endpoint Manager processes.
- [MsiReinstallFeatures](#) - specifies the MSI components to be installed (equivalent to the MSI property REINSTALL).
- [MsiReinstallModeLevel](#) - identifies what will be reinstalled (equivalent to the MSI property REINSTALLMODE).
- [MsiRepair](#) - determines if MSI repair operations are performed at the same time as RayManageSoft Unified Endpoint Manager self-healing operations.
- [MsiRepairLevel](#) - identifies what will be repaired (equivalent to the MSI property REINSTALLMODE).
- [MsiSourceLocation](#) - determines whether Windows Installer packages are installed from the local Windows Installer cache of the managed device or from a distribution location.
- [MsiUILevel](#) - determines the user interaction level for MSI (equivalent to the /q option in the msexec.exe command-line).
- [MsiUninstallArgs](#) - defines arguments to include in the MSI command-line for uninstall operations.
- [NetworkHighSpeed](#) ([Installation Agent](#)) - specifies the lowest network speed to consider to be a high-speed network connection.
- [NetworkHighUsage](#) - specifies the maximum bandwidth for high-speed connections.
- [NetworkHighUsageLowerLimit](#) - specifies the minimum NetworkHighUsage value that can be set for a managed device.
- [NetworkHighUsageUpperLimit](#) - specifies the maximum NetworkHighUsage value that can be set for a managed device.
- [NetworkLowUsage](#) - specifies the maximum bandwidth for low-speed connections.
- [NetworkLowUsageLowerLimit](#) - specifies the minimum NetworkLowUsage value that can be set for a managed device.
- [NetworkLowUsageUpperLimit](#) - specifies the minimum NetworkLowUsage value that can be set for a managed device.
- [NetworkMaxRate](#) ([Installation Agent](#)) - specifies the rate at which the managed device



accesses data over the network.

- [NetworkMinSpeed \(Installation Agent\)](#) - specifies the minimum network speed at which RayManageSoft Unified Endpoint Manager will install or update a package.
- [NetworkRetries](#) - specifies the number of times that failed network operations are retried before an alternative distribution location is attempted.
- [NetworkSense \(Installation Agent\)](#) - determines whether network checks are bypassed.
- [NetworkTimeout \(InstallationAgent\)](#) - specifies the number of seconds of inactivity before a network operation will time out.
- [NoStage](#) - determines whether files are downloaded directly to their destination folder or a staging area.
- [PolicyServerPriority](#) - specifies the priority to apply to the distribution location that is identified by the `PolicyServerURL` (internal-only) setting.
- [PromptOnCOMRegFailures](#) - determines whether the user is prompted when RayManageSoft Unified Endpoint Manager fails to register a COM server.
- [PromptOnInstallCompletion](#) - determines whether the user is informed that the installation of a package has been completed.
- [PromptOnUninstallCompletion](#) - determines whether the user is informed that the uninstallation of a package has been completed.
- [PublicAppAccess](#) - determines the access of RayManageSoft Unified Endpoint Manager to the Windows Common folders and files on Windows.
- [QuietUntilUpdate](#) - determines if the user interface of RayManageSoft Unified Endpoint Manager on a managed device is hidden until an interaction is necessary or if it is displayed.
- [RebootCmdLine](#) - used to reboot from the command-line.
- [RebootContinueAfterCmdFailure](#) - specifies whether to continue with the reboot if a prereboot command returned a non-zero exit code.
- [RebootIfRequired](#) - determines whether to reboot if RayManageSoft Unified Endpoint Manager has determined that a reboot is necessary.
- [RebootPostCommand](#) - specifies the command that is executed after rebooting a managed device using `reboot.exe`.
- [RebootPreCommand](#) - specifies the command that is executed before rebooting a managed device using `reboot.exe`.
- [RebootPromptCycles](#) - specifies the number of times an end-user can postpone the reboot of the managed device initiated by the RMS UEM AppCenter.
- [RebootPromptUnlimited](#) - specifies if prompting to reboot will continue until the managed device has rebooted.



- [RebootPromptWait](#) - specifies the time interval (in seconds) that RayManageSoft Unified Endpoint Manager has to wait before once again displaying the dialog that prompts the end-user to reboot.
- [ReinstallRequiresVersionChange](#) - determines when the RMS UEM AppCenter will upgrade, downgrade, or reinstall packages.
- [RenotifyTimeout](#) - determines the length of time in seconds that installation agent dialogs can remain hidden while waiting to time out before they are displayed to the user once more.
- [SaveAllUserSymbols](#) - determines whether RayManageSoft Unified Endpoint Manager retains the installation settings set by a top-level or prerequisite catalog.
- [SecurityPatchRebootIfRequired](#) - specifies the default response to dialogs displayed during security patch installation that prompt the user to allow a reboot.
- [SelfHeal](#) - specifies whether self-healing should occur for an individual package when RayManageSoft Unified Endpoint Manager updates machine or user policies.
- [ServiceConnectTimeout](#) - controls the amount of time that the `ndserv.exe` has in order to establish a named pipe connection with the `ndlaunch.exe`.
- [ServiceCreateTimeout](#) - controls the amount of time that the `ndlaunch.exe` has in order to establish a named pipe connection with the `ndserv.exe`.
- [StageInactivePackages](#) - used to download all application files referenced in a policy that is scheduled to be activated some time in the future.
- [StrictInstall](#) - determines if the policy agent returns a non-zero exit code if any package in the policy fails to install.
- [SupplyWorstCaseReturnValue](#) - determines whether an error is only reported when an installation agent operation fails regardless of whether the installation is successful or not.
- [TrustDatabaseFxd](#) - specifies if trusted and excluded locations can only be changed by users with administrator privileges.
- [UITimeoutWait](#) - determines the time (in seconds) that a RayManageSoft Unified Endpoint Manager installation agent dialog is being displayed before timing out and automatically selecting the default response.
- [UseTrustDatabase](#) - specifies if the distribution location from where a file is collected is taken into consideration.
- [VerifyCatalogSigned](#) - specifies if RayManageSoft Unified Endpoint Manager uses Authenticode to check the digital signature referenced in the implementation archive before installing a package.
- [VerifyFilesSigned](#) - specifies if RayManageSoft Unified Endpoint Manager checks for a valid Authenticode digital signature in executable files that it downloads before installing them.
- [VirusScan](#) - specifies if RayManageSoft Unified Endpoint Manager scans the downloaded files for viruses before installing them.



- [VirusScanCommand](#) - determines the virus scan application that is being used.

Preference Setting Listing By Behavior

Types of Behavior

The following sections describe the types of behavior that can be controlled on managed devices using preference settings. The preference settings are listed in the following groups:

- [Add/Remove Programs Options](#)
- [Application Usage Options](#)
- [Bandwidth Optimization Options](#)
- [Computer and User Information](#)
- [CPU Options](#)
- [Download Options](#)
- [File Handling Options](#)
- [Inventory Options](#)
- [Logging Options](#)
- [RayManageSoft Folder Locations](#)
- [MSI Package Options](#)
- [Network Speed and Connection Options](#)
- [Package-level Filtering Options](#)
- [Package RMS UEM AppCenter Options](#)
- [Policy Merge Options](#)
- [Preference Management Options](#)
- [Prerequisite Package Options](#)
- [Reboot Options](#)
- [Remote Execution Options](#)
- [Scheduling Options](#)
- [Security Options](#)
- [Self-heal Options](#)
- [Trusted Location Options](#)
- [Uninstall Options](#)
- [Upgrade / Downgrade Options](#)
- [Upload Options](#)
- [User Interaction Options](#)
- [Virus Scanning Options](#)
- [Windows Folder Information](#)



Add/Remove Programs Options

The following settings control how RayManageSoft Unified Endpoint Manager interacts with the **Add/Remove Programs** control panel applet during package processing:

- [AddRemove](#) - determines whether installed packages create an entry in **Add/Remove Programs**.
- [BrandARP](#) - provides the ability to exclude the name "RayManageSoft Unified Endpoint Manager" from the **Add/Remove Programs** entries for installed applications.
- [InstallerARPModify](#) - determines whether the external installer package details can be modified in **Add/Remove Programs**.
- [InstallerARPRemove](#) - determines whether external installer packages can be uninstalled using **Add/Remove Programs**.
- [UseAddRemove](#) - specifies whether the application usage agent should monitor applications found in **Add/Remove Programs**.

Application Usage Options

The following settings can be used to control the behavior of the RayManageSoft Unified Endpoint Manager application usage agent on managed devices:

- [Compress](#) ([Application Usage Agent](#)) - specifies whether application usage data files are compressed before being uploaded to the administration server.
- [Disabled](#) ([Application Usage Agent](#)) - specifies whether the application usage agent is inactive on this managed device.
- [EnableSessionLogging](#) - specifies whether session logging takes place on this managed device.
- [ExcludedMGSSs](#) - excludes applications from having usage data recorded.
- [ExcludedMSIs](#) - excludes MSI applications from having usage data recorded.
- [Manual Mapper](#) - specifies manual mappings between executable names and application names and versions.
- [ManualMapperDefaultPriority](#) - specifies the default priority for manual mappings between executable names and versions.
- [MinRunTime](#) - specifies the minimum time that an application must run for before application usage data will be recorded.
- [PreferenceUpdatePeriod](#) - specifies how often the application usage agent refreshes its settings from the registry.
- [ProcessUpdatePeriod](#) - specifies how often the application usage agent checks if new



applications are running.

- [ProductUpdatePeriod](#) - specifies how often the application usage agent refreshes its list of applications to be monitored.
- [SessionBackupPeriod](#) - specifies how often the application usage agent caches recorded data locally.
- [StartupDelay](#) - specifies the wait time between the startup of a managed device and the start of the application usage agent.
- [UploadPeriod](#) - specifies how often the usage agent should upload recorded data to the administration server.
- [UsageDirectory](#) - specifies the directory into which the application usage agent should store its recorded data.
- [UseAddRemove](#) - specifies whether the application usage agent should monitor application found in **Add/Remove Programs**.
- [UseManualMapper](#) - specifies whether the application usage agent should monitor application found in the Manual Mapper registry keys.
- [UseMGS](#) - specifies whether the application usage agent should monitor applications found in the RayManageSoft Unified Endpoint Manager application cache.
- [UseMSI](#) - specifies whether the application usage agent should monitor applications found in the native package format (MSI, RPM, or PKG).
- [UserProcessesOnly](#) - specifies whether the application usage agent should only monitor applications that are executed by a logged-in user.

Bandwidth Optimization Options

The following settings can be used to optimize the bandwidth on managed devices:

- [MinimumDCSpeed](#) - specifies the minimum network speed to the domain controller for RayManageSoft Unified Endpoint Manager to perform a client-side policy merge.
- [NetworkHighSpeed](#) ([Installation Agent](#)) - specifies the lowest network speed for a network to be considered a high-speed network connection.
- [NetworkHighSpeed](#) ([Upload Agent](#)) - specifies the lowest network speed for a network to be considered a high-speed network connection.
- [NetworkHighUsage](#) - specifies the maximum percentage of bandwidth used on a high-speed connection.
- [NetworkHighUsageLowerLimit](#) - specifies the minimum `NetworkHighUsage` value that can be set for a managed device.
- [NetworkHighUsageUpperLimit](#) - specifies the maximum `NetworkHighUsage` value that can be set for a managed device.



- [NetworkLowUsage](#) - specifies the maximum percentage of bandwidth used on a low-speed connection.
- [NetworkLowUsageLowerLimit](#) - specifies the minimum `NetworkLowUsage` value that can be set for a managed device.
- [NetworkLowUsageUpperLimit](#) - specifies the maximum `NetworkLowUsage` value that can be set for a managed device.
- [NetworkMaxRate](#) ([Installation Agent](#)) - specifies the maximum absolute bandwidth used (if other settings do not override).
- [NetworkMaxRate](#) ([Upload Agent](#)) - specifies the maximum absolute bandwidth used (if other settings do not override).
- [NetworkMinSpeed](#) ([Installation Agent](#)) - specifies the minimum speed required before RayManageSoft Unified Endpoint Manager will access the network.
- [NetworkMinSpeed](#) ([Upload Agent](#)) - specifies the minimum speed required before RayManageSoft Unified Endpoint Manager will access the network.
- [NetworkSense](#) ([Installation Agent](#)) - determines whether network checks are bypassed.
- [NetworkSense](#) ([Inventory Agent](#)) - determines whether network checks are bypassed.
- [NetworkSense](#) ([Upload Agent](#)) - determines whether network checks are bypassed.

Computer and User Information

The following settings contain information about computer and user information on the managed device. It is possible to reference these settings in package details and programmed callouts:

- [ComputerDomain](#) - the name assigned to the computer domain of the managed device.
- [ComputerDNSName](#) - the DNS name assigned to the managed device.
- [LogonServer](#) - the name of the logon server computer to which the managed device normally connects.
- [UserLogonDomain](#) - the name assigned to the domain of the user.

CPU Options

The following setting influences RayManageSoft Unified Endpoint Manager CPU usage:

- [LowProfile](#) ([Installation Agent](#), [Inventory Agent](#)) - the processing priority used for RayManageSoft Unified Endpoint Manager processes.



Download Options

The following settings influence the RayManageSoft Unified Endpoint Manager download behavior.

General Download Options

- [BootstrappedPolicy](#) - specifies the location of the policy to be applied to managed devices that do not use a policy attached to Active Directory domains.
- [CheckCertificateRevocation](#) - determines whether RayManageSoft Unified Endpoint Manager checks the certificate revocation list when accepting web server signatures from an HTTPS server.
- [HighestPriority](#) - specifies the highest upload / download priority that can be assigned to a distribution server.
- [LowestPriority](#) - specifies the lowest upload / download priority that can be assigned to a distribution server.
- [PolicyServerPriority](#) - specifies the priority to be applied to the distribution location identified by the `PolicyServerURL` setting.
- [PolicyServerURL](#) - determines the distribution location used as a source for package downloads.
- [SelectorAlgorithm](#) - contains the algorithm(s) used to determine the relative priorities for selecting the distribution server to use for uploads / downloads.
- [StageInactivePackages](#) - determines whether the managed device can download files for packages within policies that have future activation times.

Peer-to-peer File Sharing Options

The following settings can be used to control behavior of the RayManageSoft Unified Endpoint Manager peer download agent on the managed device:

- [AllowPeerToPeer](#) - defines if peer-to-peer file sharing is enabled
- [ApplyPolicy](#) - used in conjunction with `DownloadPolicy` to distinguish between the **Apply a RMS UEM AppCenter Policy** and the **Update Policy and Package Definitions in Peer Cache** events.
- [CacheDir](#) - specifies the location of the peer cache.
- [CatalogName](#) - determines the name of the peer download file that is listing the files required by the peer cache.
- [CheckpointSeconds](#) - specifies the frequency (in seconds) with which the peer download file is written to disk.
- [DiskAveragingTime](#) - used in conjunction with `DiskMaxRate`. Specifies the time period used to smooth the disk I/O traffic estimate.
- [DiskMaxRate](#) - used in conjunction with `DiskAveragingTime`. Specifies the maximum allowable averaged rate (in bytes per second) of all reads from and writes to disk caused by peer-to-peer file sharing.



- [GCDiskSlice](#) - specifies the maximum percentage of `DiskMaxRate` that can be used for peer cache cleanup operations.
- [GCMaxInterval](#) - specifies the maximum number of minutes the peer download agent should pause between examining files in the peer cache as part of cleanup operations.
- [GCMinInterval](#) - specifies the minimum number of minutes the peer download agent should pause between examining files in the peer cache as part of cleanup operations.
- [GCPeriod](#) - determines the time period (in hours) over which the peer download agent aims to view every file in the peer cache as part of the cleanup operations.
- [IgnoreConnectionWindows](#) - specifies whether to use or ignore the download time periods specified by `ParentConnectionWindows` and `PeerConnectionWindows`.
- [MinFreeDisk](#) - specifies the amount of disk space (in MB) that must be free for the peer download agent to download files to the peer cache.
- [ParentActivityTimeout](#) - specifies the period of time with no download activity, after which a **When connected to network event** is triggered in order to initiate a file download from a distribution server.
- [ParentConnectionWindows](#) - specifies the time periods during which downloads from distribution servers are permitted.
- [PeerAveragingTime](#) - used in conjunction with `PeerMaxRate`. Specifies the average time period (in minutes) used to smooth the estimation for the transfers to and from peer managed devices.
- [PeerConnectionWindows](#) - specifies the time periods during which the peer download agent can download packages from peer managed devices.
- [PeerListenQueue](#) - specifies the maximum number of connection request to queue before refusing additional connections.
- [PeerMaxRate](#) - specifies the maximum allowable rate (in bytes per second) for transfers to and from peer managed devices.
- [PeerPullPort](#) - specifies the TCP port used for peer-to-peer file fetch operations.
- [PeerPush](#) - specifies whether peer managed devices can immediately transfer requested files or if they must wait for a request.
- [PeerSearchDuration](#) - specifies the time (in seconds) the peer download agent will spend searching for files in peer managed device caches before choosing to download the file from the closest distribution server.
- [PeerSeachPort](#) - specifies the UDP port used for peer-to-peer search operations.
- [PeerTransferLimit](#) - specifies the number of simultaneous peer-to-peer search and file transfer operations allowed across all peers on the subnet.
- [PipeName](#) ([Peer Download Agent](#)) - contains the name of the operating system pipe used to communicate with the peer-to-peer download service.
- [PolicyPackageRefreshPeriod](#) - specifies the time period (in seconds) after successfully downloading package files during which the download of these files is not to be attempted again.
- [PolicyRefreshPeriod](#) - specifies the time period (in seconds) after successfully downloading a police during which the download of this policy is not to be attempted again.



- [SearchFrequency](#) - specifies the time (in tenths of seconds) between peer-to-peer file sharing requests.
- [SearchMaxOffer](#) - specifies the number of offers for a file to retrieve from peers before terminating the search.
- [SearchMinimum](#) - specifies the minimum number of requests to send for a required file.
- [SearchRetry](#) - specifies the time interval (in seconds) between requests for a required file.
- [UnusedFilePersistence](#) - specifies the time (in hours) after which files in the peer cache that have not been accessed are removed during cleanup operations.
- [UnusedFileUptime](#) - specifies the time (in minutes) after which RayManageSoft Unified Endpoint Manager will start to look for and delete unused files.
- [WANAveragingTime](#) - used in conjunction with [WANMaxRate](#). Specifies the average period of time (in minutes) used to smooth the estimate of transfers to and from a the distribution server.
- [WANMaxRate](#) - used in conjunction with [WANAveragingTime](#). Specifies the maximum allowable rate (in bytes per second) for transfers from distribution servers across all peers in this subnet.
- [WANProgressInterval](#) - specifies the frequency (in seconds) with which to send the progress announcements about file downloads from the distribution server to the peer managed devices.
- [WANRetries](#) - specifies how many times a failed WAN download is retried immediately from each distribution server at each WAN retry interval.
- [WANRetryDuration](#) - specifies how long (in minutes) to continue to allow a file to be retried for download since it was last requested by the installation agent.
- [WANRetryInterval](#) - specifies how long (in seconds) RayManageSoft Unified Endpoint Manager will retry the download after a WAN download has failed.
- [WANSearchCurrency](#) - specifies how frequently a device will ask if it peers for a file.
- [WANTimeout](#) - specifies the time (in seconds) after which to abort stalled transfers of files from the distribution server.
- [WANTransferLimit](#) - specifies the number of managed devices that can simultaneously download files from a distribution location.

Options that Affect the Actions that Occur after Download

- [ApplyLocalPolicy](#) - specifies whether to use a locally cached copy of a policy cannot be generated or downloaded.
- [NoStage](#) - specifies whether files are downloaded directly to their install location or if they are first placed in the staging area.
- [PolycypackageRefreshPeriod](#) - specifies the number of seconds after successfully downloading package files during which the download of these files should not be attempted again.
- [PolicyRefreshPeriod](#) - specifies the number of seconds after successfully downloading a



policy during which the download of these files should not be attempted again.

- [VirusScan](#) - specifies if RayManageSoft Unified Endpoint Manager scans the downloaded files for viruses before installing them.
- [VirusScanCommand](#) - determines the virus scan application that is being used.



File Handling Options

The following preferences determine file handling behavior during package processing:

- [CacheDir](#) - specifies the location to which packages are downloaded prior to the installation if peer-to-peer file sharing is enabled.
- [ConfirmSharedFileRemoval](#) - determines whether RayManageSoft Unified Endpoint Manager displays a dialog when removing a file.
- [ForceSharedFileRemove](#) - determines whether forced deletion of redundant files in the Windows system folder is allowed.
- [NoStage](#) - specifies whether files are downloaded directly to their install location or if they are first placed in the staging area.
- [PublicAppAccess](#) - determines the access of RayManageSoft Unified Endpoint Manager to the Common folders.
- [StrictInstall](#) - determines if the policy agent returns a non-zero exit code or a zero exit code if packages in the policy failed to install.

Inventory Options

The following settings determine how RayManageSoft Unified Endpoint Manager performs inventory collection on managed devices:

General

- [Compress](#) ([Inventory Agent](#)) - determines whether inventory files are compressed before being uploaded.
- [GenerateMD5](#) - specifies whether or not to calculate the MD5 digest of files being tracked by the inventory agent.
- [Inventory](#) - specifies the location to which inventory files are uploaded.
- [InventoryDirectory](#) - specifies a custom directory for the storage of inventory data.
- [InventoryFile](#) - identifies the file name of the local copy of the inventory file.
- [LowProfile](#) ([Installation Agent](#), [Inventory Agent](#)) - determines the CPU priority of RayManageSoft Unified Endpoint Manager on the managed device.
- [MachineInventoryDirectory](#) - determines the location in which to store machine inventories.
- [MachineZeroTouchDirectory](#) - determines the location in which to store machine inventories in case of a remote call.
- [ManageSoftPackages](#) - determines the installed software packages.
- [MinInventoryInterval](#) - specifies the minimum interval (in hours) between the collection of inventories.
- [NetworkSense](#) ([Inventory Agent](#)) - determines whether network checks are bypassed for uploads performed by the inventory agent.
- [ProgressDepth](#) - specifies the number of the directory levels to search at the initialization to



approximate the number of directories searched during tracking.

- [SMBIOSCmdLine](#) - specifies a command-line for non-WMI hardware inventory collection.



Options to Control Custom Scripts on Inventory Data

- [InventoryScriptsDir](#) - determines the location of scripts to be run before inventory data is uploaded through the distribution hierarchy.
- [RunInventoryScripts](#) - specifies if scripts should be run on inventory data prior to uploading inventory data through the distribution hierarchy.

Options to Control Differential Inventory

- [Difference](#) - determines whether RayManageSoft Unified Endpoint Manager will perform differential inventories rather than full inventories.
- [GenerationMax](#) - defines the number of differential inventories that may take place before a full inventory is performed.
- [IncrementalDiff](#) - specifies what differences the differential inventory will collect if differential inventory is in use.

Options to Determine Inventory Inclusions and Exclusions

- [ExcludeDirectory](#) - specifies folders to exclude from the inventory.
- [ExcludeExtension](#) - specifies file extensions to exclude from the inventory.
- [ExcludeFile](#) - specifies files to exclude from the inventory.
- [ExcludeMD5](#) - specifies an MD5 checksum. Files that match the checksum are excluded from the inventory.
- [ExcludePermissionsMask](#) - specifies an octal mask for file permissions. Files that match the mask are excluded from the inventory.
- [Hardware](#) - determines whether to track hardware in the machine context.
- [IncludeDirectory](#) - specifies a specific folder to include into the inventory.
- [IncludeExtension](#) - specifies file extensions to include into the inventory.
- [IncludeFile](#) - specifies files to include into the inventory.
- [IncludeMD5](#) - specifies whether a file matching a specific MD5 digest is to be included in the inventory.
- [IncludePermissionsMask](#) - specifies an octal mask for file permissions. Files that match the mask are to be included in the inventory.
- [IncludeRegistryKey](#) - specifies the registry keys or values to include in the inventory.
- [MSI](#) - determines whether Microsoft Installer (MSI) packages are included in the inventory.
- [PlatformSpecificPackages](#) - specifies whether the information about non-Windows, platform-specific packages is included in the inventory.
- [VersionInfo](#) - determines whether file version header information is included in the inventory.

How RayManageSoft Unified Endpoint Manager Uses Inventory and Exclusion Settings

For file tracking, many of the inventory preferences work together to determine whether files are



included in an inventory file. RayManageSoft Unified Endpoint Manager determines this in the following way:

1. RayManageSoft Unified Endpoint Manager first identifies which folders to track during the inventory process. Only folders identified by the `IncludeDirectory` setting are included, unless they are also identified by the `ExcludeDirectory` setting (`ExcludeDirectory` settings override `IncludeDirectory` settings).
2. For each file within a folder explicitly included in the inventory, RayManageSoft Unified Endpoint Manager performs the following steps to determine whether to include the file in its inventory file. All **Exclude** settings override **Include** settings.
3. RayManageSoft Unified Endpoint Manager determines whether the file is explicitly included or excluded, based on whether the values of `ExcludeMD5` and `IncludeMD5` match the MD5 checksum value of the file.
4. If the file is not explicitly included or excluded, RayManageSoft Unified Endpoint Manager determines whether the file name is explicitly included or excluded, based on the values of `ExcludeFile` and `IncludeFile`.
5. If the file name is not explicitly included or excluded, RayManageSoft Unified Endpoint Manager determines whether the file extension is explicitly included or excluded based on the values of `ExcludeExtension` and `IncludeExtension`.
6. If the file extension is not explicitly included or excluded, it is deemed to be excluded from the inventory file.



Be aware:

By default, `.exe` and `.dll` file extensions are included. This can be overridden by setting `IncludeExtension` to `NULL` or any other value.

Example

In this example, the following values are set:

- `Recurse = True`
- `IncludeDirectory = C:\Program Files\`
- `IncludeFile = template.dot`
- `ExcludeExtension = dot`

RayManageSoft Unified Endpoint Manager evaluates the files `C:\Program Files\Common Files\template.dot` and `C:\Program Files\Common Files\master.dot` in the following way:

- Because both files are within a subfolder of `C:\Program Files\`, RayManageSoft Unified Endpoint Manager will evaluate them for inclusion / exclusion.
- There are no `IncludeMD5` or `ExcludeMD5` settings to evaluate, so RayManageSoft Unified Endpoint Manager cannot explicitly include or exclude the file and moves on to evaluate file names.



- The `IncludeMD5` setting specifically shows that `template.dot` should be included. It does not explicitly include or exclude `master.dot`, so RayManageSoft Unified Endpoint Manager moves on to evaluate file extensions.
- The dot extension is explicitly excluded so `master.dot` is excluded. Because `template.dot` has already been explicitly included, its file extension is not evaluated.

Logging Options

Logging options are available for each of the RayManageSoft Unified Endpoint Manager smart-agents running on managed devices, although the number of preferences applicable to each agent does vary. They work in the same way for each agent, but work on different log files.

General Logging Preferences

- [Log](#) - specifies the location where RayManageSoft Unified Endpoint Manager uploads logging files from the managed device.
- [PolicyComplianceLog](#) - specifies the location where RayManageSoft Unified Endpoint Manager uploads policy compliance log files from the managed device.

Installation Agent

- [LogFileOld](#) ([Installation Agent](#)) - specifies the name of the file used to store additional logging information.
- [LogFileSize](#) ([Installation Agent](#)) - specifies the maximum log file size.
- [LogLevel](#) ([Installation Agent](#)) - specifies the level of logging returned by the smart agent.

Package Selection Agent

- [ConfigFile](#) - specifies the name of the system copy of the configuration file used by the selection agent.
- [ConfigFileDefault](#) - specifies the name of the default configuration file to use when all other settings fail.
- [Locale](#) - specifies the locale to use for selection agent localization.
- [LocaleDefault](#) - specifies the locale to use in the absence of other settings.
- [ReInstallRequiresVersionChange](#) - determines whether the RMS UEM AppCenter will upgrade, downgrade, or reinstall packages depending on the version number and the MD5 digest.

Policy Agent

- [BootstrappedPolicy](#) - specifies the location of the policy to be applied to managed devices that do not use policies attached to Active Directory domains.
- [InstallationStatusRefreshPeriod](#) - specifies how frequently (in seconds) RayManageSoft Unified Endpoint Manager should recreate installation events for packages that are either installed or flagged as not required.
- [LogInstallCheck](#) - specifies whether RayManageSoft Unified Endpoint Manager should recreate installation events while checking packages for an installation or an upgrade.



- [LogInstallFail](#) - specifies whether RayManageSoft Unified Endpoint Manager should log failed installation attempts.
- [LogInstallPass](#) - specifies whether RayManageSoft Unified Endpoint Manager should log successful installation events.
- [LogUninstallFail](#) - specifies whether RayManageSoft Unified Endpoint Manager should log failed uninstallation attempts.
- [LogUninstallPass](#) - specifies whether RayManageSoft Unified Endpoint Manager should log successful uninstallation events.

RayManageSoft Folder Locations

The following settings contain information about folders that RayManageSoft Unified Endpoint Manager uses. It is possible to reference these settings in package details and programmed callouts.

Installation and Package Folders

- [BaseURL](#) - specifies the web location from which the current application can be retrieved.
- [CacheDir](#) - specifies the location of the peer cache.
- [GlobalConfigSource](#) - identifies a URL that contains installation preferences.

Inventory Folders

- [Inventory](#) - specifies the location where RayManageSoft Unified Endpoint Manager uploads inventory files.
- [MachineInventoryDirectory](#) - specifies the location for machine inventories.

Policy Folders

- [BootstrappedPolicy](#) - specifies the location of the policy to be applied to managed devices that do not use policies attached to Active Directory domains.
- [MachinePolicyDirectory](#) - specifies the location in which to save the current machine policy.
- [MachinePolicyPackageDirectory](#) - determines location where package information associated with machine policy is cached.
- [PolicySource](#) - specifies the location where the policy is generated.

Other

- [Log](#) - determines the location where RayManageSoft Unified Endpoint Manager uploads logging files from the managed device.

MSI Package Options

RayManageSoft Unified Endpoint Manager has a number of settings that are used to support Microsoft Windows Installer (also referred to as MSI) and are used for building the command-line parameters to be passed to `msiexec.exe`.



When referencing one of these settings as a project variable within a RayManageSoft Unified Endpoint Manager package, it is necessary to prefix the project variable name with the **\$** symbol and enclose the project variable name in brackets. The **\$** prefix indicates to RayManageSoft Unified Endpoint Manager that the variable must be expanded when the package is installed.

For project variables that are going to be passed to the `msiexec.exe` command-line, it is also necessary to prefix the project variable name (inside the brackets) with the **!** character (also called the *unquoted value operator*). This ensures that empty strings are not displayed in quotes when a project variable with an empty value is expanded in the command-line of `msiexec.exe`.

The following is an example of the correct syntax:

```
$(!VariableName)
```

The following MSI settings are available. For more information on MSI command-lines, refer to the **Windows Platform Windows Installer SDK**.

- [MSI](#) - determines whether Microsoft Installer (MSI) packages are included in the inventory.
- [MsiReinstallFeatures](#) - specifies the MSI components to be installed (equivalent to the MSI property `REINSTALL`).
- [MsiReinstallModeLevel](#) - identifies what will be reinstalled (equivalent to the MSI property `REINSTALLMODE`).
- [MsiRepair](#) - determines if MSI repair operations are performed at the same time as RayManageSoft Unified Endpoint Manager self-healing operations.
- [MsiRepairLevel](#) - identifies what will be repaired (equivalent to the MSI property `REINSTALLMODE`).
- [MsiSourceLocation](#) - determines whether Windows Installer packages are installed from the local Windows Installer cache of the managed device or from a distribution location.
- [MsiUILevel](#) - determines the user interaction level for MSI (equivalent to the option `/q` in the `msiexec.exe` command-line).
- [MsiUninstallArgs](#) - specifies arguments to include in the MSI command-line for uninstall operations.

Network Speed and Connection Options

The following settings influence how RayManageSoft Unified Endpoint Manager uses networks for operations.

Speed

- [MinimumDCSpeed](#) - determines the minimum speed between the managed device and domain controller that is required to apply client-side policies.
- [NetworkHighSpeed](#) ([Installation Agent](#)) - determines the lowest network speed to consider to be a high-speed network connection.
- [NetworkHighSpeed](#) ([Upload Agent](#)) - determines the lowest network speed to consider to be



a high-speed network connection.

- [NetworkHighUsage](#) - specifies the maximum bandwidth for high-speed connections.
- [NetworkLowUsage](#) - specifies the maximum bandwidth for low-speed connections.
- [NetworkMaxRate](#) ([Installation Agent](#)) - determines the rate at which the managed device accesses data over the network.
- [NetworkMaxRate](#) ([Upload Agent](#)) - determines the rate at which the managed device accesses data over the network.
- [NetworkMinSpeed](#) ([Installation Agent](#)) - determines the minimum network speed at which RayManageSoft Unified Endpoint Manager will install or update a package.
- [NetworkMinSpeed](#) ([Upload Agent](#)) - determines the minimum network speed at which RayManageSoft Unified Endpoint Manager will install or update a package.

Protocols, Addresses, and Authentication

- [LogonServer](#) - determines the name of the logon server computer to which the managed device normally connects.

Other

- [ConnectionAttempts](#) - specifies the number of times that a **no connection is available** error can be reported while trying to connect to a particular distribution location as a file share.
- [EventNetType](#) - determines the type of network connections that are required to start events that only trigger if a network is available.
- [HighestPriority](#) - determines the highest upload / download priority that can be assigned to a distribution server.
- [LowestPriority](#) - determines the lowest upload / download priority that can be assigned to a distribution server.
- [ndsensNetType](#) - determines what type of network connections are monitored.
- [ndsensNetUp](#) - determines which command is executed once the `ndsensNetType` property deems to have a network connection.
- [NetworkRetries](#) - specifies the number of times failed network operations are retried before an alternative distribution location is attempted.
- [NetworkSense](#) ([Installation Agent](#)) - determines whether network checks are bypassed.
- [NetworkSense](#) ([Inventory Agent](#)) - determines whether network checks are bypassed.
- [NetworkSense](#) ([Upload Agent](#)) - determines whether network checks are bypassed.
- [NetworkTimeout](#) ([Installation Agent](#)) - specifies the number of seconds of inactivity before a network operation will time out.
- [NetworkTimeout](#) ([Upload Agent](#)) - specifies the number of seconds of inactivity before a network operation will time out.
- [SelectorAlgorithm](#) - the algorithm(s) used to determine relative priorities in selecting the distribution server to use for uploads / downloads.



Package-level Filtering Options

The following options contain information on package-level filtering during a RayManageSoft Unified Endpoint Manager client-side policy merge.

- [DisablePackageFiltering](#) - allows to skip package-level filtering during a policy merge if filtering is not required.

Package RMS UEM AppCenter Options

The following settings can be used to control the behavior of the RayManageSoft Unified Endpoint Manager package selection agent on the managed device.

- [ApplicationInstallCommand](#) - specifies a template command-line to be used to install an application package through the RayManageSoft Unified Endpoint Manager package selection agent.
- [ApplicationUninstallCommand](#) - specifies a template command-line to be used to uninstall an application package through the RayManageSoft Unified Endpoint Manager package selection agent.
- [ApplicationVerifyCommand](#) - specifies a template command-line to be used to verify / repair an application package through the RayManageSoft Unified Endpoint Manager package selection agent.
- [ConfigFile](#) - determines the name of the configuration file used by the RayManageSoft Unified Endpoint Manager user interface on managed devices.
- [DiskReservedKB](#) - determines the amount of disk space to reserve on each drive.
- [ReInstallRequiresVersionChange](#) - determines whether the RMS UEM AppCenter will upgrade, downgrade, or reinstall packages depending on the version number and the MD5 digest.

Policy Merge Options

These settings influence how RayManageSoft Unified Endpoint Manager merges Active Directory group policies. For managed devices that do not use Active Directory group policies, no policy merging is performed. Instead, the location of the policy is specified by `BootstrappedPolicy`.

General

- [AutoDetectDC](#) - determines how RayManageSoft Unified Endpoint Manager selects a domain controller for client-side policy merging.
- [EnablePolicyFailOver](#) - specifies whether a server-side policy file should be applied if a client-side policy file is unavailable.
- [HideMachineUI](#) - determines whether RayManageSoft Unified Endpoint Manager displays a user interface when applying a machine policy.
- [LauncherCommandLine](#) - specifies the installation agent command-line options to pass to RayManageSoft Unified Endpoint Manager when applying policy information.



- [MinimumDCSpeed](#) - determines the minimum speed between the managed device and domain controller that is required to apply client-side policies.
- [RetryPolicy](#) - determines whether RayManageSoft Unified Endpoint Manager will attempt to retrieve RayManageSoft Unified Endpoint Manager policies when the managed device boots if no machine schedule exists on the managed device.
- [RetryPolicyCommand](#) - specifies the command used to retrieve a policy if `RetryPolicy` is set to `True`.

Locations

- [MachinePolicyDirectory](#) - specifies the location in which to save the current machine policy.
- [MachinePolicyPackageDirectory](#) - specifies the location where package information associated with machine policy is cached.
- [PolicyComplianceLog](#) - specifies the location where RayManageSoft Unified Endpoint Manager uploads policy compliance log files from the managed device.
- [PolicySource](#) - specifies the location where the policy is generated.



Preference Setting Management Options

The following settings can determine the way RayManageSoft Unified Endpoint Manager evaluates settings on managed devices.

- [CmdLineOverrides](#) - determines whether options set on the command-line override fixed settings in the registry or network preference file.
- [GlobalConfigSource](#) - identifies a URL that contains installation settings.
- [IncludeRegistryKey](#) - specifies registry keys or values to include in the inventory.
- [MachineAlternateRegistryHive](#) - specifies the alternate registry hive.
- [SaveAllUserSymbols](#) - determines whether RayManageSoft Unified Endpoint Manager retains installation settings configured by a top-level or prerequisite package. Also see [Persistent Managed Device Preference Settings](#).

Prerequisite Package Options

The following settings influence the installation of prerequisite packages.

- [PropagatePkgChanged](#) - reinstalls the base package if the prerequisite package has changed for Third party installer packages.
- [SaveAllUserSymbols](#) - determines whether RayManageSoft Unified Endpoint Manager retains installation settings configured by a top-level or prerequisite package.

Reboot Options

In the final stages of its processing the reboot behavior is controlled by the installation agent. This means that in the normal course of events where package updates are occurring as part of a policy check, the reboot behavior effectively applies at a policy level (if one or more packages require a reboot to occur, a single reboot process is initiated at the end of the policy check). In other cases, where a package update occurs solitarily (perhaps because of a special schedule event, or through end-user action in the selection agent), the reboot can be seen to apply at the individual package level.

Installation Agent

The following settings can be used to control the reboot behavior during package processing.

- [AllowRebootIfLocked](#) - controls whether RayManageSoft Unified Endpoint Manager reboots the managed device if the package being installed requires it and the desktop is locked.
- [AllowRebootIfServer](#) - controls whether RayManageSoft Unified Endpoint Manager reboots the managed device if it is a server (used by the adoption agent, but not the installation agent).
- [AllowTimeoutIfLocked](#) - controls whether the time interval for prompting the end-user commences immediately if the desktop is locked or only commences when the desktop is unlocked.
- [AlwaysDisplayReboot](#) - controls whether RayManageSoft Unified Endpoint Manager displays



a warning to the end-user before rebooting (overrides `UserInteractionLevel` (Installation Agent)).

- [ForceReboot](#) - determines whether RayManageSoft Unified Endpoint Manager performs a forced reboot if the desktop is not locked. A forced reboot suppresses any user interaction required to close other applications that may be running.
- [ForceRebootIfLocked](#) - determines whether RayManageSoft Unified Endpoint Manager performs a forced reboot if the desktop of the end-user is locked. A forced reboot suppresses any user interaction required to close other applications that may be running.
- [RebootCmdLine](#) - used on the managed device to reboot from the command-line.
- [RebootContinueAfterCmdFailure](#) - controls whether or not to proceed with the reboot if the `RebootPreCommand` returned a non-zero exit code.
- [RebootIfRequired](#) - controls whether RayManageSoft Unified Endpoint Manager reboots the managed device if the package being installed requires it and the desktop of the end-user is not locked.
- [RebootPostCommand](#) - specifies a command to be executed after the managed device is rebooted.
- [RebootPreCommand](#) - specifies a command to be executed before the managed device is rebooted.
- [RebootPromptCycles](#) - determines the number of times the end-user can postpone the managed device reboot. Prompts occur at intervals specified by `RebootPromptWait`.
- [RebootPromptUnlimited](#) - determines if RayManageSoft Unified Endpoint Manager keeps prompting the end-user at intervals specified by `RebootPromptWait` until the managed device reboots (equivalent to `RebootPromptCycles=-1`).
- [RebootPromptWait](#) - determines the number of seconds to wait after the end-user dismisses the reboot dialog before displaying it again.
- [SecurityPatchRebootIfRequired](#) - specifies the default response to dialogs displayed during security patch installation that prompt the user to allow a reboot.
- [UITimeoutWait](#) - determines the number of seconds that installation agent dialogs display before timing out.
- [RenotifyTimeout](#) - determines the number of seconds that the installation agent waits before once again showing a user any hidden dialogs that have not yet timed out.

When RayManageSoft Unified Endpoint Manager identifies that a reboot is required, the combination of these settings determines the action that is taken.

Reboot Agent Preferences

The installation agent calls the reboot agent (`reboot.exe`) as necessary. If choosing to run the reboot agent independently, the following preferences apply:

- [RebootContinueAfterCmdFailure](#) - specifies whether or not to continue with rebooting a managed device if the execution of a prereboot command returns a non-zero exit code.
- [RebootPostCommand](#) - specifies a command to run immediately after a managed device is



rebooted.

- [RebootPreCommand](#) - specifies a command to run immediately before a managed device is rebooted.
- [RebootPromptCycles](#) - specifies the number of times an end-user can postpone the reboot of a managed device.
- [RebootPromptWait](#) - specifies the time interval (in seconds) to wait before redisplaying the dialog that prompts the end-user to reboot.

The following decision tree illustrates how the installation agent reboot settings work together. In this diagram:

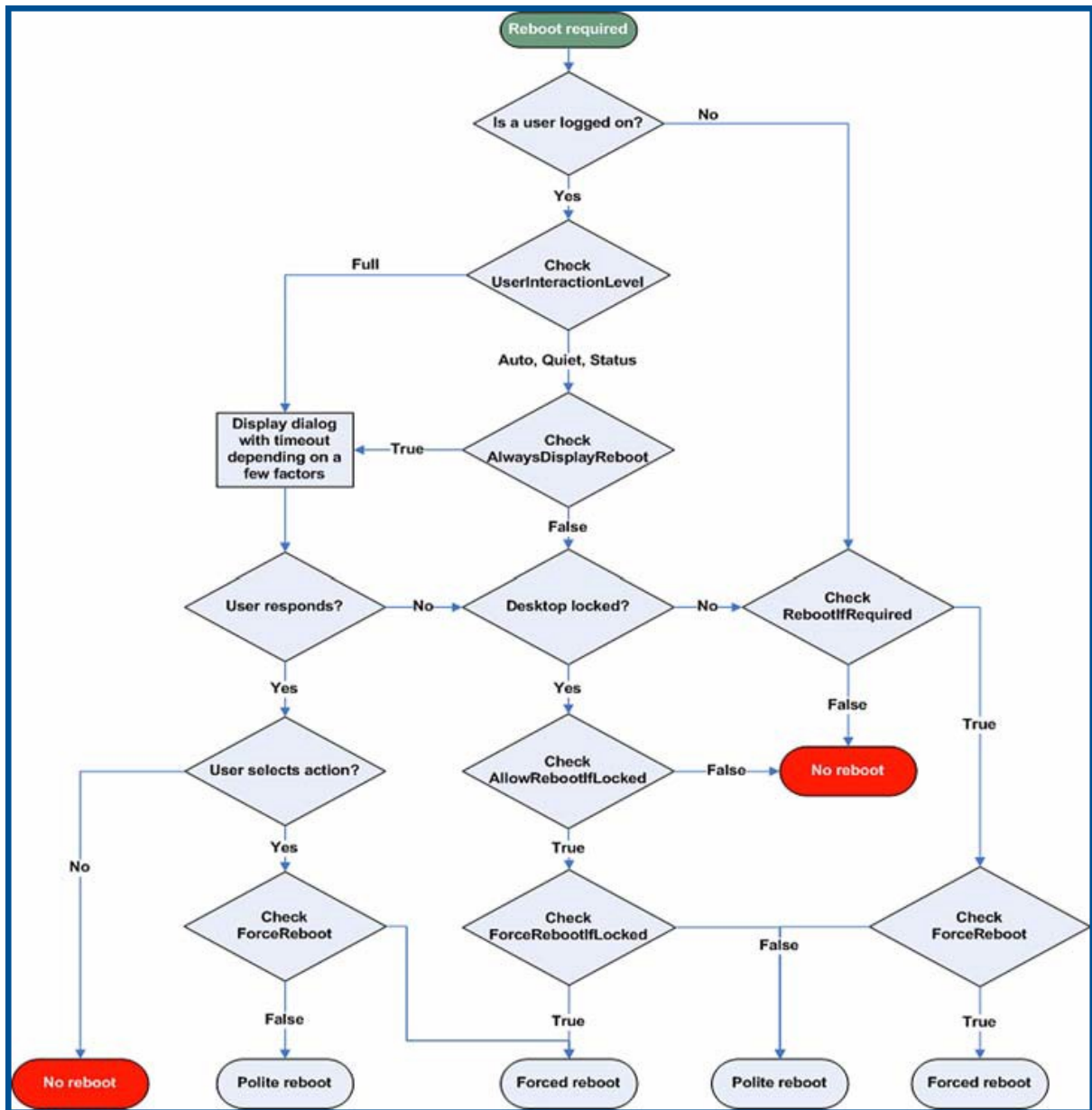
- A *Polite reboot* means a reboot action where RayManageSoft Unified Endpoint Manager alerts other open applications and requests that they shut down in an orderly manner.



Note:

Other such applications may present dialogs to the end-user through which the end-user might cancel the reboot process. In that case, some newly installed or updated applications may not function until the next reboot (A polite reboot does not involve direct interaction between RayManageSoft Unified Endpoint Manager and the end-user.).

- A *Forced reboot* means that RayManageSoft Unified Endpoint Manager ignores the state of all other applications and initiates the reboot. Only the operating system can override this. A forced reboot may cause the loss of data from open applications and should be used with care.



The decision tree to determine the correct reboot behavior on managed device based on the preference settings.

Remote Execution Options

The following setting can be used to specify behavior when tasks are being remotely executed on managed devices.

- [ListeningPort](#) - determines the port number that the TCP-based listening agent monitors for incoming requests. If not specified, port 7020 is used.



Scheduling Options

The following settings can be used to control RayManageSoft Unified Endpoint Manager task scheduling on the managed device.

General

- [ApplyPolicyIfLoggedIn](#) - specifies whether or not a computer policy is applied at the scheduled time if a user is logged on (Windows devices only).
- [DisablePeriod](#) - determines the number of seconds for which RayManageSoft Unified Endpoint Manager user schedules remain disabled when the end-user disables them in the schedule agent on the managed device (Windows devices only).
- [NativeScheduler](#) - determines whether the Microsoft Task Scheduler or RayManageSoft Unified Endpoint Manager Task Scheduler is in use (the Microsoft Task Scheduler is only available on Windows devices).
- [PolicyPackageRefreshPeriod](#) - specifies the number of hours after successfully downloading package (.osd) files during which the download of those files should not be attempted again.
- [PolicyRefreshPeriod](#) - specifies the number of hours after successfully downloading policy (.npl) files during which policy files should not be downloaded again.
- [RetryPolicy](#) - specifies whether RayManageSoft Unified Endpoint Manager will attempt to retrieve a RayManageSoft Unified Endpoint Manager policy when the managed device boots, if no machine schedule exists on the managed device.
- [RetryPolicyCommand](#) - specifies the command used to retrieve a policy if `RetryPolicy` is set to `True`

Triggers and Events

- [EventNetType](#) - specifies the type of connection being looked for in order to determine if a network is available.
- [ndsensNetType](#) - specifies the type of connection that is necessary in order to determine if the **When connected to network** trigger has occurred.
- [ndsensNetUp](#) - determines which command is executed once the `ndsensNetType` property deems to have a network connection.



Security Options

The following settings can be used to determine security behavior during package processing, uploads, and downloads. They relate to Authenticode checks and passwords for FTP authentication.

- [CheckCertificateRevocation](#) - determines whether RayManageSoft Unified Endpoint Manager checks the certificate revocation list when accepting web server signatures from an HTTPS server.
- [DisplayAllAuthcode](#) - determines the subsequent behavior after RayManageSoft Unified Endpoint Manager encounters an invalid signature when performing an Authenticode check.
- [ForceValidSignature](#) - determines whether RayManageSoft Unified Endpoint Manager prompts the user before installing a package when Authenticode signatures are valid.
- [PublicAppAccess](#) - determines RayManageSoft Unified Endpoint Manager access to **Common** folders.
- [SecurityPatchRebootIfRequired](#) - specifies the default response to dialogs displayed during security patch installation that prompt the user to allow a reboot.
- [VerifyCatalogSigned](#) - determines whether Authenticode digital signatures are checked in the RayManageSoft Unified Endpoint Manager catalog (.ndc) file before packages are installed.
- [VerifyFilesSigned](#) - determines whether executable files downloaded by RayManageSoft Unified Endpoint Manager are checked for a valid Authenticode digital signature before being installed.
- [AllowedGroups](#) – determines whether RayManageSoft Unified Endpoint Manager checks that the current user is allowed to interact directly with the RMS UEM AppCenter Agent.

Also see [Trusted Location Options](#).

Self-heal Options

The following settings determine how RayManageSoft Unified Endpoint Manager self-heal operations work on the managed device.

- [ApplicationVerifyCommand](#) - specifies a template command-line to be used to verify / repair an application package through the RayManageSoft Unified Endpoint Manager package selection agent.
- [CheckCatalogDigest](#) - determines whether RayManageSoft Unified Endpoint Manager performs a check on package-level MD5 digests during self-healing operations.
- [CheckFileDigest](#) - determines whether RayManageSoft Unified Endpoint Manager performs a check on file-level MD5 digests during self-healing operations.
- [CheckRegistry](#) (or [Reg on the command-line](#)) - determines if RayManageSoft Unified Endpoint Manager performs self-healing on registry keys and preference files.
- [MsiRepair](#) - determines if MSI repair operations are performed at the same time as RayManageSoft Unified Endpoint Manager self-healing operations.
- [MsiSourceLocation](#) - determines whether Windows Installer packages are installed from the



local Windows Installer cache of the managed device or from a distribution location.

- [SelfHeal](#) - determines whether self-healing should take place for an individual package.
- [SupplyWorstCaseReturnValue](#) - determines whether RayManageSoft Unified Endpoint Manager returns an error only when an installation agent operation fails or also when upgrades or self-heal operations fail.

Trusted Location Options

The following settings determine whether RayManageSoft Unified Endpoint Manager trusted locations are used.

- [UseTrustDatabase](#) - determines whether RayManageSoft Unified Endpoint Manager only downloads from trusted locations.
- [TrustDatabaseFxd](#) - determines whether users need administrator permissions to change trusted and excluded locations.

To Add a Trusted Location

To identify a trusted location, create a key for the location under the following registry key:

[Registry]\ManageSoft\Launcher\CurrentVersion\TrustedLocations

Then create the following subkeys and assign values to identify the location.

- `Directory` - the location of the distribution location within the specified host. To include subfolders, append * to the end of the value.
- `Host` - the computer on which the distribution location is hosted.
- `Port` - the port number for data transfer to the managed device.
- `Protocol` - the protocol for transferring files to the managed device.

To Add an Excluded Location

To identify an excluded location, create a key for the location under the following registry key:

[Registry]\ManageSoft\Launcher\CurrentVersion\ExcludedLocations

Then create the following subkeys and assign values to identify the location.

- `Directory` - the location of the distribution location within the specified host. To include subfolders, append * to the end of the value.
- `Host` - the computer on which the distribution location is hosted.
- `Port` - the port number for data transfer to the managed device.
- `Protocol` - the protocol for transferring files to the managed device.

How RayManageSoft Unified Endpoint Manager Identifies Trusted Locations



- If the `UseTrustDatabase` preference is set to `True`, RayManageSoft Unified Endpoint Manager determines trusted locations based on the following rules:
 - Only servers identified under the `TrustedLocations` key are included unless they are also listed under the `ExcludedLocations` key.
 - If there are no server identified under the `TrustedLocations` key, all servers are trusted unless listed under `ExcludedLocations` key.

Uninstall Options

The following preferences influence the uninstall behavior on the managed device:

- [ApplicationUninstallCommand](#) - specifies a template command-line to uninstall an application package through the RayManageSoft Unified Endpoint Manager package selection agent.
- [ForceSharedFileRemove](#) - determines whether shared files in the Windows system folder are deleted during uninstalls.
- [InstallerARPremove](#) - determines whether external installer packages can be uninstalled via the Windows **Add/Remove Programs** applet.

Upgrade / Downgrade Options

The following preferences determine how upgrades and downgrades are performed on the managed device.

- [ForceSharedFileRemove](#) - determines if shared files marked as redundant can be deleted.
- [ReInstallRequiresVersionChange](#) - determines when packages will be upgraded, downgraded, or reinstalled, based on the type of changes made to the package.
- [SupplyWorstCaseReturnValue](#) - determines whether RayManageSoft Unified Endpoint Manager returns an error only when an installation agent operation fails or also when upgrades or self-heal operations fail.

Upload Options

The following settings influence how information is uploaded from the managed device to reporting locations.

General

- [CheckCertificateRevocation](#) - determines whether RayManageSoft Unified Endpoint Manager checks the certificate revocation list when accepting web server signatures from an HTTPS server.
- [Compress](#) ([Inventory Agent](#)) - determines whether inventory files are compressed for the upload.
- [HighestPriority](#) - specifies the highest upload / download priority that can be assigned to a



distribution server.

- [LowestPriority](#) - specifies the lowest upload / download priority that can be assigned to a distribution server.
- [SelectorAlgorithm](#) - the algorithm(s) used to determine relative priorities in selecting the distribution server to use for uploads / downloads.



Locations from Which Data is Uploaded

- [Inventory](#) - specifies the location where RayManageSoft Unified Endpoint Manager uploads inventory files.
- [Log](#) - specifies the location where RayManageSoft Unified Endpoint Manager uploads logging files from the managed device.
- [PolicyComplianceLog](#) - specifies the location where RayManageSoft Unified Endpoint Manager uploads policy compliance log files from the managed device.

User Interaction Options

The following settings control the RayManageSoft Unified Endpoint Manager user interaction on Windows managed devices. These settings are ignored on non-Windows managed devices.

General

- [HideMachineUI](#) - determines whether RayManageSoft Unified Endpoint Manager displays a user interface when applying a machine policy.
- [QuietUntilUpdate](#) - controls whether the RayManageSoft Unified Endpoint Manager user interface is hidden if no user interaction is necessary.
- [UITimeoutWait](#) - specifies the number of seconds that installation agent dialogs display before timing out.

Prompts and Confirmations

- [AlwaysDisplayReboot](#) - controls whether RayManageSoft Unified Endpoint Manager displays a warning to the user before performing any reboot required by a package installation (overrides `UserInteractionLevel`).
- [ConfirmSharedFileRemoval](#) - determines whether RayManageSoft Unified Endpoint Manager displays a dialog when removing a file.
- [PromptOnCOMRegFailures](#) - determines whether RayManageSoft Unified Endpoint Manager prompts the user if it fails to register a COM server.
- [PromptOnInstallCompletion](#) - determines whether RayManageSoft Unified Endpoint Manager informs the user when package installation is complete when the `UserInteractionLevel` is set to `Full`.
- [PromptOnUnInstallCompletion](#) - determines whether RayManageSoft Unified Endpoint Manager informs the user when package uninstallation is complete when the `UserInteractionLevel` is set to `Full`.
- [SupplyWorstCaseReturnValue](#) - determines whether RayManageSoft Unified Endpoint Manager returns an error only when an installation agent operation fails or also when upgrades or self-heal operations fail.



Virus Scanning Options

The following settings can be used to run virus scans on the managed device.

- [VirusScan](#) - specifies if RayManageSoft Unified Endpoint Manager scans the downloaded files for viruses before installing them.
- [VirusScanCommand](#) - determines the virus scan application that is being used.

Windows Folder Information

The following settings contain information about Windows folders on the managed device. They can be referenced in package details and programmed callouts.

- [AppDataFolder](#) - specifies the path to the folder in which user-specific application details are located.
- [CommonProgramMenuFolder](#) - contains the path to Start menu program folders and shortcuts for [ALL USERS].

Alphabetical Listing of Preference Settings for Managed Devices

This section describes each setting in an alphabetical order.

For each setting listed, the details include:

- A description of the setting
- Possible values
- Registry details
- Project variable usage
- Command-line usage



AddRemove

Command-line | Registry | Project Variable

When set to `Create` or `Default`, all packages installed by RayManageSoft Unified Endpoint Manager create an entry in the **Add/Remove Programs** control panel applet. When set to `NoCreate`, RayManageSoft Unified Endpoint Manager does not create an entry in the **Add/Remove Programs** applet.



Be aware:

This setting only applies to native RayManageSoft Unified Endpoint Manager packages. It does not apply to MSI-based or general third-party package.



Be aware:

The `Default` setting means two things:

- For new installations an `AddRemove` entry is created.
- For updated installations the creation of an `AddRemove` entry for the previous version of the application is being dictated. For example, if the application had an `AddRemove` entry, then one will be created. If it did not have an `AddRemove` entry, then RayManageSoft Unified Endpoint Manager will not create an entry.

Values / Range:	Default, Create, or NoCreate
Default value:	Default

Command-line

Tool:	Installation agent
Example:	<code>-o AddRemove=NoCreate -r http://myserver/mypg.osd</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (computer preference)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	AddRemove
Reference as:	<code>\$ (AddRemove)</code>



AllowedGroups

Registry

When set to at least one security group, RayManageSoft Unified Endpoint Manager checks the current user to be a member of at least one given group when directly interacting with the RMS UEM AppCenter Agent. When no value is set, RayManageSoft Unified Endpoint Manager does not check any membership. Every user is allowed to directly interact with the RMS UEM AppCenter Agent.

Values / Range:	String
Default value:	{empty}

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

AllowPeerToPeer

Registry

Specifies whether managed devices can obtain downloaded files from other managed devices on the same LAN (peers). Peer-to-peer file sharing minimizes download volumes from distribution servers and makes downloaded files available to managed devices at LAN speed.

Values / Range:	Boolean (True or False)
Default value:	False

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	[Registry]\ManageSoft\Common



AllowRebootIfLocked

Command-line | Registry

Determines whether to reboot or not if RayManageSoft Unified Endpoint Manager has determined that a reboot is necessary and the desktop of the end-user is locked. If `AllowRebootIfLocked` and `ForceRebootIfLocked` are set to `True`, the computer reboots immediately without prompting the end-user.

This setting configures the default response to the installation agent dialog that prompts end-users to confirm a reboot:

- When set to `False`, the default response is to not reboot and the dialog times out according to `UITimeoutWait`.
- When set to `True`, the default response is to confirm the reboot.

Values / Range:	Boolean (True or False)
Default value:	False

Command-line

Tool:	Installation agent
Example:	<code>-o AllowRebootIfLocked=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (computer preference)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

AllowRebootIfServer

Command-line | Registry

This registry entry is not used RayManageSoft Unified Endpoint Manager on managed devices. It may be used when computers are automatically adopted under management.

Values / Range:	Boolean (True or False)
Default value:	False



Command-line

Tool:	Adoption Agent
Example:	-o AllowRebootIfServer=True

Registry

Installed by:	Adoption of computers under RayManageSoft Unified Endpoint Manager management. Installation of RayManageSoft Unified Endpoint Manager on a managed device.
User setting:	CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Common\Rules
Computer setting:	[Registry]\ManageSoft\Common\Rules

AllowTimeOutIfLocked

Registry

Specifies whether the process of prompting the end-user to postpone a reboot starts immediately on locked desktops or only when the desktop is unlocked.

Values / Range:	Boolean (True or False)
Default value:	True

Registry

Installed by:	Installation or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

AlwaysDisplayReboot

Command-line | Registry

This preference applies when a reboot is required as part of a package installation.

When set to `True`, RayManageSoft Unified Endpoint Manager displays a warning to the end-user regardless of the setting of the `UserInteractionLevel` (Installation agent).

Values / Range:	Boolean (True or False)



Default value:	False

Command-line

Tool:	Installation agent
Example:	-o AlwaysDisplayReboot=True

Registry

Installed by:	Adoption of computers under RayManageSoft Unified Endpoint Manager management, Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Common\Rules
Computer setting:	[Registry]\ManageSoft\Common\Rules

AppDataFolder

Project Variable

The path to the folder in which user-specific application details are located.

Values / Range:	A local directory name. Read-only!
Default value:	The default installation of Windows uses the [USER PROFILE]\Application Data folder.
Example value:	C:\Users\Jane\Application Data C:\Documents and Settings\James\ Application Data

Project Variable

Define as:	Predefined within Windows
Reference as:	\$(AppDataFolder)

ApplicationInstallCommand

Command-line | Registry

Specifies a template command-line to be used to install an application package through the RayManageSoft Unified Endpoint Manager package selection agent. The selection agent uses the value from this setting to build command-lines that are executed in order to install packages



selected by a user.

The value of this setting should always include the following special substrings:

- {1} - This substring will be replaced with the URL of the package to be installed. This value is typically passed as the value of the `-r` command-line option of the installation agent. The URL may contain space characters and therefore should be quoted appropriately in the command-line.
- {2} - This substring will be replaced with any installation agent command-line options that the selection agent determines may be needed to install the package. This value should not be quoted in the command-line.

Values / Range:	A valid command-line string containing the literal substrings {1} and {2}.
Default value:	<code>ndlaunch -r "{1}" -o SaveAllUserSymbols=False {2}</code>
Example value:	To install packages with full user interaction: <code>ndlaunch -r "{1}" -o SaveAllUserSymbols=False {2}</code> <code>-o UserInteractionLevel=Full</code>



Note:

{2} will normally expand to specify a default `UserInteractionLevel` determined by the selection agent. Therefore, in the example, the option to override the setting on the command-line appears **after** the {2} substring.

Command-line

Tool:	Package selection agent
Example:	<code>-o ApplicationInstallCommand="ndlaunch -r ""{1}""</code> <code>-o SaveAllUserSymbols=False {2}</code> <code>-o UserInteractionLevel=Full"</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Selector\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Selector\CurrentVersion</code>

ApplicationUninstallCommand

Command-line | Registry



Specifies a template command-line to be used to uninstall an application package through the RayManageSoft Unified Endpoint Manager package selection agent. The selection agent uses the value from this setting to build command-lines that are executed in order to uninstall packages selected by a user.

The value of this setting should always include the following special substrings:

- {1} - This substring will be replaced with the URL of the package to be uninstalled. This value is typically passed as the value of the `-d` command-line option of the installation agent. The URL may contain space characters and therefore should be quoted appropriately in the command-line.
- {2} - This substring will be replaced with any installation agent command-line options that the selection agent determines may be needed to uninstall the package. This value should not be quoted in the command-line.

Values / Range:	A valid command-line string containing the literal substrings {1} and {2}.
Default value:	<code>ndlaunch -d "{1}" -o SaveAllUserSymbols=False {2}</code>
Example value:	To uninstall packages with full user interaction: <code>ndlaunch -d "{1}" -o SaveAllUserSymbols=False {2} -o UserInteractionLevel=Full</code>

**Note:**

{2} will normally expand to specify a default `UserInteractionLevel` determined by the selection agent. Therefore, in the example, the option to override the setting on the command-line appears **after** the {2} substring.

Command-line

Tool:	Package selection agent
Example:	<code>-o ApplicationUninstallCommand="ndlaunch -d "{1}" -o SaveAllUserSymbols=False {2} -o UserInteractionLevel=Full"</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Selector\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Selector\CurrentVersion</code>



ApplicationVerifyCommand

Command-line | Registry

Specifies a template command-line to be used to verify/repair an application package through the RayManageSoft Unified Endpoint Manager package selection agent. The selection agent uses the value from this setting to build command-lines that are executed in order to verify packages selected by a user.

The value of this setting should always include the following special substrings:

- {1} - This substring will be replaced with the URL of the package to be verified. This value is typically passed as the value of the `-a` command-line option of the installation agent. The URL may contain space characters and therefore should be quoted appropriately in the command-line.
- {2} - This substring will be replaced with any installation agent command-line options that the selection agent determines may be needed to verify the package. This value should not be quoted in the command-line.

Values / Range:	A valid command-line string containing the literal substrings {1} and {2}.
Default value:	<code>ndlaunch -a "{1}" -o SaveAllUserSymbols=False -o MsiRepair=True -o CachedVersion=True -o SelfHeal=True -o CheckRegistry=True -o NoExec=True {2}</code>
Example value:	To require applications to be verified against their source from an appropriate distribution location and to not self-heal registry settings: <code>ndlaunch -a "{1}" -o SaveAllUserSymbols=False -o MsiRepair=True -CheckRegistry=False -o NoExec=True {2}</code>

Command-line

Tool:	Package selection agent
Example:	<code>-o ApplicationVerifyCommand= "ndlaunch -a ""{1}"" -o SaveAllUserSymbols=False -MsiRepair=True -o CheckRegistry=False -o NoExec=True {2}"</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual



	configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Selector\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Selector\CurrentVersion

ApplyLocalPolicy

Registry

Specifies whether to use a locally cached copy of a policy if a new policy cannot be generated (if client-side policy merging is in operation) or downloaded (if server-side merging is in operation). If set to `True`, a locally cached copy of the policy will be used if no version can be generated or downloaded. If set to `False`, no locally cached copy will be used (which means an attempted policy application will fail if the policy cannot be generated or downloaded).

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Policy Client\CurrentVersion
Computer setting:	[Registry]\Managesoft\Policy Client\ CurrentVersion

ApplyPolicy

Command-line

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

It is used in conjunction with `DownloadPolicy` in order to distinguish between the application of a RMS UEM AppCenter policy and the update of a policy and package definitions in peer cache.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>



Command-line

Tool:	Installation agent
Example:	-o DownloadPolicy=False

ApplyPolicyIfLoggedOn

Command-line | Registry

This setting is only applicable for Windows devices.

It specifies whether RayManageSoft Unified Endpoint Manager should apply computer policies when a user is logged on. If set to `True`, computer policies will be applied when scheduled, whether or not a user is logged on. If set to `False`, computer policies will not be applied if a user is logged on at the scheduled time. RayManageSoft Unified Endpoint Manager will attempt to apply the computer policy at the next scheduled time.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>

Command-line

Tool:	Scheduling agent
Example:	-o ApplyPolicyIfLoggedOn=False

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Schedule Agent\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Schedule Agent\ CurrentVersion

AutoDetectDC

Command-line | Registry | Project Variable

Applies only for the client-side merging policy.

When set to `True`, RayManageSoft Unified Endpoint Manager allows Windows to automatically determine which domain RayManageSoft Unified Endpoint Manager will connect to in order to apply a policy. When set to `False`, RayManageSoft Unified Endpoint Manager will apply the policy using a domain controller in the same site as the managed device. If no domain controller



is available, the policy merge will fail.

Values / Range:	Boolean (True or False)
Default value:	True

Command-line

Tool:	Installation agent
Example:	-o AutoDetectDC=False

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Common
Computer setting:	[Registry]\ManageSoft\Common

Project Variable

Define as:	AutoDetectDC
Reference as:	\$(AutoDetectDC)



BaseURL

Project Variable

The URL of the distribution location from which the current application can be retrieved.

Values / Range:	A valid URL
Default value:	Usually the folder in which the OSD/NDC files are located.
Example value:	<code>file://serverName/share/distributionLocation/ Packages/Company/Product/</code>

Project Variable

Define as:	Predefined by RayManageSoft Unified Endpoint Manager
Reference as:	<code>\$ (BaseURL)</code>

BootstrappedPolicy

Command-line | Registry

When policies are attached to Active Directory domains, the policy that is to be applied on a managed device is the result of the policy merge. For policies attached to the RayManageSoft Unified Endpoint Manager domain, a specific policy file (name and location of the file are specified in this setting) is assigned to each managed device.

Values / Range:	String
Default value:	None

Command-line

Tool:	Policy agent
Example:	<code>-o BootstrappedPolicy="ManageSoftDL\Policy\ Marketing.npl"</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager policy configuration
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Policy Client\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Policy Client\ CurrentVersion</code>



BrandARP

Command-line

Provides the ability to exclude the name "RayManageSoft Unified Endpoint Manager" from the **Add/Remove Program** entries for installed applications.

Values / Range:	Boolean (True or False)
Default value:	True

Command-line

Tool:	Installation agent
Example:	-o BrandARP=True

CacheDir

Command-line | Registry

This cache is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`). For more information see [AllowPeerToPeer](#).

This setting specifies the location of the peer cache on the managed device. Files are downloaded to this location and shared from this location with peer managed devices. If peer-to-peer file sharing is enabled, the installation agent downloads package files from the `CacheDir` location to the `CacheDirectory` instead of downloading them for the nearest distribution location if the files are available in `CacheDir`.

Values / Range:	String, any location on a local hard drive
Default value:	<code>\$(CommonAppDataFolder)\ManageSoftCorp\ManageSoft\PeerCache</code>
Example value:	<code>C:\ManageSoft\SharedFiles</code>

Command-line

Tool:	Peer download agent
Example:	<code>-debug -o CacheDir="C:\ManageSoft\MyPeerCache"</code>

Registry

Installed by:	Manual configuration



User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Downloader
Computer setting:	[Registry]\ManageSoft\Downloader

CatalogName

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

This setting specifies the name of the peer download file which records files required by the managed device to complete package installation. The peer download file is stored in the parent directory of the peer cache (specified by `CacheDir`). For more information see [AllowPeerToPeer](#).

Values / Range:	String
Default value:	catalog.ctx
Example value:	peercachefiles.ctx

Command-line

Tool:	Peer download agent
Example:	-debug -o CatalogName="mycatalog.ctx"

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Downloader
Computer setting:	[Registry]\ManageSoft\Downloader

CheckCatalogDigest

Command-line | Registry | Project Variable

This setting determines whether RayManageSoft Unified Endpoint Manager performs a check on the package-level MD5 digest during the self-healing process security checking. If set to `True`, RayManageSoft Unified Endpoint Manager verifies the correctness of the implementation archive (.ndc file) by checking the MD5 digests calculated for the downloaded file against the MD5 digest stored in the package catalog. If set to `False`, RayManageSoft Unified Endpoint Manager does not check the MD5 digest of the implementation archive. A related setting for



User settings in the registry will override the machine settings unless the machine settings are locked. See [Fixing Managed Device Settings](#).

Values / Range:	Boolean (True or False)
Default value:	False

Command-line

Tool:	Installation agent
Example:	-o CheckCatalogDigest=True

Registry

Installed by:	First run of the installation agent
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	CheckCatalogDigest
Reference as:	\$(CheckCatalogDigest)

CheckCertificateRevocation

Command-line | Registry

When downloading or uploading data from an HTTPS web server, a web server certificate is applied to the data being transferred. When receiving web server certificates from the servers, RayManageSoft Unified Endpoint Manager checks the CA (certification authority) server to ensure that the certificates are not on the CRL (certificate revocation list). If RayManageSoft Unified Endpoint Manager cannot check the CRL (for example, if the CA server is firewalled and cannot be contacted), the system can stall. To avoid this, the `CheckCertificateRevocation` setting can be used to prevent RayManageSoft Unified Endpoint Manager from performing the CRL check.

This can be set as a common registry entry in order to have the same behavior occur across all RayManageSoft Unified Endpoint Manager components, respectively agents. Furthermore, it is possible to override the common behavior by setting an overriding registry entry for any component. By default, this setting is set to check the CRL for all components.

Values / Range:	Boolean (True or False)
Default value:	True



Command-line

Tool:	All agents
Example:	-o CheckCertificateRevocation=False

Registry

Installed by:	First run of the installation agent
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Common or HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\<Agent>\CurrentVersion where <Agent> is the registry key for an individual RayManageSoft Unified Endpoint Manager agent.
Computer setting:	[Registry]\ManageSoft\Common or [Registry]\ManageSoft\<Agent>\CurrentVersion where <Agent> is the registry key for an individual RayManageSoft Unified Endpoint Manager agent.

CheckFileDigest

Command-line | Registry

Determines whether RayManageSoft Unified Endpoint Manager performs a check on file-level MD5 digest during the self-healing process. If set to `True`, RayManageSoft Unified Endpoint Manager verifies the correctness of the implementation archive (.ndc file) by checking the MD5 digest of the installed file against the relevant MD5 digest stored in the RayManageSoft Unified Endpoint Manager cache on the managed device. This test is in addition to the basic checking of file presence and file size.



WARNING

Checking MD5 digests can moderately increase the time required to perform an application repair (self-heal) activity.

If `False`, RayManageSoft Unified Endpoint Manager does not check MD5 digests during self-healing.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line



Tool:	Installation agent
Example:	-o CheckFileDigest=True

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion



CheckpointSeconds

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

It specifies the frequency (in seconds) with which the peer download file is written to disk. For more information see [AllowPeerToPeer](#).

Values / Range:	Integer between 10 - 3,600
Default value:	300

Command-line

Tool:	Peer download agent
Example:	<code>-o CheckpointSeconds=500</code>

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

CheckRegistry (or Reg on the Command Line)

Command-line | Registry | Project Variable

Determines whether RayManageSoft Unified Endpoint Manager performs self-healing on registry keys and setting files. If set to `True`, the registry keys installed by the application are self-healed. If set to `False`, registry keys and setting files are not self-healed.



WARNING

This can significantly increase the time required to perform an application repair (self-heal) activity.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Installation agent



Example:	<code>-o reg=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	CheckRegistry
Reference as:	<code>\$ (CheckRegistry)</code>

CmdLineOverrides

Registry

If set to `True`, options set on the command-line override fixed settings (in the registry or in a network setting file). if set to `False`, option set on the command-line do not override fixed settings.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

CommonProgramMenuFolder

Project Variable

The path to the **Start** menu program folder and shortcuts for `[ALL USERS]`.

Values / Range:	Local directory path. Read-only!



Default value:	The default installation of Windows uses the [ALL USERS PROFILE]\Start Menu\Programs folder. For Windows 7, 8, and 10 the path defaults to: C:\ProgramData\Microsoft\Windows\Start Menu\ Programs For Windows Vista the path defaults to: C:\Documents and Settings\Public\Start Menu\ Programs For Windows 2000/XP the path defaults to: C:\Documents and Settings\All Users\Start Menu\ Programs For Windows NT the path defaults to: C:\Winnt\Profiles\All Users\Start Menu\ Programs
Example value:	C:\ProgramData\Microsoft\Windows\Start Menu\ Programs

Project Variable

Define as:	Predefined within Windows
Reference as:	\$(CommonProgramMenuFolder)

Compress (Application Usage Agent)

Command-line | Registry

Specifies whether or not application usage data files are compressed before being uploaded to the administration server for inclusion in the database. If set to `True`, RayManageSoft Unified Endpoint Manager compresses the application usage data file for upload. If set to `False`, RayManageSoft Unified Endpoint Manager leaves the application usage data file uncompressed.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>

Command-line

Tool:	Application usage agent
Example:	<code>-o Compress=False</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	Not available



Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion



Compress (Inventory Agent)

Command-line | Registry

Specifies whether or not inventory data files are compressed before being uploaded to the administration server for inclusion in the database. If set to `True`, RayManageSoft Unified Endpoint Manager compresses the inventory data file for upload. If set to `False`, RayManageSoft Unified Endpoint Manager leaves the inventory data file uncompressed.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>

Command-line

Tool:	Inventory agent
Example:	<code>-o Compress=False</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	Not available
Computer setting:	<code>[[Registry]\ManageSoft\Tracker\CurrentVersion</code>

ComputerDomain

Registry | Project Variable

The domain name of the managed device.

Values / Range:	The canonical domain name of the managed device. Read-only!
Default value:	The default value is retrieved from Windows
Example value:	<code>mycompany.com</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common</code>



Computer setting:	[Registry]\ManageSoft\Common

Project Variable

Define as:	Predefined on operating systems supporting Active Directory.
Reference as:	\$(ComputerDomain)

ComputerDNSName

Project Variable

The DNS name assigned to the managed device.

Values / Range:	The fully-qualified domain name of the managed device.
Default value:	\$(ComputerName) .\$(ComputerDomain)
Example value:	mycomputer.mycompany.com

Project Variable

Define as:	Predefined on operating systems supporting Active Directory.
Reference as:	\$(ComputerDNSName)

ConfigFile

Command-line | Registry

Identifies the system copy of the configuration file used by the package selection agent on managed devices. This does not point to the configuration file of the end-user. This is automatically (re)created from this system copy, but only if the copy has a different version number. The configuration file determines both, the skin (user interface design) and the localization of the selection agent.

	Be aware: Setting the value on the command-line will cause it to be written to the <code>HKEY_CURRENT_USER</code> hive of the registry in order to start the same <code>skin/locale</code> next time the selection agent is used.

Setting the value on the command-line to a non-empty but invalid value will clear the registry setting again.

Values / Range:	Any path to a valid RayManageSoft Unified Endpoint Manager



	configuration file
Default value:	<code>\$(ConfigFileDefault)</code>
Example value:	<code>C:\Program Files\ManageSoft\Selector\Skins\MySkin\DE\config.xml</code>

Command-line

Tool:	Package selection agent
Example:	<code>-o ConfigFile="C:\Program Files\ManageSoft\Selector\Skins\Default\DE\default.xml"</code>

Registry

Installed by:	Manual configuration or by the selection agent storing a value set on the command-line.
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Selector\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Selector\CurrentVersion</code>

ConfigFileDefault

Command-line | Registry

Identifies the system copy of the default configuration file used by the package selection agent on managed devices. This configuration file will be used whenever the selection agent cannot find a configuration file in paths defined by the local settings of the end-user or by the `ConfigFile` setting.



Be aware:

Setting the value on the command-line does not cause it to be written to the registry. Be cautious about replacing the default value with a literal as this will negate the effects of other preference setting show in the default value.

Values / Range:	Any path and filename of a valid RayManageSoft Unified Endpoint Manager configuration file
Default value:	<code>\$(SkinsDirectory)\Default\\$(Locale)\\$(ConfigName)</code>
Example value:	<code>C:\Program Files\ManageSoft\Selector\Skins\MySkin\DE\config.xml</code>

Command-line



Tool:	Package selection agent
Example:	<code>-o ConfigFile="C:\Program Files\ManageSoft\ Selector\Skins\Default\DE\default.xml"</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Selector\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Selector\CurrentVersion

ConfirmSharedFileRemoval

Command-line | Registry | Project Variable

Only applicable if `UserInteractionLevel` is set to `Full`.

When set to `True`, RayManageSoft Unified Endpoint Manager displays a dialog when removing a file that has a reference-count value greater than zero. When set to `False`, RayManageSoft Unified Endpoint Manager does not display a dialog.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>

Command-line

Tool:	Installation agent
Example:	<code>-o ConfirmSharedFileRemoval=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	<code>ConfirmSharedFileRemoval</code>
Reference as:	<code>\$(ConfirmSharedFileRemoval)</code>



ConnectionAttempts

Command-line | Registry | Project Variable

When RayManageSoft Unified Endpoint Manager is trying to connect to a particular distribution location, this setting specifies how many time it will accept a **no connection is available** error before discarding the distribution location from the list of available locations. The no connection is available condition is only detected when using file-share as the connection protocol and occurs when the number of active connections to a file share reaches the maximum allowed. This setting is not relevant for the distribution locations that are accessed via HTTP, HTTPS, or FTP. Also see [NetworkRetries](#).

Values / Range:	Numeric
Default value:	2

Command-line

Tool:	Installation agent
Example:	-o ConnectionAttempts=100

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	ConnectionAttempts
Reference as:	\$(ConnectionAttempts)

Difference

Command-line | Registry

If set to `True`, the inventory agent will perform differential inventories rather than full inventories until the maximum number of differential inventories has been performed (defined in [GenerationMax](#)). RayManageSoft Unified Endpoint Manager will then perform a full inventory and restart the differential inventories. See the [IncrementalDiff](#) setting entry for details about the type of differential inventories that will be created. If set to `False`, the inventory agent will always perform full inventories.

**Be aware:**

By default the inventory agent gathers full inventories and it is recommended to **not** alter this. The full inventories process is considerably faster than the differential inventories.

Values / Range:	Boolean (True or False)
Default value:	False

Command-line

Tool:	Inventory agent
Example:	-o Difference=False

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

Disabled (Application Usage Agent)

Command-line | Registry

Specifies whether the application usage agent is inactive on this managed device (same name is used by the schedule agent). If set to **True**, RayManageSoft Unified Endpoint Manager does not record application usage data. If set to **False**, RayManageSoft Unified Endpoint Manager records application usage data.

Values / Range:	Boolean (True or False)
Default value:	False

Command-line

Tool:	Application usage agent
Example:	-o Disabled=False

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager usage agent on a managed device (Computer setting)



User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

DisablePackageFiltering

Registry

If set to `True`, `DisablePackageFiltering` improves the performance of client-side policy merging in cases where package-level filtering is not used. When performing a policy merge, RayManageSoft Unified Endpoint Manager loads each policy (not necessarily each package) and determines its package-level filtering requirements. This setting instructs RayManageSoft Unified Endpoint Manager to skip that process by assuming there is no package-level filtering applied to the packages.



Be aware:

Only set this option if it is ensured that package-level filtering is not used and will not be used.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	No default in registry; default behavior is <code>False</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting; must be manually set in <code>mgsetup.ini</code>).
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Policy Client\ CurrentVersion

DisablePeriod

Command-line | Registry

Specifies the number of seconds for which RMS UEM AppCenter user schedules remain disabled. The default value is 3,600 seconds (one hour). If set to `3600`, RayManageSoft Unified Endpoint Manager schedules are automatically enabled again after one hour.

Values / Range:	Integer between 0 - 2,147,493,647
Default value:	3600



Command-line

Tool:	Scheduling agent
Example:	-o DisablePeriod=600

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Schedule Agent\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Schedule Agent\ CurrentVersion

DiskAveragingTime

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`). This setting is used in conjunction with `DiskMaxRate` to limit disk I/O operations activities associated with updating the peer cache and sharing files with peer managed devices. These operations include:

- Downloads from distribution servers.
- Transfers to and from peers.
- Internal copying of files to the peer cache when duplicate versions of a file are requested.

`DiskAveragingTime` specifies the average period (in minutes) used to smooth the estimate of transfers to and from disk. See [DiskMaxRate](#) for details about how these settings are used together. Increasing the value of this setting means that the estimate takes longer to change as the actual transfer rate changes. In normal use, no change of this value will be needed. RayManageSoft Unified Endpoint Manager retrieves the value for this setting from the registry every five seconds. It is not necessary to restart RayManageSoft Unified Endpoint Manager on a managed device after changing the value of this setting.

Values / Range:	Integer between 0 - 60
Default value:	2

Command-line

Tool:	Peer download agent
Example:	-debug -o DiskAveragingTime=10



Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

DiskMaxRate

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`). It specifies the maximum allowable rate (in bytes per second) for all disk I/O activities associated with updating the peer cache and sharing files with peer managed devices. `DiskMaxRate` is used in conjunction with `DiskAveragingTime` to limit disk I/O operations. RayManageSoft Unified Endpoint Manager calculates the sum of disk reads and writes that have occurred to update the peer cache and share files with peer managed devices:

- Downloads from distribution servers.
- Transfers to and from peers.
- Internal copying of files to the peer cache when duplicate versions of a file are requested.

It does not include the very small amounts of disk I/O associated with saving the peer download file. Since disk transfers occur in blocks and not as a continuous stream, RayManageSoft Unified Endpoint Manager smooths out the variation in transfer rates, using the `DiskAveragingTime` and a simple exponential decay algorithm. The result is an estimate of the disk transfer rate. Transfer rates will be decreased if the estimated rate exceeds the specified `DiskMaxRate` and increased if they are below the specified `DiskMaxRate` (Transfers can creep up to the `DiskMaxRate`, but will drop back rapidly when the estimate rate is greater than the `DiskMaxRate`). RayManageSoft Unified Endpoint Manager retrieves the value for this setting from the registry every five seconds. It is not necessary to restart RayManageSoft Unified Endpoint Manager on a managed device after changing the value of this setting.

Values / Range:	Integer between 1,024 - 134,217,728
Default value:	134217728

Command-line

Tool:	Peer download agent
Example:	<code>-debug -o DiskMaxRate=2048</code>

Registry

Installed by:	Manual configuration
User setting:	Not available



Computer setting:	[Registry]\ManageSoft\Downloader

DiskReservedKB

Command-line | Registry | Project Variable

The amount of disk space reserved on each drive. When checking whether there is enough disk space to install the application, RayManageSoft Unified Endpoint Manager attempts to leave this amount free on each drive to which it is installing files.

If there will be less than this amount of free space after the installation of the application is completed:

- If `UserInteractionLevel` is set to `Full`, RayManageSoft Unified Endpoint Manager prompts the end-user to determine whether or not to continue with the installation. If the end-user elects to not proceed (default choice), the installation fails.
- If `UserInteractionLevel` is set to any other value but `Full`, the installation fails.

Values / Range:	Integer between 1 - 1,000,000,000
Default value:	1024

Command-line

Tool:	Installation agent
Example:	-o DiskReservedKB=2048

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	DiskReservedKB
Reference as:	\$(DiskReservedKB)

DisplayAllAuthcode

Command-line | Registry | Project Variable

Only applicable when `UserInteractionLevel` is set to `Full`.



Determines the behavior when RayManageSoft Unified Endpoint Manager performs an authentication check and encounters an invalid signature. If set to `True`, the installation agent operation fails without alerting the user. If set to `False`, RayManageSoft Unified Endpoint Manager displays a dialog to allow the user to choose whether to continue with the installation agent operation or not.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Installation agent
Example:	<code>-o DisplayAllAuthCode=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	<code>DisplayAllAuthcode</code>
Reference as:	<code>\$(DisplayAllAuthcode)</code>



EmbedFileContentDirectory

Command-line | Registry

This option is Windows only!

`EmbedFileContentDirectory` specifies folders that must be scanned in search for ISO/IEC 19770-2 software



Note:

Subfolders may be included, based on the value of `Recurse` (which defaults to `true`). When recursion is needed, specific subfolders may also be excluded (see `ExcludeEmbedFileContentDirectory`).

Values / Range:	Any valid folder path. Multiple paths may be specified with a semi-colon separator (;) between them.
Default value:	"%ProgramData%,%ProgramFiles%,%PROGRAMFILES(x86)%" This default value applies on Windows platforms when the registry key is not present and the option is not specified in the command-line. Be aware: If the registry key is present but has a null value (or the option is given in the command-line but without a value), scanning for SWID tags is turned off. Note: On UNIX-like platforms there is no default path scanned. To embed ISO tag files on these platforms, paths in this preference can be specified by either using a command-line or in the co-located <code>ndtrack.ini</code> file that holds preferences for <code>ndtrack.sh</code>.

Command-line

Tool:	Inventory agent
Example:	<code>-o EmbedFileContentDirectory="C:\Program Files (x86) "</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Tracker\CurrentVersion</code>



Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

EmbedFileContentExtension

Command-line | Registry

`EmbedFileContentExtension` defines the file extension(s) that must be matched for a small text file (by design, an ISO tag file) to be embedded with the upload inventory (.ndi) file.

Values / Range:	Any valid file extension, including the leading dot or period character. Multiple file extensions may be included, separated by the semicolon character.
Default value:	swidtag

Command-line

Tool:	Inventory agent
Example:	-o EmbedFileContentExtension="swidtag;swtag"

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp \ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

EmbedFileContentSize

Command-line | Registry

`EmbedFileContentSize` specifies an upper file size limit in bytes for text files (such as ISO tag files) that are to be included/embedded in the uploaded inventory (.ndi) file.

Values / Range:	Any valid integer which is interpreted as bytes.
Default value:	1000000 This default is approximately equivalent to one Megabyte.

Command-line

Tool:	Inventory agent



Example:	<code>-o EmbedFileContentSize="1024"</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

EnablePolicyFailOver

Command-line | Registry

This setting only applies if client-side policy is enabled (`PolicySource=Client`).

When set to `True`, if a client-side policy file cannot be accessed, RayManageSoft Unified Endpoint Manager instead uses a server-side policy file if one is available. The server-side policy is applied as normal with one exception: no applications will be uninstalled, even if they are no longer in the policy and marked to be removed when no longer in the policy. Using server-side policy is a one-off event. The `PolicySource` setting remains unchanged. When set to `False`, no policy will be applied if a client-side policy file is not available.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Installation agent
Example:	<code>-o Enable PolicyFailOver=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion



EnableSessionLogging

Registry

Determines whether the following events are recorded in the application usage log:

- A session starts or ends for any application identified by the native package format (.msi, .rpm, or .pkg), the Manual Mapper registry, **Add/Remove programs**, or RayManageSoft Unified Endpoint Manager packages.
- A session starts or ends for applications not identified by the above mechanisms.
- A session ends for an identified application if the session is shorter than the minimum run time in seconds (see [MinRunTime](#)).

If set to `True`, these events are logged. If set to `False`, these events are not logged.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Usage Agent\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

EventNetType

Command-line | Registry

This setting is only applicable for Windows devices.

Events that are set to execute only when the network is available. This entry can be used to identify the type of network to look for using one of the following settings:

- 1: Local area network (LAN)
- 2: Wide area network (WAN)
- 3: Either a LAN or a WAN

For example: If an event has been configured to **Only run if a network connection is available** and `EventNetType = 1`, at the time the event is scheduled to run, the scheduling agent will check for a LAN connection before running the event and skip the event if the connection is not present at that time.



Value / Range:	1, 2, or 3
Default value:	3

Command-line

Tool:	Scheduling agent
Example:	-o EventNetType=1

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Schedule Agent\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Schedule Agent\ CurrentVersion

ExcludeDirectory

Command-line | Registry

Excludes a specified folder from the inventory. If `Recurse` is `True`, then all subfolders are also excluded. This setting can accept multiple values. If a folder is identified in both, the `ExcludeDirectory` and the `IncludeDirectory` settings, it is excluded. Exclusions always override inclusions. For more information, refer to [How RayManageSoft Unified Endpoint Manager Uses Inventory Inclusion and Exclusion Settings](#).

Values / Range:	Valid folders
Default value:	{empty}
Example value:	\$(WinDirectory)

Command-line

Tool:	Inventory agent
Example:	-o Excludedirectory=C:\Temp

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Tracker\CurrentVersion



Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

ExcludedMGSs

Command-line | Registry

This setting can accept multiple values. It allows for the exclusion of specific RayManageSoft Unified Endpoint Manager installed executable from the application usage process list. Once excluded, no application usage data will be recorded for these application.

Values / Range:	Semicolon separated list
Default value:	{empty}
Example value:	acrobat;office

Command-line

Tool:	Application usage agent
Example:	-o ExcludedMGSs="acrobat;office"

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager usage agent on a managed device
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\CurrentVersion

ExcludedMSIs

Command-line | Registry

This setting is only applicable for Windows devices.

This setting can accept multiple values. It excludes specific native package format (MSI) applications from having application usage data recorded. Once excluded, no application usage data will be recorded from these applications.

Values / Range:	Valid application names
Default value:	RayManageSoft Unified Endpoint Manager for managed devices product code GUID



Example value:	{00000409-78E1-11D2-B60F-006097C998E7}

Command-line

Tool:	Application usage agent
Example:	-o ExcludeMSIs= "{00000409-78E1-11D2-B60F-006097C998E7}"

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager usage agent on a managed device
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

ExcludeEmbedFileContentDirectory

Command-line | Registry

`ExcludeEmbedFileContentDirectory` identifies a subpath within the current search target (declared in `EmbedFileContentDirectory`) that must be excluded from scanning for ISO tag files.

Values / Range:	One (or more) folder(s) to be excluded from the search path scanned for ISO tag files to embed in the uploaded inventory (.ndi) file. Multiple paths should be separated by the semi-colon character.
Default value:	{empty}

Command-line

Tool:	Inventory agent
Example:	-o ExcludeEmbedFileContentDirectory ="C:Program Files (x86)\Adobe"

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp \ManageSoft\Tracker\CurrentVersion
Computer setting:	[REGISTRY]\ManageSoft\Tracker\CurrentVersion



ExcludeExtension

Command-line | Registry

For files within a folder included in an inventory, RayManageSoft Unified Endpoint Manager excludes files with the specified extension from the inventory. If set to the value * (**asterisk**), it excludes all files. This setting can accept multiple values. For more information, refer to [How RayManageSoft Unified Endpoint Manager Uses Inventory Inclusion and Exclusion Settings](#).

Values / Range:	File extensions (no period required)
Default value:	{empty}
Example value:	DLL

Command-line

Tool:	Inventory agent
Example:	-o ExcludeExtension=dll

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion



ExcludeFile

Command-line | Registry

For files within a folder included in an inventory, RayManageSoft Unified Endpoint Manager excludes a specific file from the inventory. This setting can accept multiple values. For more information, refer to [How RayManageSoft Unified Endpoint Manager Uses Inventory Inclusion and Exclusion Settings](#).

Values / Range:	Valid file names
Default value:	{empty}
Example value:	myfile.txt

Command-line

Tool:	Inventory agent
Example:	-o ExcludeFile=myfile.txt

Registry

Installed by:	Manual configuration
User setting:	HKEY_HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

ExcludeFileSystemType

Command-line | Registry

This option is non-windows only!

For UNIX-like devices, `ExcludeFileSystemType` allows to prevent inventory collection from specific types of file systems that may otherwise be included (This preference is not applicable to Microsoft Windows).

This file system blacklist is complemented by a whitelist in `IncludeFileSystemType`.

**Note:**

If a file system type is specified in both lists, the exclude has priority!

Keep in mind the potential interaction between the following preferences:

- `IncludeDirectory`
- `IncludeNetworkDrives`



- `IncludeFileSystemType` and `ExcludeFileSystemType` (on UNIX-like systems only).

Of these, `IncludeDirectory` has the lowest priority, and priority increases down the list. This means that on UNIX-like systems, `IncludeFileSystemType` (the highest priority) can be an exception to the general rule that "exclude overrides include".

Values / Range:	Comma-separated list of standard file system names, as recognized by the UNIX mount command. Either omit white space or enclose the list in double quotation marks.
Default value:	No default value in [Registry] and no default behavior (equivalent to a default value of "").

Command-line

Tool:	Inventory agent
Example:	<code>-o ExcludeFileSystemType=zfs</code>

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp \ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

ExcludeMD5

Command-line | Registry

For files within a folder included in an inventory, RayManageSoft Unified Endpoint Manager excludes an MD5 checksum and excludes any files from the inventory that have an MD5 value equal to the value stored in this setting. This setting can accept multiple values. For more information, refer to [How RayManageSoft Unified Endpoint Manager Uses Inventory Inclusion and Exclusion Settings](#).

Values / Range:	Valid MD5 value
Default value:	{empty}
Example value:	7d9d2440656fdb3645f6734465678c60

Command-line

Tool:	Inventory agent
Example:	<code>-o ExcludeMD5=7d9d2440656fdb3645f6734465678c60</code>



Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Tracker\CurrentVersion
Computer setting:	Registry\ManageSoft\Tracker\CurrentVersion

ExcludePermissionsMask

Command-line | Registry

This option is non-windows only!

This setting specifies which files should not be scanned during a RMS UEM AppCenter inventory. The value should be an octal mask for the file permissions in the format used by the `chmod` command. Files which match this mask will be excluded from the scan. If an exclamation is added before the mask, the files which do **not** match this mask will be excluded from the scan.

Values / Range:	Octal value in the format used for <code>chmod</code>
Default value:	{empty}
Example value:	0777 This value will cause the reporting of every file (not recommended for performance reasons).

Command-line

Tool:	Inventory agent
Example:	-o ExcludePermissionsMask=0113

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals, managed device settings package or manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

ForceReboot

Command-line | Registry

`RebootIfRequired` is responsible for end-user prompts about a required reboot. If `ForceReboot` is `True` and the default response to the prompt dialog is to reboot, the prompts



are modified to prevent the end-user from vetoing a reboot.

This setting determines the type of reboot (forced or polite) initiated by RayManageSoft Unified Endpoint Manager after that prompt:

- If set to `True`, RayManageSoft Unified Endpoint Manager performs a forced reboot. This suppresses any user interaction required to close down other applications that may be running which means that unsaved work may be lost.
- If set to `False`, RayManageSoft Unified Endpoint Manager performs a polite reboot. This offers end-users the opportunity to save work and close down other applications before continuing with the reboot.

If the desktop is locked, the installation and the adoption agent use `ForceRebootIfLocked` instead of `ForceReboot`. For details about how this setting works in combination with other installation settings to determine the appropriate reboot action, see [Reboot Options](#).

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Installation agent, adoption agent
Example:	<code>-o ForceReboot=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Launcher\CurrentVersion</code>

ForceRebootIfLocked

Command-line | Registry

`AllowRebootIfLocked` is responsible for end-user prompts about a required reboot if the desktop is locked. If `ForceRebootIfLocked` is `True` and the default response to the prompt dialog is to reboot, the prompts are modified to prevent end-user from vetoing a reboot.

`ForceRebootIfLocked` determines the type of reboot (forced or polite) initiated by RayManageSoft Unified Endpoint Manager after that prompt:

- If set to `True`, RayManageSoft Unified Endpoint Manager performs a forced reboot. This



suppresses any user interaction required to close down other applications that may be running which means that unsaved work may be lost.

- If set to `False`, RayManageSoft Unified Endpoint Manager performs a polite reboot. This offers end-users the opportunity to save work and close down other applications before continuing with the reboot.

For details about how this setting works in combination with other installation settings to determine the appropriate reboot action, see [Reboot Options](#).

Values / Range:	Boolean (True or False)
Default value:	True

command-line

Tool:	Installation agent, adoption agent
Example:	<code>-o ForceRebootIfLocked=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

ForceSharedFileRemove

Command-line | Registry | Project Variable

Allows forced deletion of redundant files in the Windows system folder. By default, when files in a package are marked as redundant, after the installation they are deleted on the managed device. However, because files within the Windows system folder may be shared by other packages, they are not deleted. `ForceSharedFileRemove` allows for the deletion of these files.

If `True`, redundant files within the Windows system folder are deleted when the other redundant files in a package are deleted. If `False`, files in the Windows system folder are not deleted. This setting also determines the default response to keeping shared files during the uninstallation of packages. If `True`, the default response is to not keep the files. If `False`, the default response is to keep the shared files.



Be aware:

To control this behavior for a single package, it must be set as a project variable in the package (Registry entries stored in a package are only set after the installation of the package).



Values / Range:	Boolean (True or False)
Default value:	False

Command-line

Tool:	Installation agent
Example:	-o ForceSharedFileRemove=True

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	ForceSharedFileRemove
Reference as:	\$(ForceSharedFileRemove)

ForceValidSignature

Command-line | Registry | Project Variable

When testing whether a package should be installed, the installation agent uses Authenticode technology to validate a digital signature. If the signature is invalid, the installation agent examines this setting. If set to **True**, the installation stops and the end-user is informed of the failure. If set to **False**, RayManageSoft Unified Endpoint Manager displays a Microsoft dialog that informs about the failure but asks the end-user if they want to proceed anyway. This practice is not recommended.

A related setting for User settings in the registry will override the machine settings unless the machine settings are locked. See [Fixing Managed Devices Settings](#).

Values / Range:	Boolean (True or False)
Default value:	False

Command-line

Tool:	Installation agent



Example:	<code>-o ForceValidSignature=True</code>

Registry

Installed by:	First run of installation agent
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	ForceValidSignature
Reference as:	<code>\$(ForceValidSignature)</code>



GCDiskSlice

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

It specifies the percentage of `DiskMaxRate` that can be used for checking the consistency of the peer cache and cleaning up files that are no longer required in it.

Values / Range:	Integer between 1 and 50
Default value:	2

Command-line

Tool:	Peer download agent
Example:	<code>-debug -o GCDiskSlice=24</code>

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

GCMaxInterval

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

It specifies the maximum number of minutes the peer download agent should pause between examining files in the peer cache for cleanup. This setting is used in conjunction with `GCMinInterval` and `GCPeriod`. `GCMaxInterval` takes precedence over `GCPeriod`. The peer download agent will not increase the time interval between examining files in the peer cache, even if that means, it will examine all files in the peer cache more than once within the period specified by `GCPeriod`.

Values / Range:	Integer between 10 and 1.440
Default value:	60

Command-line



Tool:	Peer download agent
Example:	-debug -o GCMaxInterval=720

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

GCMinInterval

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (AllowPeerToPeer is True).

It specifies the minimum number of minutes the peer download agent should pause between examining files in the peer cache for cleanup. This setting is used in conjunction with GCMinInterval and GCPeriod. GCMaxInterval takes precedence over GCPeriod. The peer download agent will not examine files more frequently than specified by this setting, even if this means, that it will not examine all files in the peer cache within the period specified by GCPeriod.

Values / Range:	Integer between 10 and 600
Default value:	60

Command-line

Tool:	Peer download agent
Example:	-debug -o GCMinInterval=20

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

GCPeriod

Command-line | Registry



This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

It specifies the number of hours which the RayManageSoft Unified Endpoint Manager peer download agent attempts to visit all files in the peer cache as part of the cleaning up operations. The default is to attempt to examine and clean up unused files from the peer cache for a period of 12 hours. This minimizes the impact on the end-user of the managed device.

Once started, the cleanup operation continues while the managed device is on. `GCPeriod` is used to help determine the time interval at which files in the peer cache are examined by cleanup operations. It is used in conjunction with `GCMinInterval` (which specifies the minimum number of minutes the peer download agent should pause between examining files in the peer cache) and `GCMaxInterval` (which specifies the maximum number of minutes the peer download agent should pause between examining files in the peer cache).

Both, `GCMaxInterval` and `GCMinInterval`, take precedence over `GCPeriod`. Files will not be examined more frequently than at the intervals allowed by `GCMinInterval` and `GCMaxInterval`, even if it means that not all files in the peer cache will be examined in the period specified by `GCPeriod`.

Values / Range:	Integer between 1 and 744
Default value:	12

Command-line

Tool:	Peer download agent
Example:	<code>-debug -o GCPeriod=20</code>

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

GenerateMD5

Command-line | Registry

Specifies whether or not to calculate the MD5 digest of any file being tracked by the inventory agent and include it with the stored inventory data. MD5 digests, if included in the inventory, are used as key to uniquely identify files. If an MD5 is not present, files are identified by date and file size. MD5 digests are more reliable for this purpose, but be aware that calculating MD5 digests will degrade the performance where many files are being tracked.



This use of MD5 digests is unrelated to the comparison completed by the installation agent prior to downloading and installing files.

Values / Range:	Boolean (True or False)
Default value:	False

Command-line

Tool:	Inventory agent
Example:	-o GenerateMD5=True

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

GenerationMax

Command-line | Registry

This only applies if differential inventories are being used (Difference is True).

Defines the number of differential inventories that may take place before a full inventory is performed.

Values / Range:	Integer between 1 - 1,000,000,000
Default value:	9 (every 10th inventory is a full inventory)

Command-line

Tool:	Inventory agent
Example:	-o GenerationMax=5

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Tracker\CurrentVersion



Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

GlobalConfigSource

Registry

Points the RayManageSoft Unified Endpoint Manager installation agent to **URL** or **UNC** path on the network that contains installation settings. These settings are stored in the .ini file format.

Values / Range:	Valid URL or UNC Path
Default value:	No default
Example value:	UNC: \\server\share\path\network.ini URL: http://server/share/path/network.ini

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Hardware

Command-line | Registry

This setting is only effective when running in machine context.

Allows to track hardware by either using Windows Management Instrumentation (WMI) or native APIs. If WMI is available, it is used for tracking.

If set to `True`, it allows the tracking of hardware inventory. If set to `False`, it does not track hardware inventory.

Values / Range:	Boolean (True or False)
Default value:	<code>True</code>

Command-line

Tool:	Inventory agent
Example:	<code>-o Hardware=False</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual



	configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

HideMachineUI

Command-line | Registry

If set to `True`, RayManageSoft Unified Endpoint Manager does not display a user interface when applying a machine policy.

**WARNING**

Do not edit! Setting this entry to `False` could result in hidden dialog boxes while requiring user input!

Values / Range:	Boolean (True or False)
Default value:	True

Command-line

Tool:	Scheduling agent
Example:	-o HideMachineUI=False

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed machine (Computer setting)
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Schedule Agent\CurrentVersion

HighestPriority

Registry

Specifies the highest upload/download priority that can be assigned to a distribution server. The lower the number, the higher the priority. When assigning priorities, RayManageSoft Unified Endpoint Manager normalizes the calculated priority to fit within the range identified by `HighestPriority` and `LowestPriority`. The highest priority is commonly set to 1.

Values / Range:	Recommended 1-100 (but can extend from -231 to 231)



Default value:	No default in registry; default behavior uses 10.
Example value:	10

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\NetSelector\CurrentVersion
Computer setting:	[[Registry]\ManageSoft\NetSelector\ CurrentVersion

Http_proxy

Command-line | Registry | Project Variable

Proxy settings for the RayManageSoft Unified Endpoint Manager installation agent.

Values / Range:	Any valid URL
Default value:	Not to use a proxy
Example value:	tmnis.com;tmnis.com.de

Command-line

Tool:	Installation agent
Example:	-o http_proxy=tmnis.com;tmnis.com.de

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	http_proxy
Reference as:	\$(http_proxy)



IgnoreConnectionWindows

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

If set to `True`, settings of `ParentConnectionWindows` and `PeerConnectionWindows` are ignored. This means, that managed devices can connect to distribution servers and peers at any time.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Installation agent
Example:	<code>-o IgnoreConnectionWindows=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	Not available
Computer setting:	<code>[Registry]\ManageSoft\Common</code>



IncludeDirectory

Command-line | Registry

Includes a specific folder to the inventory. If `Recurse` is `True`, then all subfolders are also included. If the value of this entry is set to "\", it means that all folders are included. This setting can accept multiple values.

If a folder is defined in both, the `ExcludeDirectory` and `IncludeDirectory` settings, it is excluded. Exclusions always override inclusions. For more information, refer to [How RayManageSoft Unified Endpoint Manager Uses Inventory Inclusion and Exclusion Settings](#).

Values / Range:	Valid folder
Default value:	{empty}
Example value:	C:\Program Files

Command-line

Tool:	Inventory agent
Example:	-o IncludeDirectory=C:\Temp

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

IncludeExtension

Command-line | Registry

For files within a folder included in an inventory, RayManageSoft Unified Endpoint Manager includes files with the specified extension from the inventory. If set to the value * (**asterisk**), it includes all files. This setting can accept multiple values. For more information, refer to [How RayManageSoft Unified Endpoint Manager Uses Inventory Inclusion and Exclusion Settings](#).

Values / Range:	File extensions (no period required)
Default value:	{empty}
Example value:	bat



Command-line

Tool:	Inventory agent
Example:	-o IncludeExtension=exe

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

IncludeFile

Command-line | Registry

For files within a folder included in an inventory, RayManageSoft Unified Endpoint Manager includes a specific file from the inventory. This setting can accept multiple values. For more information, refer to [How RayManageSoft Unified Endpoint Manager Uses Inventory Inclusion and Exclusion Settings](#).

Values / Range:	Valid file names
Default value:	{empty}
Example value:	myfile.txt

Command-line

Tool:	Inventory agent
Example:	-o IncludeFile=myfile.txt

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion



IncludeFileSystemType

Command-line | Registry | Project Variable

This option is non-windows only!

For UNIX like devices, `IncludeFileSystemType` allows to include specific types of file systems that may otherwise be excluded (this preference is not applicable to Microsoft Windows).

The `.ufs`, `.zfs`, and `.lofs` file systems use virtual device notes (within the operating system) rather than listing their drives as physical `/dev/...` services. This makes it more difficult to determine whether they are local or remote file systems and they would therefore logically be excluded when `IncludeNetworkDrives=False` (the default). When these file systems are running locally on a UNIX-like device, this setting allows for the exclusion of network drives and still allows for inventory collection from the local file system by nominating the file system type(s).

This file system whitelist is completed by a blacklist in `ExcludeFileSystemType`.



Note:

If a file system type is specified in both lists, the exclude has priority.

Keep in mind the potential interaction between the following preferences:

- `IncludeDirectory`
- `IncludeNetworkDrives`
- `IncludeFileSystemType` and `ExcludeFileSystemType` (on UNIX like systems only).

Of these, `IncludeDirectory` has the lowest priority and the priority increases down the list. This means that on UNIX like systems, `IncludeFileSystemType` (the highest priority) can be an exception to the general rule that "exclude overrides include".

Values / Range:	Comma-separated list of standard file system type names, as recognized by the UNIX mount command. Either omit white space or enclose the list in double quotation marks.
Default value:	No default value in [Registry]. If no value is specified in the registry or the command-line, the default behavior is <code>.ufs, .zfs, .lofs</code> .

Command-line

Tool:	Inventory agent
Example:	<code>-o IncludeFileSystemType=ufs,lofs</code>

Registry

Installed by:	Manual configuration



User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp \ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

IncludeMD5

Command-line | Registry

For files within a folder included in an inventory, RayManageSoft Unified Endpoint Manager includes a specific MD5 digest. For more information, refer to [How RayManageSoft Unified Endpoint Manager Uses Inventory Inclusion and Exclusion Settings](#).

Values / Range:	Valid MD5 value
Default value:	{empty}
Example value:	7d9d2440656fdb3645f6734465678c60

Command-line

Tool:	Inventory agent
Example:	-o IncludeMD5=7d9d2440656fdb3645f6734465678c60

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ \ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

IncludeRegistryKey

Command-line | Registry

This option is Windows only!

This setting is set in order to instruct the inventory agent to track the specified registry keys or values. In order to collect all values under a specified key, the key path specified must end with a trailing backslash. If the path specified corresponds to a key (rather than a registry value) but does not end with a trailing backslash, only the (default) value (if set) for the specified key will be collected.

For example:

- HKLM\SOFTWARE\ManageSoft Corp\ManageSoft\ will track all values under the specified



key.

- HKLM\SOFTWARE\ManageSoft Corp\ManageSoft will only track the default values under the specified key (Note that the default values are typically not set.).

When setting this setting, the following can be used:

- The * wildcard to replace a key or value.
- The abbreviations HKLM, HKCU, HKCR, HKU, and HKCC. These will automatically expand to the appropriate values.

Values / Range:	Valid registry key or value
Default value:	If no value is specified, RayManageSoft Unified Endpoint Manager uses HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\
Example value:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\ - tracks all registry entries under this key HKEY_LOCAL_MACHINE\SOFTWARE*\ - tracks all registry keys and values under HKLM\SOFTWARE HKLM\SOFTWARE\Microsoft* - tracks all values under HKLM\SOFTWARE\Microsoft HKEY_LOCAL_MACHINE\SOFTWARE*\CurrentVersion*\ - illustrates the use of multiple wildcards

Command-line

Tool:	Inventory agent
Example:	-o IncludeRegistryKey= "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\"

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion



IncludePermissionsMask

Command-line | Registry

This setting specifies which files should be scanned during a RMS UEM AppCenter inventory. The value should be an octal mask for the file permissions in the format used by the `chmod` command. Files which match this mask will be included in the scan. If an exclamation is added before the mask, the files which do **not** match this mask will be included in the scan

Values / Range:	Octal value in the format used for <code>chmod</code>
Default value:	{empty}
Example value:	0777 This value will cause the reporting of every file (not recommended for performance reasons).

Command-line

Tool:	Inventory agent
Example:	-o IncludePermissionsMask=0113

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals, managed device settings packae or manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

IncrementalDiff

Command-line | Registry

If differential inventory is in use (`Difference=True`), then this entry determines what differences the differential inventory will collect.

- If `True`, the differential inventory will list differences from the last inventory file (which may be either differential or full).
- If `False`, the differential inventory will list differences from the last full inventory file.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line



Tool:	Inventory agent
Example:	-o IncrementalDiff=True

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

InstallationStatusRefreshPeriod

Command-line | Registry

Specifies how frequently (in seconds) RayManageSoft Unified Endpoint Manager should recreate installation events for packages that are installed and packages flagged as not required. This setting is useful if installation records have been removed on the administration server, as the recreated records on the managed devices will repopulate the records on the administration server.

Values / Range:	Integer between 0 and 31,556,926
Default value:	604800 (1 week)

Command-line

Tool:	Installation agent
Example:	-o InstallationStatusRefreshPeriod=31556926

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	In order of precedence: - HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion - HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Common
Computer setting:	In order of precedence: [Registry]\ManageSoft\Launcher\CurrentVersion [Registry]\ManageSoft\Common



InstallerARPMModify

Command-line | Registry | Project Variable

If set to `True`, details of software installed using RayManageSoft Unified Endpoint Manager external installer packages can be modified with the Microsoft **Add/Remove Programs** control panel applet. If set to `False`, these details cannot be modified within **Add/Remove Programs**. It is likely that this setting will need to be different for individual packages.



Be aware:

To control the behavior for a single package, this must be set as a project variable in the package (Registry entries stored in a package are only set after the installation of that package.).

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>

Command-line

Tool:	Installation agent
Example:	<code>-o InstallerARPMModify=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	<code>InstallerARPMModify</code>
Reference as:	<code>\$(InstallerARPMModify)</code>

InstallerARPRemove

Command-line | Registry | Project Variable

If set to `True`, software installed using RayManageSoft Unified Endpoint Manager external installer packages can be uninstalled within the Microsoft **Add/Remove Programs** control panel applet. If set to `False`, the software cannot be uninstalled within **Add/Remove Programs**. It is likely that this setting will need to be different for individual packages.

**Be aware:**

To control the behavior for a single package, this must be set as a project variable in the package (Registry entries stored in a package are only set after the installation of that package.).

Values / Range:	Boolean (True or False)
Default value:	False

Command-line

Tool:	Installation agent
Example:	-o InstallerARPRemove=True

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	InstallerARPRemove
Reference as:	\$(InstallerARPRemove)

Inventory

Registry

Instructs RayManageSoft Unified Endpoint Manager to upload inventory files from managed devices to the specified server location

**WARNING**

This setting is configured during installation and should not be altered by end-users!

Values / Range:	Valid location
Default value:	\$(ServerLocation)\Inventories\\$(MachineId).ndi



Example value:	<code>\$(ServerLocation)\Inventories\\$(UserId) on \$(MachineId) at \$(DateTime) \$(Generation).ndi</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Common\Rules
Computer setting:	[Registry]\ManageSoft\Common\Rules

InventoryDirectory

Command-line

This is the general parameter that can be set as a custom directory for the storage of inventory data by the inventory agent.



Be aware:

In case the parameter is not set, the agent takes the default value as storage location for the inventory data. For further information refer to the `MachineInventoryDirectory` and `MachineZeroTouchDirectory` settings.

Values / Range:	Valid location
Default value:	<code>Default{empty}</code>

Command-line

Tool:	Inventory agent
Example:	<code>-o InventoryDirectory=C:\Inventory</code>

InventoryFile

Command-line | Registry

Identifies the name of a local copy of the inventory file. The name may exist of Windows properties that can be expanded to identity a value. For example, the default value `$(UserName) on $(MachineId).ndi` expands in a way that the name contains the account and the machine ID related to the inventory.

Values / Range:	<code>*.ndi</code>



Default value:	<code>\$(UserName) on \$(MachineId).ndi</code>
Example value:	<code>myComputer.ndi</code>

Command-line

Tool:	Inventory agent
Example:	<code>-o InventoryFile=myfile.ndi</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Tracker\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Tracker\CurrentVersion</code>

InventoryScripts

Command-line | Registry

Specifies the scripts to run during the machine inventory. Due to its nature, this setting may be available to only a subset of the package's environments, languages, and architectures. Additionally, this setting cannot have customized values.

Values / Range:	List of script files
Default value:	<code>{empty}</code>

Command-line

Tool:	Inventory agent
Example:	n/a

Registry

Installed by:	Manual Configuration
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Tracker\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Tracker\CurrentVersion</code>



InventoryScriptsDir

Command-line | Registry

The location of scripts to be run immediately before inventory data is uploaded through the distribution hierarchy. All scripts that exist in this location are run.

Values / Range:	A valid location
Default value:	<code>\$(ScriptDir)\InventoryScanningOptionsInventoryScripts</code>
Example value:	<code>C:\LocalScripts\</code>

Command-line

Tool:	Inventory agent
Example:	<code>-o InventoryScriptDir=C:\data</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager for managed devices
User setting:	Not available
Computer setting:	<code>[Registry]\ManageSoft\Tracker\CurrentVersion</code>

LauncherCommandLine

Registry

Specifies installation agent parameters to pass to RayManageSoft Unified Endpoint Manager when applying policy information.

Values / Range:	Valid installation agent command-line parameters
Default value:	<code>{empty}</code>
Example value:	<code>-o UserInteractionLevel=Quiet</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Policy Client\CurrentVersion</code>



Computer setting:	[Registry]\ManageSoft\PolicyClient\ CurrentVersion

ListeningPort

Registry

Specifies the port number that the TCP-based listening agent monitors for incoming requests.

	Be aware: If changing the port on which managed devices are listening for jobs, it is necessary to make a corresponding change to the <code>ListeningPort</code> setting on the distribution server.

Values / Range:	Any valid port number
Default value:	7020
Example value:	9080

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\RemoteExecution\CurrentVersion
Computer setting:	[Registry]\ManageSoft\RemoteExecution\ CurrentVersion

Locale

Command-line | Registry

The local setting used by the selection agent. This setting usually reflects the value of the `UserLocale` setting but it can be manually overridden for testing purposes. Where there are alternate localizations of the user interface available, the selection agent will try to match the system setting for `locale` with the `locale` variable in the application file directory path, thereby switching to the appropriately localized user interface.

Values / Range:	Any two-character abbreviation that is valid for <code>locale</code> . For the currently valid values, check ISO 3166-1-alpha-2 code .
Default value:	\$(UserLocale)
Example value:	DE



Command-line

Tool:	Package selection agent
Example:	<code>-o Locale="DE"</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Selector\CurrentVersion
Computer setting:	[[Registry]\ManageSoft\Selector\CurrentVersion

Project Variable

Define as:	AddRemove
Reference as:	<code>\$ (AddRemove)</code>

LocaleDefault

Command-line | Registry

The local setting used by the selection agent. This setting usually reflects the value of the `UserLocale` setting but it can be manually overridden for testing purposes. Where there are alternate localizations of the user interface available, the selection agent will try to match the system setting for `locale` with the `locale` variable in the application file directory path, thereby switching to the appropriately localized user interface.

Values / Range:	Any two- or three-character abbreviation that is valid for <code>locale</code> . Any third character (representing the dialect) is ignored. For the currently valid values, check ISO 3166-1-alpha-2 code .
Default value:	EN
Example value:	DE

Command-line

Tool:	Package selection agent
Example:	<code>-o LocaleDefault="DE"</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual



	configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Selector\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Selector\CurrentVersion

Log

Registry

Instructs RayManageSoft Unified Endpoint Manager to upload log files from the managed device to the specified server location

Values / Range:	Valid location
Default value:	\$(ServerLocation)\Logs\\$(MachineId) at \$(DateTime)_\$(GUID).log
Example value:	\$(ServerLocation)\Logs\\$(MachineId) at \$(DateTime).log

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Common\Rules
Computer setting:	[[Registry]\ManageSoft\Common\Rules

LogFile (Installation Agent)

Command-line | Registry | Project Variable

Specifies the name of the file which is used to store the logging information.

Values / Range:	Local and UNC network files
Default value:	\$(TempDirectory)\ManageSoft\installation.log
Example value:	C:\temp\Installation.log

Command-line

Tool:	Installation agent
Example:	-o LogFile=C:\temp\installation.log



Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	LogFile
Reference as:	\$(LogFile)

LogFileOld (Installation Agent)

Command-line | Registry | Project Variable

When the installation agent log file reaches its maximum size (as defined in `LogFileSize` (Installation agent)), the file is renamed according to the value in `LogFileOld`. This overwrites the previous file with this name.

Values / Range:	Local and UNC network files
Default value:	\$(TempDirectory)\ManageSoft\installation.old.log
Example value:	C:\temp\Installation_old.log

Command-line

Tool:	Installation agent
Example:	-o LogFileOld=C:\temp\installation_old.log

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	LogFileOld



Reference as:	<code>\$(LogFileOld)</code>

LogFileSize (Installation Agent)

Command-line | Registry | Project Variable

When the main installation agent log file reaches its maximum size (as defined in `LogFile` (Installation agent)) reaches the size defined in `LogFileSize` (Installation agent), the file is renamed according to the value in `LogFileOld` (Installation agent). A new log file is created. By this, additional log information is being retained.

The size must be expressed as the number of bytes of the maximum allowed log size. If this entry is empty or set to zero, there is no log size limit and the size of the log file continues to grow.

Values / Range:	Numeric (number of bytes)
Default value:	524288
Example value:	3126000 (3 MB)

Command-line

Tool:	Installation agent
Example:	<code>-o LogFileSize=1024000</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion</code> • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common</code>
Computer setting:	In order of precedence: • <code>[Registry]\ManageSoft\Launcher\CurrentVersion</code> • <code>[Registry]\ManageSoft\Common</code>

Project Variable

Define as:	<code>LogFileSize</code>
Reference as:	<code>\$(LogFileSize)</code>



LogInstallCheck

Command-line | Registry

Specifies whether RayManageSoft Unified Endpoint Manager should recreate installation events while checking packages for an installation or an upgrade. If installation event records are recreated, they use the current date as the installation date. This setting is useful if installation records have been removed on the administration server. See the [How Installation Event Settings Interact](#) section for a description on how this setting interacts with others that create or update installation event records.

Values / Range:	Boolean (True or False)
Default value:	False

Command-line

Tool:	Installation agent
Example:	-o LogInstallCheck=True

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	In order of precedence: • [Registry]\ManageSoft\Launcher\CurrentVersion • [Registry]\ManageSoft\Common

How Installation Event Settings Interact

When policy is applied, the following occurs:

- If the same version of the package is already installed:
 - If LogInstallCheck is True, an installation event record is created
 - If LogInstallCheck is False, no installation event record is created
- If the same version of the package is not installed, and the package is required on this computer, installation is attempted and:
 - If installation succeeds and LogInstallPass is True, the successful installation is logged
 - If installation fails and LogInstallFail is True, the failed installation is logged



- If the same version of the package is not installed, and the package is not required for this computer:
 - If any existing version of this package is currently installed, the existing installation event record is left unchanged
 - If no existing version of this package is installed, and the package is new in policy, a “not required” installation event record is created
 - If no existing version of this package is installed, and the package is not new in policy:
 - If `InstallationStatusRefreshPeriod` is 0 or `LogNotRequiredCheck` is `True`, a “not required” installation event record is created
 - If `InstallationStatusRefreshPeriod` has a non-zero value or `LogNotRequiredCheck` is `False`, no installation event record is created.

LogInstallFail

Command-line | Registry

Specifies whether (`True`) or not (`False`) RayManageSoft Unified Endpoint Manager should log failed installation attempts. See the [How Installation Event Settings Interact](#) section for a description on how this setting interacts with others that create or update installation event records.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>

Command-line

Tool:	Installation agent
Example:	<code>-o LogInstallFail=False</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	HKIn order of precedence: • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion</code> • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common</code>
Computer setting:	In order of precedence: • <code>[Registry]\ManageSoft\Launcher\CurrentVersion</code> • <code>[Registry]\ManageSoft\Common</code>



LogInstallPass

Command-line | Registry

Specifies whether (True) or not (False) RayManageSoft Unified Endpoint Manager should log successful installation events. See the [How Installation Event Settings Interact](#) section for a description on how this setting interacts with others that create or update installation event records.

Values / Range:	Boolean (True or False)
Default value:	True

Command-line

Tool:	Installation agent
Example:	-o LogInstallPass=False

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	In order of precedence: • [Registry]\ManageSoft\Launcher\CurrentVersion • [Registry]\ManageSoft\Common

LogLevel (Installation Agent)

Command-line | Registry | Project Variable

Determines the level of logging returned by the RayManageSoft Unified Endpoint Manager installation agent. The information from this logging is send to the file which matches the name stored in the `LogFile` (installation agent) setting.

More information regarding logging and levels of logging can be found in the [Appendix II: Logging on Managed Devices](#).

Values / Range:	One or more logging levels.
Default value:	A-z (logs all)



Example value:	G0,4

Command-line

Tool:	Installation agent
Example:	-o LogLevel=G0,4

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	In order of precedence: • [Registry]\ManageSoft\Launcher\CurrentVersion • [Registry]\ManageSoft\Common

Project Variable

Define as:	LogLevel
Reference as:	\$(LogLevel)

LogonServer

Project Variable

The name of the logon server computer to which the managed device normally connects.

Values / Range:	UNC name of the domain controller that validates user logons
Default value:	Name of the logon server
Example value:	\\myserver

Project Variable

Define as:	Predefined within the Windows network configuration
Reference as:	\$(LogonServer)



LogUninstallFail

Command-line | Registry

Specifies whether (True) or not (False) RayManageSoft Unified Endpoint Manager should log failed uninstall attempts. See the [How Installation Event Settings Interact](#) section for a description on how this setting interacts with others that create or update installation event records.

Values / Range:	Boolean (True or False)
Default value:	True

Command-line

Tool:	Installation agent
Example:	-o LogUninstallFail=False

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	In order of precedence: • [Registry]\ManageSoft\Launcher\CurrentVersion • [Registry]\ManageSoft\Common

LogUninstallPass

Command-line | Registry

Specifies whether (True) or not (False) RayManageSoft Unified Endpoint Manager should log successful uninstalls. See the [How Installation Event Settings Interact](#) section for a description on how this setting interacts with others that create or update installation event records.

Values / Range:	Boolean (True or False)
Default value:	True

Command-line



Tool:	Installation agent
Example:	-o LogUninstallPass=False

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	In order of precedence: • [Registry]\ManageSoft\Launcher\CurrentVersion • [Registry]\ManageSoft\Common

LowestPriority

Registry

Specifies the highest upload/download priority that can be assigned to a distribution server. The higher the number, the lower the priority. When assigning priorities, RayManageSoft Unified Endpoint Manager normalizes the calculated priority to fit within the range identified by `HighestPriority` and `LowestPriority`. The lowest priority is commonly set to 100.

Values / Range:	Recommended 1-100 (but can extend from -231 to 231)
Default value:	99

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\NetSelector\CurrentVersion
Computer setting:	[Registry]\ManageSoft\NetSelector\CurrentVersion

LowProfile (Installation Agent, Inventory Agent)

Command-line | Registry | Project Variable

Determines the CPU priority of RayManageSoft Unified Endpoint Manager on the managed device.



- If set to `True`, RayManageSoft Unified Endpoint Manager processes run with low priority.
- If set to `False`, RayManageSoft Unified Endpoint Manager processes run with normal priority.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	No default in registry; default behavior is <code>False</code>

Command-line

Tool:	Installation agent, inventory agent
Example:	<code>-o LowProfile=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	• <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion</code> • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Tracker\CurrentVersion</code>
Computer setting:	• <code>[Registry]\ManageSoft\Launcher\CurrentVersion</code> • <code>[Registry]\ManageSoft\Tracker\CurrentVersion</code>

Project Variable

Define as:	<code>LowProfile</code>
Reference as:	<code>\$(LowProfile)</code>

MachineAlternateRegistryHive

Registry | Project Variable

Specifies an alternative registry hive to be used by the managed device during the self-update.

**Be aware:**

The default value allows RayManageSoft Unified Endpoint Manager managed device settings to be controlled by the native Active Directory Group Policy.

These default locations are not visible to end-users. Alternative registry hives have no effect on the `DownloadSettings`, `UploadSettings`, and `Rules` keys under `SOFTWARE\ManageSoft Corp\ManageSoft\Common`.

**Be aware:**

The loading sequence for the registry settings is:

- Default machine hive
(`"HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ManageSoft"`)
- Alternative machine hive
(pointed to by `MachineAlternateRegistryHive` under `HKEY_LOCAL_MACHINE`)
- Alternative user hive
(pointed by `UserAlternateRegistryHive` under `HKEY_CURRENT_USER`)

Values / Range:	Valid registry hive
Default value:	<code>SOFTWARE\Policies\ManageSoft Corp\ManageSoft</code>

Registry

Installed by:	Manual configuration
User setting:	not available
Computer setting:	<code>[Registry]\ManageSoft\Common</code>

Project Variable

Define as:	<code>MachineAlternateRegistryHive</code>
Reference as:	<code>\$(MachineAlternateRegistryHive)</code>

MachineInventoryDirectory

Command-line | Registry

The location in which to store machine inventories.

Values / Range:	Valid location
Default value:	<code>\$(CommonAppDataFolder)\ManageSoft Corp\ManageSoft\Tracker\Inventories</code>

Command-line

Tool:	Inventory agent
Example:	<code>-o MachineInventoryDirectory=C:\ManageSoft Corp\ManageSoft\Tracker\Inventories</code>

Registry



Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

MachinePolicyCommand

Command-line | Registry

The command to execute to perform an application of machine policy on the managed device.

Values / Range:	A valid command-line string containing the mgspolicy.exe
Default value:	"\$(ProgramFiles)\ManageSoft\Policy Client\mgspolicy.exe" -t Machine

Command-line

Tool:	Policy agent
Example:	"\$(ProgramFiles)\ManageSoft\Policy Client\mgspolicy.exe" -t Machine -o UserInteractionLevel=quiet

Registry

Installed by:	RayManageSoft Unified Endpoint Manager policy configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Policy Client\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Policy Client\CurrentVersion

MachinePolicyDirectory

Registry

The location used to store the current machine policy.

Values / Range:	Valid folder and path
Default value:	\$(CommonAppDataFolder)\ManageSoft Corp\ManageSoft\Policy\Client\Policies\Merged\Machine



Example value:	C:\Temp\MachinePolicies

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\NetSelector\CurrentVersion
Computer setting:	[Registry]\ManageSoft\NetSelector\ CurrentVersion

MachinePolicyPackageDirectory

Registry

The location used to cache package information associated with the machine policy.

Values / Range:	Valid folder and path
Default value:	\$(CommonAppDataFolder)\ManageSoft Corp\ ManageSoft\Policy\Client\Packages
Example value:	C:\Temp\MachinePolicies\PackageInfo

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Policy Client\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Policy Client\ CurrentVersion

MachineZeroTouchDirectory

Command-line

The location used for machine inventories in case of a remote call. The default entry can be changed when calling the inventory agent.

Values / Range:	Valid location
Default value:	\$(CommonAppDataFolder)\ManageSoft Corp\ ManageSoft\Tracker\ZeroTouch



Command-line

Tool:	Inventory agent
Example:	<code>-o MachineZeroTouchDirectory=C:\ManageSoft Corp\ManageSoft\Tracker\ZeroTouch</code>

ManageSoftPackages

Command-line | Registry

If this value is set to `True`, information on all software installed onto the computer will be gathered. If this option is set to `False`, no information will be gathered.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>

Command-line

Tool:	Inventory agent
Example:	<code>-o ManageSoftPackages=False</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Tracker\ManageSoftPackages</code>
Computer setting:	<code>[Registry]\ManageSoft\Tracker\ManageSoftPackages</code>

Manual Mapper

Registry

Allows for the mapping of any executable name to a specific product to include application usage metering. This setting can be used to specify an executable that will not be detected as installed by either RayManageSoft Unified Endpoint Manager or the native package format, or is not detected from **Add/Remove Programs**.

Create a key under:

`Usage Agent\CurrentVersion\Manual Mapper\`



This key is the application identifier for the mapper. Create multiple values for this key:

Application="application name (friendly string)"

ExecutablePath="path to executable, may contain regular expression"



Be aware:

It is possible to either specify a file name or a folder name. When specifying Windows executable paths, the file names can be specified under the Windows Installation directories but not simply Windows system folder names. Windows system folder names such as `C:\Windows` and `C:\Windows\System32` will be ignored.

Version="version"

Regex="true" (this is only required if ExecutablePath contains regular expressions)

Priority="priority for this key, which takes precedence over the default priority specified by the ManualMapperDefaultPriority"



Be aware:

If no priority is specified, the value of `ManualMapperDefaultPriority` is used.

Typical regular expression syntax is supported for the configuration of the usage metering. See [Mozilla Developer Network - Regular Expressions](#) for reference.



Note:

Expressions that affect vertical spacing, such as newline and carriage returns, have no effect in this context and are not supported. `[]` is used to escape characters with a special meaning.

A summary of commonly used regular expressions is:

Regular Expression	Matches
.	Matches any single character
*	Matches any preceding character one or more times
[xyz]	A character set. Matches any one of the enclosed characters. A range of characters can be specified by using a hyphen. For example, <code>[a-d]</code> is the same as <code>[abcd]</code> .
x y	Matches x or y . For example <code>Office 10 Office 11</code> matches Office 10 or Office 11 but not Office 12 .

Example:

Applications in the Windows Directory should not be monitored (recommended). But at a later date one program shall be monitored: **Solitaire** (`sol.exe`).



Example key:

```
Application="Solitaire"  
ExecutablePath="C:\WINNT\System32\sol.exe"  
Version="1.0"
```

To track use of `sol.exe` even if users install it in a different location use wildcards:

```
Application="Solitaire"  
ExecutablePath".*\sol[.]exe"  
Version="1.0"  
Regex="true"
```

Values / Range:	String
Default value:	None

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Usage Agent\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Usage\CurrentVersion

ManualMapperDefaultPolicy

Registry

For application usage tracking, a file or directory can only be "owned" by one application. If more than one application that are being tracked specify the same file or directory, the value for this setting is used to determine to which application the file or directory will be allocated for tracking. This process occurs, when the application is specified for tracking. The application with the highest value for this setting owns the file or directory. If more than one application specifies the same file or directory and those applications have identical priorities the application where the usage tracking has most recently been defined takes precedence.

The default value that is defined for this setting is 20 and is automatically higher than the value that is being assigned to other data sources such as Windows Installer, **Add/Remove Programs**, etc. These alternate data sources are assigned a priority of 10 (The order in which usage data is constructed is: the Manual Mapper setting values, the native package format, the RayManageSoft Unified Endpoint Manager cache, **Add/Remove Programs**.).

Values / Range:	Integer between 1 and 10,000
Default value:	20

Registry



Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Usage Agent\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

MinFreeDisk

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (AllowPeerToPeer is True).

It specifies the amount of free disk space (in MB) that must exist on a managed device in order for the peer download agent to download files. The peer download agent checks the free disk space before starting to download a file.

Values / Range:	Integer between 10 and 2,000,000
Default value:	100

Command-line

Tool:	Peer download agent
Example:	-debug -o MinFreeDisk=500

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader



MinimumDCSpeed

Command-line | Registry | Project Variable

This setting only applies for client-side policy merging when `AutoDetectDC` is `False`.

It specifies the minimum network speed (in bits per second) between the managed device and the domain controller that is required to apply the policy. If the detected speed is below the defined value, the client-side policy will not be applied.

Values / Range:	Numeric (bits per second)
Default value:	No default, RayManageSoft Unified Endpoint Manager will attempt a connection regardless of the speed.
Example value:	1000

Command-line

Tool:	Installation agent
Example:	<code>-o MinimumDCSpeed=1000</code>

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Common
Computer setting:	[Registry]\ManageSoft\Common

Project Variable

Define as:	<code>MinimumDCSpeed</code>
Reference as:	<code>\$(MinimumDCSpeed)</code>

MinInventoryInterval

Command-line | Registry

Specifies the minimum interval (in hours) between the collection of inventories. The inventory agent will neither generate nor upload an inventory if it is invoked in less than the specified period of time after the generation of the most recent inventory. This setting controls the collection of inventories under RayManageSoft Unified Endpoint Manager as well as zero-touch inventories.

The time of the last inventory generation is determined by looking at the last modified time of



the last cached inventory file which is typically stored under
Application Data\ManageSoft Corp\ManageSoft\Tracker\Inventories\.

Values / Range:	Any non-negative integer
Default value:	0

Command-line

Tool:	Inventory agent
Example:	-o MinInventoryInterval=24 Generates an inventory at most once a day.

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

MinRunTime

Command-line | Registry

Specifies the minimum time in seconds an application must run before the application usage data for it will be recorded. The value must be greater than 0. If this is not the case, the default will be used.

Values / Range:	Integer greater than 0
Default value:	60

Command-line

Tool:	Application usage agent
Example:	-o MinRunTime=90

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager usage agent on a managed device
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\CurrentVersion



MSI

Command-line | Registry

This option is Windows only!

If set to `True`, Microsoft Installer (MSI) package information is added to the inventories. If set to `False`, RayManageSoft Unified Endpoint Manager does not include MSI package information in inventories.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>

Command-line

Tool:	Inventory agent
Example:	<code>-o MSI=False</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Tracker\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Tracker\CurrentVersion</code>

MsiOpenProducts

Command-line | Registry

Specify the product codes which are to be inspected fully, which involves calculating the result of all applied transforms and patches before retrieval of all applied transforms and patches before retrieval of the `UpgradeCode` and `PIDKEY` properties. The value `*` includes all products. Additionally, this settings cannot have customized values.

Values / Range:	List of MSI products codes.
Default value:	<code>{empty}</code>

Command-line

Tool:	Inventory agent
Example:	n/a



Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\Manage Corp \ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

MsiReinstallFeatures

Registry | Project Variable

This option is Windows only!

Identifies which MSI components will be installed. This is the equivalent to the MSI property `REINSTALL`. For more information on MSI properties refer to <https://docs.microsoft.com/en-us/windows/win32/msi/properties>.

Values / Range:	See the documentation for Microsoft Windows Installer
Default value:	ALL (install all components)

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	MsiReinstallFeatures
Reference as:	\$(!MsiReinstallFeatures)

MsiReinstallModeLevel

Registry | Project Variable

This option is Windows only!

Identifies what will be reinstalled. This can be changed files, newer files, registry files, or all files. This is the equivalent to the MSI property `REINSTALLMODE` and the option `/f` in the `msiexec.exe` command-line. For more information on MSI properties refer to <https://docs.microsoft.com/en-us/windows/win32/msi/properties>.



Values / Range:	Any combination of the following letters: a, c, d, e, m, p, o, s, u, v. See the documentation for Microsoft Windows Installer for details about what each letter represents.
Default value:	osmu
Example value:	vomus (complete reinstall)

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	MsiReinstallModeLevel
Reference as:	\$(!MsiReinstallModeLevel)

MsiRepair

Registry | Project Variable

This option is Windows only!

This setting works in conjunction with `MsiReinstallFeatures`.

While `MsiReinstallFeatures` controls which MSI repair operations are used to reinstall packages, `MsiRepair` determines whether these repairs are performed at the same time as the RayManageSoft Unified Endpoint Manager self-healing operations.

If set to `True`, the MSI repairs are initiated at the same time as the self-healing operations. If set to `False`, the MSI repairs are not initiated when RayManageSoft Unified Endpoint Manager performs the self-healing operations.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device



User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	MsiRepair
Reference as:	\$(!MsiRepair)



MsiRepairLevel

Registry | Project Variable

This option is Windows only!

Identifies what will be repaired. This can be changed files, newer files, registry files, or all files. This is the equivalent to the MSI property `REINSTALLMODE` and the option `/f` in the `msiexec.exe` command-line. For more information on MSI properties refer to <https://docs.microsoft.com/en-us/windows/win32/msi/properties>.

Values / Range:	Any combination of the following letters: a, c, d, e, m, p, o, s, u, v. See the documentation for Microsoft Windows Installer for details about what each letter represents.
Default value:	vomus
Example value:	osmu

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	MsiRepairLevel
Reference as:	\$(!MsiRepairLevel)

MsiSourceLocation

Command-line | Registry

This option is Windows only!

Specifies whether the managed devices should install a Windows Installer package from the local Windows Installer cache or from a distribution location. For more information on MSI properties refer to <https://docs.microsoft.com/en-us/windows/win32/msi/properties>.

Values / Range:	Cache (to install from a local cache) or Server (to install from a distribution location)
Default value:	Cache



Command-line

Tool:	Installation agent
Example:	-o MsiSourceLocation=Server

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

MsiUILevel

Registry | Project Variable

This option is Windows only!

Indicates the user interaction level for the MSI. The user interaction level can be set to full, basic, reduced, or no UI. It is equivalent to the /q argument on the `msiexec.exe` command-line. For more information on MSI properties refer to <https://docs.microsoft.com/en-us/windows/win32/msi/properties>.

Values / Range:	/q, /qn, /qb, /qr, /qf, /qn+, /qb+, /qb+!, /qb-, /qb-! See the documentation for Microsoft Windows Installer for details about what each letter represents.
Default value:	Depends on the UserInteractionLevel setting: • If set to Quiet, Auto, or Status, MsiUILevel defaults to /qn. • If set to Full, MsiUILevel defaults to /qb.
Example value:	/qn

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	MsiUILevel



Reference as:	<code>\$(!MsiUILevel)</code>



MsiUninstallArgs

Registry | Project Variable

This option is Windows only!

Records any arguments to include in the MSI command-line for uninstall operations.

Values / Range:	See the documentation for Microsoft Windows Installer
Default value:	{empty}
Example value:	/l*v c:\temp\msi.log (A command-line argument to turn on logging)

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	MsiUninstallArgs
Reference as:	\$(!MsiUninstallArgs)

NativeScheduler

Command-line | Registry

Indicates whether or not RayManageSoft Unified Endpoint Manager task scheduling is used. The following options are available:

- taskschd - The Microsoft Task Scheduler is used to run events. If the Microsoft Task Scheduler is not available, the RayManageSoft Unified Endpoint Manager Task Scheduler will be used.
- ndtask - The RayManageSoft Unified Endpoint Manager is used to run events. If the RayManageSoft Unified Endpoint Manager Task Scheduler is not available, the Microsoft Task Scheduler will be used.

Values / Range:	taskschd or ndtask
Default value:	ndtask



Command-line

Tool:	Scheduling agent
Example:	-o NativeScheduler=taskschd

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	not available
Computer setting:	[Registry]\ManageSoft\Schedule Agent\CurrentVersion

ndsensNetType

Command-line | Registry

This value determines when a **When connected to network** trigger is deemed to have occurred causing the command given by `ndsensNetUp` to be executed. It will only trigger if the network is of a certain type. There are three possible values:

- 1: Local area network (LAN)
- 2: Wide area network (WAN)
- 3: Either a LAN or a WAN

RayManageSoft Unified Endpoint Manager monitors these network types. For example, if `ndsensNet=2`, RayManageSoft Unified Endpoint Manager only looks for connections to a WAN.

Values / Range:	1, 2, or 3
Default value:	3

Command-line

Tool:	Scheduling agent
Example:	-o ndsensNetType=2

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Schedule Agent\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Schedule Agent\



	CurrentVersion



ndsensNetUp

Registry

This setting is only applicable for Windows device.

The value determines which command is executed once the `ndsensNetType` property deems to have a network connection.

Values / Range:	Valid executable
Default value:	<code>ndschedag.exe -o OnConnect=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Schedule Agent\ CurrentVersion

NetworkHighSpeed (Installation Agent)

Command-line | Registry | Project Variable

This value specifies the lowest network speed (in bits per second) that RayManageSoft Unified Endpoint Manager will consider to be a high-speed network connection to a server.

RayManageSoft Unified Endpoint Manager needs to identify whether a high-speed network connection or a low-speed network connection is in operation in order to determine the bandwidth to be used for uploads and downloads. The bandwidth percentage is stored in `NetworkHighSpeed` (installation agent) and `NetworkLowUsage`.

If `NetworkHighSpeed` is set to 0 (default), RayManageSoft Unified Endpoint Manager does not limit the bandwidth usage according to the measured network speed. With this configuration, content is downloaded at the maximum rate specified by the `NetworkMaxRate` (installation agent) setting and the `NetworkHighSpeed` (installation agent) and `NetworkLowUsage` values are ignored.

Values / Range:	Numeric (number of bits per second)
Default value:	0
Example value:	32



Command-line

Tool:	Installation agent
Example:	-o NetworkHighSpeed=32

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	NetworkHighSpeed
Reference as:	\$(NetworkHighSpeed)

NetworkHighSpeed (Upload Agent)

Command-line | Registry | Project Variable

This value specifies the lowest network speed (in bits per second) that RayManageSoft Unified Endpoint Manager will consider to be a high-speed network connection to a server.

RayManageSoft Unified Endpoint Manager needs to identify whether a high-speed network connection or a low-speed network connection is in operation in order to determine the bandwidth to be used for uploads and downloads. The bandwidth percentage is stored in `NetworkHighSpeed` (upload agent) and `NetworkLowUsage`.

If `NetworkHighSpeed` is set to 0 (default), RayManageSoft Unified Endpoint Manager does not limit the bandwidth usage according to the measured network speed. With this configuration, content is downloaded at the maximum rate specified by the `NetworkMaxRate` (upload agent) setting and the `NetworkHighSpeed` (upload agent) and `NetworkLowUsage` values are ignored.

Values / Range:	Numeric (number of bits per second)
Default value:	0
Example value:	32

Command-line

Tool:	Upload agent
Example:	-o NetworkHighSpeed=32



Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Uploader\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	In order of precedence: • [Registry]\ManageSoft\Uploader\CurrentVersion • [Registry]\ManageSoft\Common

Project Variable

Define as:	NetworkHighSpeed
Reference as:	\$(NetworkHighSpeed)

NetworkHighUsage

Command-line | Registry | Project Variable

This setting specifies the maximum percentage of bandwidth that RayManageSoft Unified Endpoint Manager uses for uploads and downloads on a high-speed connection.

If `NetworkHighUsage` is configured to be outside the range specified by `NetworkHighUsageLowerLimit` and `NetworkHighUsageUpperLimit` and the lower limit is strictly less than the upper limit, `NetworkHighUsage` is automatically set to the closest range endpoint. For example, considering a case where `NetworkHighUsageLowerLimit` is 10 and `NetworkHighUsageUpperLimit` is 40. If `NetworkHighUsage` is set to 5, RayManageSoft Unified Endpoint Manager resets it to 10. If `NetworkHighUsage` is set to 60, RayManageSoft Unified Endpoint Manager resets it to 40.

If `NetworkHighUsage` is set to 0, the installation agent will download files using 0.1 % of the measured bandwidth. If peer-to-peer file sharing is enabled (`AllowPeerToPeer` is `True`), this setting does not apply. Instead see [ParentConnectionWindows](#) and [PeerConnectionWindows](#).

Values / Range:	Numeric (percentage 0-100)
Default value:	100
Example value:	55

Command-line



Tool:	Installation agent
Example:	-o NetworkHighUsage=55

Registry

Installed by:	For downloads the installation of RayManageSoft Unified Endpoint Manager on a managed device. For Uploads manual configuration.
User setting:	For installation agent downloads in order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common For data reporting agent uploads in order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Uploader\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	[For installation agent downloads in order of precedence: • [Registry]\ManageSoft\Launcher\CurrentVersion • [Registry]\ManageSoft\Common For data reporting agent uploads in order of precedence: • [Registry]\ManageSoft\Uploader\CurrentVersion • [Registry]\ManageSoft\Common

Project Variable

Define as:	NetworkHighUsage
Reference as:	\$(NetworkHighUsage)

NetworkHighUsageLowerLimit

Command-line | Registry | Project Variable

Specifies the minimum `NetworkHighUsage` value that can be set for a managed device by an end-user moving the bandwidth slider control in the installation agent.

The bandwidth usage slider control is only available if:

- The connection speed to the distribution location can be determined.
- The installation agent is downloading from a distribution location to which the detected connection speed is at least the speed specified by `NetworkHighSpeed` (installation agent).
- The `NetworkHighUsageLowerLimit` is strictly less than the `NetworkHighUsageUpperLimit`.

The `NetworkHighUsage` value is recorded under the `HKEY_CURRENT_USER` registry area of the



user.

Values / Range:	Numeric (percentage 0-100)
Default value:	100
Example value:	10

Command-line

Tool:	Installation agent
Example:	-o NetworkHighUsageLowerLimit=10

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	In order of precedence: • [Registry]\ManageSoft\Launcher\CurrentVersion • [Registry]\ManageSoft\Common

Project Variable

Define as:	NetworkHighUsageLowerLimit
Reference as:	\$(NetworkHighUsageLowerLimit)

NetworkHighUsageUpperLimit

Command-line | Registry | Project Variable

Specifies the maximum `NetworkHighUsage` value that can be set for a managed device by an end-user moving the bandwidth slider control in the installation agent.

The bandwidth usage slider control is only available if:

- The connection speed to the distribution location can be determined.
- The installation agent is downloading from a distribution location to which the detected connection speed is at least the speed specified by `NetworkHighSpeed` (installation agent).
- The `NetworkHighUsageLowerLimit` is strictly less than the `NetworkHighUsageUpperLimit`.



The `NetworkHighUsage` value is recorded under the `HKEY_CURRENT_USER` registry area of the user.

Values / Range:	Numeric (percentage 0-100)
Default value:	100
Example value:	90

Command-line

Tool:	Installation agent
Example:	<code>-o NetworkHighUsageUpperLimit=90</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion</code> • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common</code>
Computer setting:	In order of precedence: • <code>[Registry]\ManageSoft\Launcher\CurrentVersion</code> • <code>[Registry]\ManageSoft\Common</code>

Project Variable

Define as:	<code>NetworkHighUsageUpperLimit</code>
Reference as:	<code>\$(NetworkHighUsageUpperLimit)</code>

NetworkLowUsage

Command-line | Registry | Project Variable

This setting specifies the maximum percentage of bandwidth that RayManageSoft Unified Endpoint Manager uses for uploads and downloads on a low-speed connection.

If `NetworkLowUsage` is configured to be outside the range specified by `NetworkLowUsageLowerLimit` and `NetworkLowUsageUpperLimit` and the lower limit is strictly less than the upper limit, `NetworkLowUsage` is automatically set to the closest range endpoint. For example, considering a case where `NetworkLowUsageLowerLimit` is 10 and `NetworkLowUsageUpperLimit` is 40. If `NetworkLowUsage` is set to 5, RayManageSoft Unified



Endpoint Manager resets it to 10. If `NetworkLowUsage` is set to 60, RayManageSoft Unified Endpoint Manager resets it to 40.

If `NetworkLowUsage` is set to 0, the installation agent will download files using 0.1 % of the measured bandwidth. If peer-to-peer file sharing is enabled (`AllowPeerToPeer` is `True`), this setting does not apply. Instead see [ParentConnectionWindows](#) and [PeerConnectionWindows](#).

Values / Range:	Numeric (percentage 0-100)
Default value:	100
Example value:	45

Command-line

Tool:	Installation agent
Example:	<code>-o NetworkLowUsage=45</code>

Registry

Installed by:	For downloads the installation of RayManageSoft Unified Endpoint Manager on a managed device. For Uploads manual configuration.
User setting:	For installation agent downloads in order of precedence: • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion</code> • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common</code> For data reporting agent uploads in order of precedence: • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Uploader\CurrentVersion</code> • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common</code>
Computer setting:	For installation agent downloads in order of precedence: • <code>[Registry]\ManageSoft\Launcher\CurrentVersion</code> • <code>[Registry]\ManageSoft\Common</code> For data reporting agent uploads in order of precedence: • <code>[Registry]\ManageSoft\Uploader\CurrentVersion</code> • <code>[Registry]\ManageSoft\Common</code>

Project Variable

Define as:	<code>NetworkLowUsage</code>
Reference as:	<code>\$(NetworkLowUsage)</code>



NetworkLowUsageLowerLimit

Command-line | Registry | Project Variable

This setting is only applicable for Windows devices.

Specifies the minimum `NetworkLowUsage` value that can be set for a managed device by an end-user moving the bandwidth slider control in the installation agent.

The bandwidth usage slider control is only available if:

- The connection speed to the distribution location can be determined.
- The installation agent is downloading from a distribution location to which the detected connection speed is at least the speed specified by `NetworkHighSpeed` (installation agent).
- The `NetworkLowUsageLowerLimit` is strictly less than the `NetworkLowUsageUpperLimit`.

The `NetworkLowUsage` value is recorded under the `HKEY_CURRENT_USER` registry area of the user.

Values / Range:	Numeric (percentage 0-100)
Default value:	100
Example value:	10

Command-line

Tool:	Installation agent
Example:	<code>-o NetworkLowUsageLowerLimit=10</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion</code> • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common</code>
Computer setting:	In order of precedence: • <code>[Registry]\ManageSoft\Launcher\CurrentVersion</code> • <code>[Registry]\ManageSoft\Common</code>

Project Variable



Define as:	NetworkLowUsageLowerLimit
Reference as:	\$(NetworkLowUsageLowerLimit)

NetworkLowUsageUpperLimit

Command-line | Registry | Project Variable

Specifies the maximum `NetworkLowUsage` value that can be set for a managed device by an end-user moving the bandwidth slider control in the installation agent.

The bandwidth usage slider control is only available if:

- The connection speed to the distribution location can be determined.
- The installation agent is downloading from a distribution location to which the detected connection speed is at least the speed specified by `NetworkHighSpeed` (installation agent).
- The `NetworkLowUsageLowerLimit` is strictly less than the `NetworkLowUsageUpperLimit`.

The `NetworkLowUsage` value is recorded under the `HKEY_CURRENT_USER` registry area of the user.

Values / Range:	Numeric (percentage 0-100)
Default value:	100
Example value:	90

Command-line

Tool:	Installation agent
Example:	-o NetworkLowUsageUpperLimit=90

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion</code> • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common</code>
Computer setting:	In order of precedence: • <code>[Registry]\ManageSoft\Launcher\CurrentVersion</code> • <code>[Registry]\ManageSoft\Common</code>



Project Variable

Define as:	NetworkLowUsageUpperLimit
Reference as:	\$(NetworkLowUsageUpperLimit)

NetworkMaxRate (Installation Agent)

Command-line | Registry | Project Variable

This value represents the bytes per second at which the managed device accesses data over the network. This setting is not used if the network speed can be determined and the `NetworkHighSpeed` (installation agent) setting is set to a non-zero value.

If peer-to-peer file sharing is enabled (`AllowPeerToPeer` is `True`), this setting does not apply. Instead see [ParentConnectionWindows](#) and [PeerConnectionWindows](#).

Values / Range:	Numeric (bytes per second)
Default value:	0 (unlimited)
Example value:	64

Command-line

Tool:	Installation agent
Example:	-o NetworkMaxRate=64

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	In order of precedence: • [Registry]\ManageSoft\Launcher\CurrentVersion • [Registry]\ManageSoft\Common

Project Variable

Define as:	NetworkMaxRate
Reference as:	\$(NetworkMaxRate)



NetworkMaxRate (Upload Agent)

Command-line | Registry | Project Variable

This value represents the bytes per second at which the managed device accesses data over the network. This setting is not used if the network speed can be determined and the `NetworkHighSpeed` (upload agent) setting is set to a non-zero value.

If peer-to-peer file sharing is enabled (`AllowPeerToPeer` is `True`), this setting does not apply. Instead see [ParentConnectionWindows](#) and [PeerConnectionWindows](#).

Values / Range:	Numeric (bytes per second)
Default value:	0 (unlimited)
Example value:	64

Command-line

Tool:	Upload agent
Example:	<code>-o NetworkMaxRate=64</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Uploader\CurrentVersion</code> • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common</code>
Computer setting:	In order of precedence: • <code>[Registry]\ManageSoft\Uploader\CurrentVersion</code> • <code>[Registry]\ManageSoft\Common</code>

Project Variable

Define as:	<code>NetworkMaxRate</code>
Reference as:	<code>\$(NetworkMaxRate)</code>

NetworkMinSpeed (Installation Agent)

Command-line | Registry | Project Variable



This setting represents the minimum network speed for RayManageSoft Unified Endpoint Manager to initiate a check for updates.

Values / Range:	Numeric (bytes per second)
Default value:	No default in registry; default behavior 1
Example value:	2000

Command-line

Tool:	Installation agent
Example:	-o NetworkMinSpeed=2000

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	In order of precedence: • [Registry]\ManageSoft\Launcher\CurrentVersion • [Registry]\ManageSoft\Common

Project Variable

Define as:	NetworkMinSpeed
Reference as:	\$(NetworkMinSpeed)

NetworkMinSpeed (Upload Agent)

Command-line | Registry | Project Variable

This setting represents the minimum network speed for RayManageSoft Unified Endpoint Manager to initiate a check for updates.

Values / Range:	Numeric (bytes per second)
Default value:	No default in registry; default behavior 1
Example value:	2000



Command-line

Tool:	Upload agent
Example:	-o NetworkMinSpeed=2000

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Uploader\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	In order of precedence: • [Registry]\ManageSoft\Uploader\CurrentVersion • [Registry]\ManageSoft\Common

Project Variable

Define as:	NetworkMinSpeed
Reference as:	\$(NetworkMinSpeed)

NetworkRetries

Command-line | Registry | Project Variable

This setting represents the number of times a failed network operation is retried before an alternative download location is attempted.


Note:

The maximum number of attempts to connect to a file share is controlled by the `ConnectionAttempts` setting and **not** by the `NetworkRetries` setting.

Values / Range:	Numeric
Default value:	1

Command-line

Tool:	Installation agent
Example:	-o NetworkRetries=2



Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	NetworkRetries
Reference as:	\$(NetworkRetries)

NetworkSense (Installation Agent)

Command-line | Registry | Project Variable

This setting determines whether network checks are bypassed. If set to `True`, RayManageSoft Unified Endpoint Manager performs network checks (such as bandwidth speed). If set to `False`, RayManageSoft Unified Endpoint Manager bypasses any network checks. If peer-to-peer file sharing is enabled (`AllowPeerToPeer` is `True`), this setting does not apply. Instead refer to the [ParentConnectionWindows](#) and [PeerConnectionWindows](#).

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Installation agent
Example:	<code>-o NetworkSense=False</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: - HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion - HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	In order of precedence: [Registry]\ManageSoft\Launcher\CurrentVersion [Registry]\ManageSoft\Common



Project Variable

Define as:	NetworkSense
Reference as:	\$(NetworkSense)

NetworkSense (Inventory Agent)

Command-line | Registry

This setting determines whether network checks are bypassed for uploads performed by the inventory agent. If set to `True`, RayManageSoft Unified Endpoint Manager performs network checks (such as bandwidth speed). If set to `False`, RayManageSoft Unified Endpoint Manager bypasses any network checks.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	inventory agent
Example:	<code>-o NetworkSense=False</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Tracker\CurrentVersion</code> • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common</code>
Computer setting:	In order of precedence: • <code>[Registry]\ManageSoft\Tracker\CurrentVersion</code> • <code>[Registry]\ManageSoft\Common</code>

NetworkSense (Upload Agent)

Command-line | Registry | Project Variable

This setting determines whether network checks are bypassed by the upload agent. If set to `True`, RayManageSoft Unified Endpoint Manager performs network checks (such as bandwidth speed). If set to `False`, RayManageSoft Unified Endpoint Manager bypasses any network checks.



Values / Range:	Boolean (True or False)
Default value:	False

Command-line

Tool:	Upload agent
Example:	-o NetworkSense=False

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Uploader\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	In order of precedence: • [Registry]\ManageSoft\Uploader\CurrentVersion • [Registry]\ManageSoft\Common

Project Variable

Define as:	NetworkSense
Reference as:	\$(NetworkSense)

NetworkTimeout (Installation Agent)

Command-line | Registry | Project Variable

Determines the length of time of inactivity measured in seconds after which a network operation will time out.

Values / Range:	Numeric (seconds)
Default value:	30

Command-line

Tool:	Installation agent
Example:	-o NetworkTimeout=10



Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	In order of precedence: • [Registry]\ManageSoft\Launcher\CurrentVersion • [Registry]\ManageSoft\Common

Project Variable

Define as:	NetworkTimeout
Reference as:	\$(NetworkTimeout)

NetworkTimeout (Upload Agent)

Command-line | Registry | Project Variable

Determines the length of time of inactivity measured in seconds after which a network operation will time out.

Values / Range:	Numeric (seconds)
Default value:	600 (ten minutes)

Command-line

Tool:	Upload agent
Example:	-o NetworkTimeout=1000

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Uploader\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common



Computer setting:	In order of precedence: • [Registry] \ManageSoft \Uploader \CurrentVersion • [Registry] \ManageSoft \Common

Project Variable

Define as:	NetworkTimeout
Reference as:	\$(NetworkTimeout)

NonAdSoftwareAssignment

Registry

This setting changes the default behavior of the managed device agent. It will use a uniquely generated GUID to request machine policies instead of the combination of the machine name and the domain. This is useful in environments where no active directory can or should be used.

Values / Range:	Boolean (True or False)
Default value:	True

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	Not available
Computer setting:	[Registry] \ManageSoft \PolicyClient \CurrentVersion

NoStage

Command-line | Registry | Project Variable

If set to `True`, files are downloaded directly to their install location without first placing them in the staging area. As a result, no checks are performed on files before they overwrite any existing files. If set to `False`, RayManageSoft Unified Endpoint Manager uses a staging area before transferring files to their install location.

	Be aware: This bypasses the staging area and is not recommended.

Values / Range:	Boolean (True or False)



Default value:	False

Command-line

Tool:	Installation agent
Example:	-o NoStage=True

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	NoStage
Reference as:	\$(NoStage)

ParentActivityTimeout

Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

RayManageSoft Unified Endpoint Manager peer download agent can trigger a **When connected to network** event that can be used to trigger a scheduled task. For example, a task can run when a dialup line is up and in use.

The peer download agent triggers the **When connected to network** event when either it or a peer it can see in the network initiates a file download from a distribution server. This occurs when no download has been active for at least `ParentActivityTimeout` seconds.

Values / Range:	Integer that is less than 7,200 (120 minutes)
Default value:	300 (5 minutes)
Example value:	150

Registry

Installed by:	Manual configuration



User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Common

ParentConnectionWindows

Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`) and `IgnoreConnectionWindows` is `False`.

It specifies the time periods during which the RayManageSoft Unified Endpoint Manager peer download agent can download packages from its closest distribution server and upload status information to reporting locations (To specify the time periods during which downloads from peer managed devices are allowed use `PeerConnectionWindows`).

Downloads in progress at the end of a time period will be stopped immediately and subsequent downloads of the same file will continue from that point.

**Be aware:**

When remote execution operations require data to be uploaded or downloaded these operations override the peer-to-peer settings.

Also see [AllowPeerToPeer](#), [PeerConnectionWindows](#), and [IgnoreConnectionWindows](#).

Values / Range:	String in HHMM-HHMM:PP, HHMM-HHMM:PP format where: • HHMM is a local time in 24 hour format (0000-2359). If not specified, the time period is the whole day. If the end time is earlier than the start time, it is assumed to be for the following day. For example, 0400-0100 specifies the period between 4 am on the first day and 1 am on the following day. • PP is a percentage of the end-to-end bandwidth that can be used by this managed device (optional). How the maximum available bandwidth is calculated is described in PeerMaxRate. The amount of the bandwidth available for a managed device is the maximum rate divided by the number of peers conducting transfers (regardless of the distribution server used by the peers). Multiple non-overlapping periods separated by commata can be specified.
Default value:	{empty}
Example value:	2300-0100:85 (between 11 pm and 1 am at 85% of the available bandwidth)



Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Common

PeerAveragingTime

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (AllowPeerToPeer is True).

In conjunction with `PeerMaxRate` it is used to limit the bandwidth used for peer-to-peer file sharing operations. It specifies the average period (in minutes) used to smooth the estimation for the transfers to and from peer managed devices. See [PeerMaxRate](#) for details about how these settings are used together.

Increasing the value of this setting means that the estimation takes longer to change as the actual transfer rate changes. In normal use, it is not necessary to change the value for this setting. RayManageSoft Unified Endpoint Manager retrieves the value for this setting from the registry every five seconds. It is not necessary to restart RayManageSoft Unified Endpoint Manager on managed devices after changing the value of this setting.

Values / Range:	Integer between 1 - 60
Default value:	5

Command-line

Tool:	Peer download agent
Example:	-debug -o PeerAveragingTime=10

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader



PeerConnectionWindows

Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`) and `IgnoreConnectionWindows` is `False`.

It specifies the time periods during which the RayManageSoft Unified Endpoint Manager peer download agent can download packages from peer managed devices (To specify time periods during which the peer download agent can download packages from the nearest distribution server use `ParentConnectionWindows`).

Downloads in progress at the end of a time period will be stopped immediately and subsequent downloads of the same file will continue from that point.

Values / Range:	String in HHMM-HHMM:PP, HHMM-HHMM:PP format where: • HHMM is a local time in 24 hour format (0000-2359). If not specified, the time period is the whole day. If the end time is earlier than the start time, it is assumed to be for the following day. For example, 0400-0100 specifies the period between 4 am on the first day and 1 am on the following day. • PP is a percentage of the end-to-end bandwidth that can be used by this managed device (optional). How the maximum available bandwidth is calculated is described in PeerMaxRate. Multiple non-overlapping periods separated by commas can be specified.
Default value:	None
Example value:	2300-0100:85 (between 11 pm and 1 am at 85% of the available bandwidth)

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Common

PeerListenQueue

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).



It specifies the maximum number of connection request to queue before refusing additional connections. Under some TCP configurations, this prevents requests from being rejected when peer-to-peer is configured to pull files (`PeerPush` is `False`) and a number of files are requested in less than 100 milliseconds.

Consider setting this setting if the following errors are logged by `mgddl.exe` or if advised by a Raynet support representative:

- Error code 10054 - an existing connection was forcibly closed by the remote host. This often appears in configurations where `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect` has a value of 1 or 2. This configuration results in "half open" connections as the Windows TCP-layer SYN attack prevention blocks the connections opened by the RMS UEM AppCenter for peer-to-peer file transfer.
- Error code 10061 - No connection could be made because the target machine actively refused it.

Values / Range:	Integer between 1 - 100
Default value:	5

Command-line

Tool:	Peer download agent
Example:	<code>-debug -o PeerListenQueue=15</code>

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	<code>[Registry]\ManageSoft\Downloader</code>

PeerMaxRate

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

It specifies the maximum allowable rate (in bytes per second) for transfers to and from peer managed devices.

The value of this setting should be chosen based on the speed of the LAN connection. For example, if the LAN connection is a 100 MB/s connection, the value for this setting can be set to 1,048,576 (1 MB/s) to ensure that peer-to-peer file sharing operations do not use more than 10% of the available bandwidth.



`PeerMaxRate` is used in conjunction with `PeerAveragingTime` to limit bandwidth used by peer-to-peer file sharing operations. RayManageSoft Unified Endpoint Manager calculates the sum of file transfers that have occurred between this managed device and peer managed devices. Since transfers occur in blocks and not as continuous stream, RayManageSoft Unified Endpoint Manager smooths out the variation in transfer rates using the `PeerAveragingTime` and a simple exponential decay algorithm. This result is an estimate of the transfer rate. Transfer rates will be decreased if the estimated rate exceeds the specified `PeerMaxRate` and increased if they are below the specified `PeerMaxRate` (Transfers can creep up to the `PeerMaxRate`, but they will drop back rapidly if the estimated rate is greater than the `PeerMaxRate`.).

RayManageSoft Unified Endpoint Manager retrieves the value for this setting from the registry every five seconds. It is not necessary to restart RayManageSoft Unified Endpoint Manager on a managed device after the value of this setting has been changed.

Values / Range:	Integer between 1,024 - 134,217,728
Default value:	16777216

Command-line

Tool:	Peer download agent
Example:	<code>-debug -o PeerMaxRate=2048 http://myserver/mypg.osd</code>

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

PeerPullPort

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

It specifies the TCP port used for peer-to-peer file fetch operations. This port must not be firewalled.

Also see [PeerPush](#) and [AllowPeerToPeer](#).

Values / Range:	Integer between 1,000 - 65,535
Default value:	6087



Command-line

Tool:	Peer download agent
Example:	<code>-debug -o PeerPullPort=7400</code>

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

PeerPush

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

If the value of this setting is `True`, peer managed devices can immediately push a file in response to a request for the file. Allowing for immediate pushing of files reduces the UDP traffic from searching, but since the port used cannot be configured, this is not suitable for managed devices running firewall software. In networks where most of the peers are firewalled, this setting should be set to `False`.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>

Command-line

Tool:	Peer download agent
Example:	<code>-debug -o PeerPush=False</code>

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader



PeerSearchDuration

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

It specifies the number of seconds the peer download agent will spend searching for files in peer managed device caches before choosing to download the file from the closest distribution server.

Values / Range:	Integer between 3 and 600
Default value:	10

Command-line

Tool:	Peer download agent
Example:	<code>-debug -o PeerSearchDuration=30</code>

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

PeerSearchPort

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

This value specifies the UDP port used for peer-to-peer search operations. This port must not be firewalled.

Values / Range:	Integer between 1,000 - 65,535
Default value:	6087

Command-line

Tool:	Peer download agent
Example:	<code>-debug -o PeerSearchPort=7400</code>



Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

PeerTransferLimit

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer is True`).

This setting specifies the number of simultaneous peer-to-peer search and file transfer operations allowed across all peers on the subnet. Before commencing a file search or transfer operation, the managed device checks to see how many peers are currently performing searches or transfers. The managed device will not start a search or transfer if the number of managed devices currently downloading is equal to or greater than the `PeerTransferLimit` configured for this device.

Values / Range:	Integer between 1 - 64
Default value:	10

Command-line

Tool:	Peer download agent
Example:	-debug -o PeerTransferLimit=30

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

PipeName (Peer Download Agent)

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer is True`).



The name of the operating system pipe used to communicate with the RayManageSoft Unified Endpoint Manager peer-to-peer download service (pipes are used to supply the output of one program as input to another). During normal operation, it is not necessary to change this value.

Values / Range:	String
Default value:	RayManageSoft Download Service
Example value:	My Testing Service

Command-line

Tool:	Peer download agent
Example:	-debug -o PipeName="My Testing Service"

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Downloader
Computer setting:	[Registry]\ManageSoft\Downloader

PlatformSpecificPackages

Command-line | Registry

Specifies whether the information about non-Windows, platform-specific packages (for example .lpp, .pkg, .rpm, and .sd-ux) is included in the software inventory. This setting is ignored on Windows computers.

Values / Range:	Boolean (True or False)
Default value:	True (when the registry value has not been set)
Example value:	False

Command-line

Tool:	Inventory agent
Example:	-o PlatformSpecificPackages=True

Registry

Installed by:	Update settings package on a managed device (computer setting)



User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

PolicyComplianceLog

Registry

Instructs RayManageSoft Unified Endpoint Manager to upload policy compliance log files from the managed device to the specified server location.

This setting is configured during installation and should not be altered by end-users.

Values / Range:	Valid location
Default value:	\$(ServerLocation)\PolicyComplianceLogs\ \$(UserId) on \$(MachineId) at \$(DateTime).plc
Example value:	\$(ServerLocation)\PolicyComplianceLogs\ \$(UserId) on \$(MachineId) at \$(DateTime).plc

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Common\Rules
Computer setting:	[Registry]\ManageSoft\Common\Rules

PolicyPackageRefreshPeriod

Registry

This setting specifies the number of seconds after successfully downloading package (.osd) files during which the download of these files should not be attempted again. If a value for this setting is configured, each time the policy is applied, the policy agent checks to see if the package files required by a policy have been downloaded within this time period. If this is the case, the currently downloaded package files are used for installation.

If the package files have not been downloaded within the time interval, they are downloaded only if they have changed since they were last downloaded to the managed device (The check for this depends on the protocol in use. For HTTP download an **If-Modified-Since** HTTP request is used. Equivalent requests are made for other protocols.).

For example, a package file MyApplication.osd was downloaded at 4 PM and used to install the application MyApplication. The value of PolicyPackageRefreshPeriod is set to 43200 (12



hours). A scheduled task applies a policy and attempts to update `MyApplication` at 8 PM. Since 8 PM is less than 12 hours after `MyApplication.osd` was last downloaded, no attempt to download the file is made.

If no value is set for this setting, package files are always downloaded regardless of whether or not they have changed since they were last downloaded. If newer packager files (those that have changed since the last download to the managed device) are to be downloaded when the policy is applied, the value for this setting needs to be set to 0 (zero).

Values / Range:	Integer ranging from 0 - 1,000,000,000
Default value:	86400 seconds (24 hours)
Example value:	28800 seconds (8 hours)

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Common
Computer setting:	[Registry]\ManageSoft\Common

PolicyRefreshPeriod

Registry

This setting specifies the number of seconds after successfully downloading policy (.npl) files during which the download of these files should not be attempted again. If a value for this setting has been configured, each time the policy is applied, the policy agent checks to see if the policy files have been downloaded within this time period. If this is the case, the currently downloaded policy files are used to apply the policy.

If the policy files have not been downloaded within the time interval, they are downloaded only if they have changed since they were last downloaded to the managed device (The check for this depends on the protocol in use. For HTTP download an **If-Modified-Since HTTP** request is used. Equivalent requests are made for other protocols.).

For example, policy files were downloaded at 4 PM. The value of `PolicyRefreshPeriod` is set to 43200 (12 hours). A scheduled task starts applying the policy at 8 PM. Since 8 PM is less than 12 hours after the policy was last downloaded, no attempt to download more recent policy files is made.

If no value has been configured for this setting, policy files are always downloaded regardless of whether or not they have changed since they were last downloaded. If newer policy files (those that have changed since the last download to the managed device) are to be downloaded when the policy is applied, the value for this setting needs to be set to 0 (zero).



Values / Range:	Integer ranging from 0 - 1,000,000,000
Default value:	86400 seconds (24 hours)
Example value:	28800 seconds (8 hours)

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Common
Computer setting:	[Registry]\ManageSoft\Common

PolicyServerPriortiy

Command-line | Registry

Specifies the priority to apply to the distribution location identified by the `PolicyServerURL` setting. Configuring this setting to a low value (high priority) such as 0 results in the server identified by the `PolicyServerURL` being used as a source for package downloads in preference to other servers. Setting it to a high value (low priority) such as 100 results in the server being prioritized after other servers.

`PolicyServerPriortiy` can also be set to the case-insensitive literal string `Invalid`. With this value, the server identified by `PolicyServerURL` will not be considered at all for package downloads.

Values / Range:	Recommended range of 0 - 100, or <code>Invalid</code>
Default value:	50

Command-line

Tool:	Installation agent
Example:	<code>-o PolicyServerPriority=1</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion



PolicyServerURL

Registry

Determines the distribution location used as a source for package downloads unless the PolicyServerPriority is lower than the priority of other servers.

Values / Range:	Path to valid policy device for the device
Default value:	<code>\$(DownloadRootURL)/Policies/Merged/ \$(URLComputerDomain)Machine/ \$(MachineName).nlp</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Policy Client\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Policy Client\ CurrentVersion</code>



PolicySource

Registry

The location where the policy is generated. There are two option:

- **Server:** NPL policy files are generated on the administration server and distributed for use.
- **Client:** The managed device retrieves the policy directly from the Active Directory.

Client-side merging is only available for managed devices that are connected to the Active Directory (It is possible to use the `EnablePolicyFailover` setting to switch to using server-side policy in the event that the Active Directory is not reachable at the time the client-side policy is due for application.).

Values / Range:	Server or Client
Default value:	Server

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Policy Client\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Policy Client\ CurrentVersion

PreferenceUpdatePeriod

Command-line | Registry

Specifies how often (in seconds) the application usage agent will refresh its settings from the registry. The value must be greater than 0, otherwise the default value will be used.

Values / Range:	Integer greater than 0
Default value:	86400

Command-line

Tool:	Application usage agent
Example:	-o PreferenceUpdatePeriod="90"

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a



	managed device (Computer setting)
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

ProcessUpdatePeriod

Command-line | Registry

Specifies how often (in seconds) the application usage agent will check for newly started or exited applications. The value must be greater than 0 otherwise the default value will be used.

Values / Range:	Integer greater than 0 (number of seconds)
Default value:	60

Command-line

Tool:	Application usage agent
Example:	-o ProcessUpdatePeriod=90

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

ProductUpdatePeriod

Command-line | Registry

Specifies how often (in seconds) the application usage agent will check for newly installed applications. The value must be greater than 0 otherwise the default value will be used.

Values / Range:	Integer greater than 0 (number of seconds)
Default value:	86400

Command-line



Tool:	Application usage agent
Example:	-o ProductUpdatePeriod=90

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

ProgressDepth

Registry

The number of directory levels to search at the initialization to approximate the number of directories searched during tracking.

Values / Range:	Integer between 1 - 10
Default value:	No default in registry; default behavior 3

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

PromptOnCOMRegFailures

Command-line | Registry | Project Variable

Only applicable when `UserInteractionLevel` (Installation agent) is set to `Full`.

If set to `True`, RayManageSoft Unified Endpoint Manager prompts the user when it fails to register a COM server. If set to `False`, RayManageSoft Unified Endpoint Manager does not prompt the user and continues with the installation of the package.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)



Default value:	True

Command-line

Tool:	Installation agent
Example:	-o PromptOnCOMRegFailure=False

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	PromptOnCOMRegFailures
Reference as:	\$(PromptOnCOMRegFailures)

PromptOnInstallCompletion

Command-line | Registry | Project Variable

Only applicable if `UserInteractionLevel` (installation agent) is set to `Full`.

If set to `True`, RayManageSoft Unified Endpoint Manager informs the user that the installation has been completed. If set to `False`, RayManageSoft Unified Endpoint Manager does not inform the user about the completion of the installation.

Values / Range:	Boolean (True or False)
Default value:	False

Command-line

Tool:	Installation agent
Example:	-o PromptOnInstallCompletion=True

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)



User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	PromptOnInstallCompletion
Reference as:	\$(PromptOnInstallCompletion)

PromptOnUninstallCompletion

Command-line | Registry | Project Variable

Only applicable if `UserInteractionLevel` (installation agent) is set to `Full`.

If set to `True`, RayManageSoft Unified Endpoint Manager informs the user that the package uninstall has been completed. If set to `False`, RayManageSoft Unified Endpoint Manager does not inform the user about the completion of the uninstall.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Installation agent
Example:	<code>-o PromptOnUninstallCompletion=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	PromptOnUninstallCompletion
Reference as:	\$(PromptOnUninstallCompletion)



PropagatePkgChanged

Command-line | Registry | Project Variable

This is only applicable for Third-party installer packages

If set to `True`, RayManageSoft Unified Endpoint Manager reinstalls the base package if the prerequisites for the package have changed.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Installation agent
Example:	<code>-o PropagatePkgChanged=False</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	<code>PropagatePkgChanged</code>
Reference as:	<code>\$(PropagatePkgChanged)</code>

PublicAppAccess

Command-line | Registry | Project Variable

Determines RayManageSoft Unified Endpoint Manager access to the Windows Common folders and file on Windows. The options are:

- `FullAccess` - RayManageSoft Unified Endpoint Manager can access areas of the file system available to all users.
- `NoAccess` - RayManageSoft Unified Endpoint Manager cannot access areas of the file system available to all users.



Note:



	This setting does not override file system access. The <code>FullAccess</code> option does not provide access through RayManageSoft Unified Endpoint Manager if the user does not already have access to the Common areas of the file system.

Values / Range:	<code>FullAccess</code> or <code>NoAccess</code>
Default value:	<code>FullAccess</code>

Command-line

Tool:	Installation agent
Example:	<code>-o PublicAppAccess=NoAccess</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Launcher\CurrentVersion</code>

Project Variable

Define as:	<code>PublicAppAccess</code>
Reference as:	<code>\$(PublicAppAccess)</code>



QuietUntilUpdate

Command-line | Registry | Project Variable

If set to `True`, this option hides the RayManageSoft Unified Endpoint Manager user interface on the managed device until either a user interaction is necessary or a package requires installation, upgrading, or uninstalling. The user interface is hidden while RayManageSoft Unified Endpoint Manager checks to see if an update is required. If the user interface is being displayed, it is displayed according to the `UserInteractionLevel` setting. If set to `False`, the RayManageSoft Unified Endpoint Manager user interface is being displayed according to the `UserInteractionLevel` setting, whether or not a user interaction is required or not.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Installation agent
Example:	<code>-o QuietUntilUpdate=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	<code>QuietUntilUpdate</code>
Reference as:	<code>\$(QuietUntilUpdate)</code>

RebootCmdLine

Command-line | Registry

Used on the managed device to reboot from the command-line.

Values / Range:	Name of the executable in the command path
Default value:	<code>"\$(RebootPath)"</code>



Command-line

Tool:	Installation agent
Example:	"\$(RebootPath)" -t 60

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

RebootContinueAfterCmdFailure

Command-line | Registry

Specifies whether to continue with the reboot of the managed device if the prereboot command returned a non-zero exit code (typically indicating that an error has occurred or a warning has been generated).

Values / Range:	Boolean (True or False)
Default value:	True

Command-line

Tool:	Reboot agent
Example:	reboot.exe -c false

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

RebootForceWindowToTop

Command-line | Registry

Force the reboot dialog to be the top window during the final stage of user prompting.



Values / Range:	Boolean
Default value:	false

Command-line

Tool:	Reboot agent
Example:	-o RebootForceWindowToTop=true

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common
Computer setting:	In order of precedence: • [Registry]\ManageSoft\Launcher\CurrentVersion • [Registry]\ManageSoft\Common

RebootIfRequired

Command-line | Registry

Determines whether to reboot if RayManageSoft Unified Endpoint Manager has determined that a reboot is necessary.

This setting configures the default response to the dialog that prompts end-users to confirm a reboot:

- If set to `False`, the default response is to not reboot
- If set to `True`, the default response is to reboot. If `ForceReboot` is also `True`, the end-user is not given an option and the managed device will do a reboot.

If the dialog times out with no user response, or if it is not displayed because of the `UserInteractionLevel` and `AlwaysDisplayReboot` settings, or if no user is logged on, RayManageSoft Unified Endpoint Manager will reboot automatically if `RebootIfRequired` is `True`.

If the desktop is locked, the installation and adoption agents uses `AllowRebootIfLocked` instead of `RebootIfRequired`.



For details about how this setting works in combination with other installation settings to determine the appropriate reboot action, refer to the *Reboot options* section.

Values / Range:	Boolean (True or False)
Default value:	False

Command-line

Tool:	Adoption agent, installation agent
Example:	-o RebootIfRequired=True

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

RebootPostCommand

Command-line | Registry

This setting specifies the command that is executed after rebooting a managed device using `reboot.exe`. The command specified here is copied to `HKLM\SOFTWARE\ManageSoft Corp\ManageSoft\Common\RunOnce` from where it will be executed by the scheduling agent after the managed device reboots.

Values / Range:	String
Default value:	none
Example value:	chkdsk /f

Command-line

Tool:	Reboot agent
Example:	-a "regsrv32 /s /u C:\filename.dll" will register a DLL

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration



User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

RebootPreCommand

Command-line | Registry

This setting specifies the command that is executed before rebooting a managed device using `reboot.exe`.

Values / Range:	String
Default value:	none
Example value:	cleanmgr

Command-line

Tool:	Reboot agent
Example:	-b "regsrv32 /s /u C:\filename.dll" will register a DLL

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

RebootPromptCycles

Command-line | Registry

This setting specifies the number of time an end-user can postpone the reboot of the managed device initiated by the RMS UEM AppCenter. The postpone cycle is either terminated when the end-user chooses to postpone or reboot or at the conclusion of the period of time that is specified by `RebootPromptWait`. If all postpone cycles have been completed, the final reboot dialog is displayed. The appearance and behavior of the final reboot dialog is based on the settings of the `RebootIfRequired`, `ForceReboot`, and `UITimeoutWait` settings.

If `RebootPromptCycles` is set to 0 (default), the final reboot dialog is presented to the end-user immediately with no options to postpone the reboot. For example, if `RebootPromptCycles` is



set to 2, the postponement dialog is presented to the end-user a maximum of two times. Assuming that the end-user chooses to postpone the reboot each time, after the second postponement, the final reboot dialog will be displayed after the time interval specified by `RebootPromptWait`. The appearance and behavior of this dialog is based on the settings of `RebootIfRequired`, `ForceReboot`, and `UITimeoutWait`.

If both of these settings and `RebootPromptUnlimited` are set, `RebootPromptUnlimited` takes precedence. Configuring this setting to -1 is equivalent to setting `RebootPromptUnlimited=True`. For more information, also refer to [UITimeoutWait](#), [RebootPromptWait](#), [RebootPromptUnlimited](#), [RebootIfRequired](#), [ForceReboot](#), and [AllowTimeoutIfLocked](#).

Values / Range:	Integer
Default value:	0

Command-line

Tool:	Reboot agent
Example:	<code>reboot.exe -p 10</code> <code>reboot.exe -o RebootPromptCycles=10</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Launcher\CurrentVersion</code>

RebootPromptUnlimited

Command-line | Registry

This setting specifies if prompting to reboot will continue until the managed device has rebooted. This is equivalent to `RebootPromptCycles=-1`. If both, `RebootPromptCycles` and `RebootPromptUnlimited` have been set, `RebootPromptUnlimited` will take precedence. For more information, also refer to [UITimeoutWait](#), [RebootPromptWait](#), [RebootIfRequired](#), [ForceReboot](#), [AllowTimeoutIfLocked](#), and [RebootPromptCycles](#).

Values / Range:	Boolean (True or False)
Default value:	False

Command-line



Tool:	Reboot agent
Example:	<code>reboot.exe -u reboot.exe -p -1</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

RebootPromptWait

Command-line | Registry

The time interval in seconds that RayManageSoft Unified Endpoint Manager has to wait before once again displaying the dialog that prompts the end-user to reboot. For more information also refer to [AllowTimeoutIfLocked](#) and [RebootPromptCycles](#).

Values / Range:	Integer greater than zero
Default value:	600

Command-line

Tool:	Reboot agent
Example:	<code>-w 1200</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Recurse

Command-line | Registry

`Recurse` controls whether the inventory agent (ndtrack executable) drills down for inventory collection:



- When set to `True`, the tracker includes folders beneath the top-level folder(s) specified by `IncludeDirectory` **or** `EmbedFileContentDirectory`.
- When set to `False`, the tracker does not recurse folders beneath the top level folder(s). It only tracks files immediately within the folder(s) specified by `IncludeDirectory` or `EmbedFileConentDirectory`.

Values / Range:	Boolean
Default value:	<code>True</code>

Command-line

Tool:	Inventory agent
Example:	<code>-o Recurse=true</code>

Registry

Installed by:	Manual configuration
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp \ManageSoft\Tracker\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Tracker\CurrentVersion</code>



RefreshPeriod

Command-line | Registry

The number of minutes between the automatic refresh of data held by the package selection agent. This refreshes the underlying data and, in the factory supplied user interface, also the tabular data that is displayed to the end-user.

Values / Range:	Numeric greater than zero (number of minutes)
Default value:	5 (minutes)

Command-line

Tool:	Package selection agent
Example:	-o RefreshPeriod=10

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Selector\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Selector\CurrentVersion

ReinstallRequiresVersionChange

Command-line | Registry | Project Variable

Determines when the RMS UEM AppCenter will upgrade, downgrade, or reinstall packages.

If set to `True`, the RMS UEM AppCenter will upgrade, downgrade, or reinstall packages on a managed device if either of the following has changed:

- The version number of the package.
- The MD5 digest calculated for all the package details that apply to this device based on the current platform, language, and architecture (as opposed to the MD5 of the overall package).

This behavior protects against the reinstallation of applications if the package has changed, but if those changes do not affect the current managed device. This still allows self-healing to occur in the event of file corruption and for upgrades to occur when changes to a package do affect the current managed device.

If set to `False`, the RMS UEM AppCenter will upgrade, downgrade, or reinstall packages on a managed device if either of the following has changed:



- The MD5 digest for the entire package.
- The version number of the package.

Values / Range:	Boolean (True or False)
Default value:	True

Command-line

Tool:	Installation agent
Example:	-o ReInstallRequiresVersionChange=False

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuraion
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	ReInstallRequiresVersionChange
Reference as:	\$(ReInstallRequiresVersionChange)

RenotifyTimeout

Command-line | Registry | Project Variable

Determines the length of time in seconds that installation agent dialogs can remain hidden while waiting to time out before they are displayed to the user once more.

Values / Range:	Numeric (seconds)
Default value:	240 (4 minutes)

Command-line

Tool:	Installation agent
Example:	-o RenotifyTimeout=10

Registry



Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	In order of precedence: • HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion • HKEY_CURRENT_USER\SOFTWARE\ManageSoft corp\ManageSoft\Common
Computer setting:	In order of precedence: • [Registry]\ManageSoft\Launcher\CurrentVersion • [Registry]\ManageSoft\Common

Project Variable

Define as:	RenotifyTimeout
Reference as:	\$(RenotifyTimeout)

ReportCompliance

Command-line | Registry



WARNING

This setting should not be changed from the default value of `False` as policy compliance logs are not currently imported by the RMS UEM AppCenter.

If set to `True`, managed devices will generate and upload `.plc` (policy compliance) files. If set to `False`, they will not.

Values / Range:	Boolean
Default value:	<code>False</code>

Command-line

Tool:	Policy agent
Example:	<code>-o ReportCompliance=true</code>

Registry

Installed by:	Installation of Security Manager on managed devices
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion



Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

RetryPolicy

Command-line | Registry

If set to `True`, if no machine schedule exists on the managed device when the managed device is booting, RayManageSoft Unified Endpoint Manager will attempt to retrieve the RayManageSoft Unified Endpoint Manager policy. RayManageSoft Unified Endpoint Manager uses the command within the `RetryPolicyCommand` setting to retrieve the policy. This is useful when performing automatic adoption of managed devices to ensure that the temporary network outages do not halt the RayManageSoft Unified Endpoint Manager adoption process.

If set to `False`, if no machine schedule exists on the managed device when the managed device is booting, RayManageSoft Unified Endpoint Manager will not retrieve the RayManageSoft Unified Endpoint Manager policy.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Scheduling agent
Example:	<code>-o RetryPolicy=False</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Schedule Agent\CurrentVersion

RetryPolicyCommand

Command-line | Registry

If `RetryPolicy` is set to `True`, RayManageSoft Unified Endpoint Manager uses the command stored in `RetryPolicyCommand` to attempt to retrieve the group policy. The policy is either retrieved from the last known policy location, or can be included in the `RetryPolicyCommand` value.

Values / Range:	Any valid policy agent command-line



Default value:	<code>mgspolicy -t Machine</code> <code>-o UserInteractionLevel=Quiet</code>
Example value:	<code>mgspolicy -t Machine</code>

Command-line

Tool:	Scheduling agent
Example:	<code>-o RetryPolicyCommand=mgspolicy</code> <code>-t Machine</code> <code>-o UserInteractionLevel=Quiet</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Schedule Agent\ CurrentVersion

RunInventoryScripts

Command-line | Registry

If `True`, this setting specifies that inventory scripts should be run after managed devices have been inventoried. All scripts located in the location specified by `InventoryScriptsDir` are executed immediately after the inventory data collection is complete.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Inventory agent
Example:	<code>-o RunInventoryScripts=True</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion



SaveAllUserSymbols

Command-line | Registry | Project Variable

Determines whether RayManageSoft Unified Endpoint Manager retains the installation settings set by a top-level or prerequisite catalog.

- If set to `True`, RayManageSoft Unified Endpoint Manager retains the existing values for settings.
- If set to `False`, it saves only the settings used by the current package.

Also see [Persistent Managed Device Preference Settings](#).

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Installation agent
Example:	<code>-o SaveAllUserSymbols=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Launcher\CurrentVersion</code>

Project Variable

Define as:	<code>SaveAllUserSymbols</code>
Reference as:	<code>\$(SaveAllUserSymbols)</code>

SearchFrequency

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

The requesting managed device sends multiple UDP broadcast requests to cater for the fact that some packets may be dropped during transmission and so that it can assemble a number of possible sources from which to retrieve the required files. This setting specifies the time (in tenths of a second) between the requests.



Values / Range:	Integer between 1 - 10
Default value:	10

Command-line

Tool:	Peer download agent
Example:	-debug -o SearchFrequency=5

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader



SearchMaxOffer

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

Since offers to send a requested file might be received from more than one peer, this setting specifies the number of offers of a file to receive from peers before terminating the search. Increasing this number can help distribute the load and reduce file transfer failures, but waiting for more offers can also extend the time that is needed for searching. If the number of offers is reached before the number of requests specified by `SearchMinimum` is reached, additional requests will be sent until the number for `SearchMinimum` is reached.

Values / Range:	Integer between 1 - 10
Default value:	5

Command-line

Tool:	Peer download agent
Example:	<code>-o debug -o SearchMaxOffer=3</code>

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

SearchMinimum

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

The requesting managed device sends multiple UDP broadcast requests to cater for the fact that some packets may be dropped during transmission and so that it can assemble a number of possible sources from which to retrieve required files. This setting specifies the minimum number of requests to send. It will transmit this number of requests even if it receives sufficient offers of the file from peer managed devices before it has sent all requests.

Values / Range:	Integer between 1 - 20
Default value:	2



Command-line

Tool:	Peer download agent
Example:	-debug -o SearchMinimum=5

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

SearchRetry

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

While `SearchMinimum` specifies the number of requests to send for each required file, `SearchRetry`, specifies the time interval (in seconds) between the requests.

Values / Range:	Integer between 60 - 3,600
Default value:	600

Command-line

Tool:	Peer download agent
Example:	-debug -o SearchRetry=1200

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

SecurityPatchRebootIfRequired

Registry | Project Variable

This setting is only used when security patches are being installed. If the installation of a security



patch requires a reboot and the value of this setting is `True`, `RebootIfRequired` is set to `True`.

If this setting is used as a variable in a security package, the **Set variable before processing package** checkbox needs to be checked when creating the package in order to set the variable before the package installation command is run.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	<code>SecurityPatchRebootIfRequired</code>
Reference as:	<code>\$(SecurityPatchRebootIfRequired)</code>

SelectorAlgorithm

Registry

Specifies the algorithms used to assign values to the `Priority` registry keys for download and upload locations.

After application of the nominated algorithms, the managed device will attempt to collect packages from the server with the highest priority. In the event of a connection failure, the managed device uses the other prioritized servers remaining on the list as failover servers.

RayManageSoft Unified Endpoint Manager includes the following algorithms:

- `MgsADSiteMatch`
Moves all servers in the site of the current managed devices to the front of the priority list.
- `MgsBandwidth`
Priorities are based on end-to-end bandwidth availability to the server.
- `MgsDHCP`
Priorities are based on lists of servers specified in DHCP.
- `MgsDomainMatch`
Priorities are determined by the closest match in domain name.
- `MgsIPMatch`



Priorities are determined by the closest IP address match.

- `MgsNameMatch`

Matches prefixes in the computer names.

- `MgsPing`

Priorities are determined by fastest ping response time.

- `MgsRandom`

Random priorities are assigned.

- `MgsServersFromAD`

Priorities are determined according to lists of servers specified in the Active Directory.

- `MgsSubnetMatch`

Moves all servers in the current subnet to the front of the priority list, but still retains the relative order of existing priorities.



Be aware:

Each algorithm may be given an integer parameter that determines the number of servers to which priorities will be assigned to. Some algorithms may also be given an additional Boolean attribute that can cause unmatched servers to be discarded from the list (priority set to the string literal `invalid`). Some algorithms also accept other parameters.

Values / Range:	<code>MgsADSiteMatch, MgsBandwidth, MgsDHCP, MgsDomainMatch, MgsIPMatch, MgsNameMatch, MgsPing, MgsRandom, MgsServersFromAD, MgsSubnetMatch(nDGRandom, nDGDomainMatch, nDGIPMatch; also available for backward compatibility).</code>
Default value:	<code>MgsPing; MgsSubnetMatch</code>
Example value:	• <code>MgsRandom(3)</code> This means that RayManageSoft Unified Endpoint Manager should randomly assign the top three servers (based on the priorities currently assigned). • <code>MgsADSiteMatch(True); MgsSubnetMatch</code> This means that RayManageSoft Unified Endpoint Manager lists servers outside of the site of the current managed device as "invalid" (<code>MgsSubnetMatch</code> will only prioritize valid servers set by <code>MgsADSiteMatch</code>).

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\NetSelector\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\NetSelector\CurrentVersion</code>



SelfHeal

Command-line | Registry | Project Variable

Specifies whether self-healing should occur for an individual package when RayManageSoft Unified Endpoint Manager updates machine or user policies.

- `True` means that all packages on this managed device should self-heal.
- `False` means that no packages on this managed device should self-heal.
- Any other value means that self-healing should be attempted only on packages with a `SelfHeal` property whose value matches this string. For example, if a package has a `SelfHeal` value of `AlwaysHealMe`, and `SelfHeal` on a device is also set to `AlwaysHealMe`, self-healing of that package will occur on that device.

**Be aware:**

If using `SelfHeal` as a package variable, set the **Set variable before processing package** checkbox when creating the package.

Values / Range:	String
Default value:	True

Command-line

Tool:	Installation agent
Example:	<code>-o SelfHeal="False"</code>

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	SelfHeal
Reference as:	<code>\$(SelfHeal)</code>

ServiceConnectTimeout

Registry

This setting controls the amount of time that the `ndserv.exe` has in order to establish a named



pipe connection with the `ndlaunch.exe`. The default value for a timeout is 20 seconds.

Values / Range:	Integer greater than 0 (number of seconds)
Default value:	20
Example value:	30

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

ServiceCreateTimeout

Registry

This setting controls the amount of time that the `ndlaunch.exe` has to establish a named pipe connection with the `ndserv.exe`. The default value for a timeout is 30 seconds.

Values / Range:	Integer greater than 0 (number of seconds)
Default value:	30
Example value:	20

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

SessionBackupPeriod

Command-line | Registry

Specifies how often in seconds the application usage agent will cache already recorded



application usage data. The value must be greater than 0 otherwise the default value will be used.

Values / Range:	Integer greater than 0
Default value:	3600

Command-line

Tool:	Application usage agent
Example:	<code>-o SessionBackupPeriod=90</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

SMBIOSCmdLine

Command-line | Registry

Specifies the command-line used to invoke `smbios2.exe` to gather BIOS information during zero-touch hardware inventory collection. This setting is not used during the normal inventory collection by RayManageSoft Unified Endpoint Manager.

The `smbios2.exe` is a utility developed by IBM that RayManageSoft Unified Endpoint Manager uses to collect a range of information about a computer if WMI is not available on the computer. It is possible to execute `smbios2.exe /h` by hand to obtain information about possible command arguments that can be used with the `smbios2.exe`.

The default value of the `SMBIOSCmdLine` setting includes the `/G` option, which attempts to collect as much information about the computer as possible. The `/G` option collects BIOS information using one particular approach, which very old BIOSes may not support. If old BIOSes are in use within an organization, customizing this preference setting value to use the `/a` option instead of `/G` should be considered. `/a` uses an alternative approach for collecting information which is supported by older BIOSes. However, use of the `/a` option is known to result in problems such as hangs and crashes on some more recent hardware, including many Dell and IBM computers.

Relative paths to executables in this preference setting are treated as relative to the directory containing `ndtrack.exe`.

This setting can be set to an empty value in order to prevent the inventory agent from using the



`smbios2.exe` tool. This results in less BIOS information being collected during zero-touch hardware inventory collection.

The command-line used to execute `smbios2.exe` normally includes `conspawn`, as shown in the default value below. `conspawn` is an executable used by RayManageSoft Unified Endpoint Manager to reliably execute 16-bit DOS applications on various versions of Windows.

In order to successfully use `smbios2.exe` to gather inventory data, `smbios2.exe`, `conspawn.exe`, and `ide21201.vxd` should all exist in the same directory as `ntrack.exe`.

Values / Range:	Any valid command-line that will execute <code>smbios2.exe</code> that results in output being written to standard output. This commandline should include the <code>/l</code> argument.
Default value:	<code>conspawn smbios2.exe /l /G</code>
Example value:	<code>conspawn smbios2.exe /l /a</code>

Command-line

Tool:	Inventory agent
Example:	<code>-t Machine</code> <code>-o SMBIOSCmdLine="conspawn smbios2.exe /l /a"</code>

Registry

Installed by:	RayManageSoft Unified Endpoint Manager internals or manual configuration
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Tracker\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Tracker\CurrentVersion</code>

StageInactivePackages

Command-line | Registry

Used to download (stage) all application files referenced in a policy that is scheduled to be activated some time in the future. This allows packages to be installed immediately once the policy is activated without having to wait for lengthy downloads, as the files have already been unobtrusively downloaded beforehand. If this setting is set to `False`, RayManageSoft Unified Endpoint Manager does not start downloading application files until the policy is activated.

Values / Range:	Boolean (True or False)
Default value:	<code>False</code>



Command-line

Tool:	Installation agent
Example:	-o StageInactivePackages=True

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

StartupDelay

Registry

Specifies the wait time (in seconds) between a managed device booting up and the application usage agent starting. This can be used to delay the application usage agent startup to allow managed devices to boot up faster and provide the end-user with an interactive desktop more quickly. When the application usage agent startup is delayed, any applications executed prior to its initialization will not be tracked as used.

Values / Range:	Integer greater than 0 (number of seconds)
Default value:	0

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Usage Agent\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

StrictInstall

Command-line | Registry

If set to `True`, the policy agent returns a non-zero exit code if any package in policy fails to install. If set to `False`, the policy agent may return a zero exit code even if packages failed to install. Do not use the policy agent's return code to test for success unless this setting is set to `True`.

**WARNING**

Do not use the return code of the policy agent to test for success unless this setting is set to `True`.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	No registry default; default behavior <code>False</code>

Command-line

Tool:	Installation agent
Example:	<code>-o StrictInstall=True</code>

Registry

Installed by:	Manual configuration
User setting:	In order of precedence: • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion</code> • <code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Common</code>
Computer setting:	In order of precedence: • <code>[Registry]\ManageSoft\Launcher\CurrentVersion</code> • <code>[Registry]\ManageSoft\Common</code>



SupplyWorstCaseReturnValue

Command-line | Registry | Project Variable

If set to `False`, RayManageSoft Unified Endpoint Manager only returns an error when an installation agent operation fails regardless of whether the installation is successful or not.

If set to `True`, an error is reported if an installation fails during an application self-heal, revision, or upgrade.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Installation agent
Example:	<code>-o SupplyWorstCaseReturnValue=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	<code>SupplyWorstCaseReturnValue</code>
Reference as:	<code>\$(SupplyWorstCaseReturnValue)</code>

TrustDatabaseFxd

Registry

If set to `True`, trusted and excluded locations can only be changed by users with administrator privileges. If set to `False` or if this setting has not been configured on the managed device, RayManageSoft Unified Endpoint Manager allows any user to change the trusted and excluded locations.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>



Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

UITimeoutWait

Command-line | Registry

Determines the number of seconds that a RayManageSoft Unified Endpoint Manager installation agent dialog displays before timing out and automatically selecting the default response. The first dialog to time out will do so after the specified period (or never, if the time out period is set to 0 seconds). Subsequent dialogs will time out after a maximum of 60 seconds. For example, if the time out period is set to 300 seconds and the first dialog does time out after 300 seconds, subsequent dialogs will time out after 60 seconds.

For details about how this setting works in combination with other installation settings to determine appropriate reboot actions, see [Reboot Options](#).

Values / Range:	Integer greater than 0 (number of seconds)
Default value:	300

Command-line

Tool:	Installation agent
Example:	-o UITimeoutWait=30

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

UnusedFilePersistence

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing



(AllowPeerToPeer is True).

Files will be deleted from the peer cache during clean up operations if they have not been accessed for more than the number of hours specified by this setting.

This setting also influences when the cleanup operations are started. Cleanup operations do not start immediately when a managed device starts up as this may result in the peer cache being cleaned out on managed devices that have been turned off for long periods. Instead, cleanup operations are started as soon as one of the following is true:

- One hour has elapsed after RayManageSoft Unified Endpoint Manager has last requested file downloads
- One quarter of the time specified by this setting has passed since the managed device started up. For example, if this setting is set to 120, cleanup operations will start after the managed device has been active for 30 hours if they have not been started earlier.

Values / Range:	Integer between 24 and 8,760
Default value:	120

Command-line

Tool:	Peer download agent
Example:	-debug -o UnusedFilePersistence=240

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

UnusedFileUptime

Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (AllowPeerToPeer is True).

It specifies how long (in minutes) to wait after receiving the first request from the installation agent before starting to look for and delete unused files.

Values / Range:	Integer between 0 and 1,440
Default value:	60



Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader



UploadPeriod

Command-line | Registry

Specifies how often (in seconds) the application usage agent will upload recorded application usage data to the specified server. The value must be greater than 0 otherwise the default value will be used.

Values / Range:	Integer greater than 0 (in seconds)
Default value:	86400

Command-line

Tool:	Application usage agent
Example:	-o UploadPeriod=3600

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

UsageDirectory

Registry

Specifies the directory under which a cache for application usage data is created before it is uploaded to the administration server.

**WARNING**

This setting should not be changed by the user as it is set during the installation.

Values / Range:	Valid location
Default value:	\$(CommonAppDataFolder)\ManageSoft Corp\ManageSoft \Usage Agent\UsageData

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)



User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

UseAddRemove

Command-line | Registry

This setting is only applicable for Windows devices.

If set to `True`, RayManageSoft Unified Endpoint Manager records application usage data for applications that are detected from **Add/Remove Programs**. If set to `False`, RayManageSoft Unified Endpoint Manager does not use **Add/Remove Programs** to detect applications.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Application usage agent
Example:	<code>-o UseAddRemove=True</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

UseManualMapper

Command-line | Registry

If set to `True`, RayManageSoft Unified Endpoint Manager records application usage data for applications that are detected from the Manual Mapper registry keys. If set to `False`, RayManageSoft Unified Endpoint Manager does not use the Manual Mapper registry keys to detect applications.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>



Command-line

Tool:	Application usage agent
Example:	-o UseManualMapper=True

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

UseMGS

Command-line | Registry

This setting is only applicable for Windows devices.

If set to `True`, RayManageSoft Unified Endpoint Manager records application usage data for applications that are detected from the RayManageSoft Unified Endpoint Manager application cache. If set to `False`, RayManageSoft Unified Endpoint Manager does not use the application cache to detect applications.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>

Command-line

Tool:	Application usage agent
Example:	-o UseMGS=False

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion



UseMSI

Command-line | Registry

If set to `True`, RayManageSoft Unified Endpoint Manager records application usage data for applications that are detected in the native package format (MSI, RPM, or PKG). If set to `False`, RayManageSoft Unified Endpoint Manager does not use the native package format when detecting applications.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>

Command-line

Tool:	Application usage agent
Example:	<code>-o UseMSI=False</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

UserLogonDomain

Registry | Project Variable

Domain name of the user. For managed devices running Windows 2000 or later, this is automatically configured during the adoption of the managed device

Values / Range:	The canonical domain name of the user. Read-only!
Default value:	The default is the value retrieved from Windows.
Example value:	<code>mycompany.com</code>

Registry

Installed by:	Windows 2000 or later
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Common



Computer setting:	[Registry]\ManageSoft\Common

Project Variable

Define as:	Predefined on operating systems supporting Active Directory.
Reference as:	\$(UserLogonDomain)

UserProcessesOnly

Command-line | Registry

If set to `True`, RayManageSoft Unified Endpoint Manager only records application usage data for applications run by users other than `SYSTEM` (or `root` in non-Windows environments). If set to `False`, RayManageSoft Unified Endpoint Manager records application usage data for all applications.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>True</code>

Command-line

Tool:	Application usage agent
Example:	<code>-o UserProcessesOnly=False</code>

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Usage Agent\ CurrentVersion

UseTrustDatabase

Command-line | Registry | Project Variable

If the installation agent is deciding whether to install a package, this setting specifies if the distribution location from where the files are collected is taken into consideration. If set to `True`, the installation agent will check whether the distribution location from which a RayManageSoft Unified Endpoint Manager catalog (`.osd` file) is collected is a trusted location.

A related setting for User settings in the registry will override the machine settings unless the machine settings are locked. Also refer to [Fixing Managed Device Settings](#).

**Note:**

If `VerifyTrustOrSign` is `True`, this setting will be ignored.

Values / Range:	Boolean (True or False)
Default value:	False

Command-line

Tool:	Installation agent
Example:	<code>-o UseTrustDatabase=True</code>

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	<code>UseTrustDatabase</code>
Reference as:	<code>\$(UseTrustDatabase)</code>

VerifyCatalogSigned

Command-line | Registry | Project Variable

If set to `True`, the installation agent uses Authenticode to check the digital signature referenced in the implementation archive before installing a package. RayManageSoft Unified Endpoint Manager implementation archives have the extension `.ndc`. If set to `False`, RayManageSoft Unified Endpoint Manager does not check the digital signature before installing a package.

A related setting for User settings in the registry will override the machine settings unless the machine settings are locked. Also refer to [Fixing Managed Device Settings](#).

**Note:**

If `VerifyTrustOrSign` is `True`, this setting will be ignored.

Values / Range:	Boolean (True or False)
Default value:	False



Command-line

Tool:	Installation agent
Example:	-o VerifyCatalogSigned=True

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	VerifyCatalogsigned
Reference as:	\$(VerifyCatalogsigned)

VerifyFilesSigned

Command-line | Registry | Project Variable

If set to `True`, RayManageSoft Unified Endpoint Manager checks for a valid Authenticode digital signature in executable files that it downloads before it installs them. If set to `False`, RayManageSoft Unified Endpoint Manager does not check executable files for a valid digital signature.

Values / Range:	Boolean (<code>True</code> or <code>False</code>)
Default value:	<code>False</code>

Command-line

Tool:	Installation agent
Example:	-o VerifyFilesSigned=True

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion



Project Variable

Define as:	VerifyFilesSigned
Reference as:	\$(VerifyFilesSigned)

VersionInfo

Command-line | Registry

If set to `True`, RayManageSoft Unified Endpoint Manager includes the file version header information in the inventory. If set to `False`, RayManageSoft Unified Endpoint Manager does not include the file version header information in the inventory.

Values / Range:	Boolean (True or False)
Default value:	True

Command-line

Tool:	Inventory agent
Example:	-o VersionInfo=False

Registry

Installed by:	Manual configuration
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Tracker\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Tracker\CurrentVersion

VirusScan

Command-line | Registry | Project Variable

If set to `True`, RayManageSoft Unified Endpoint Manager scans the downloaded files for viruses before the installation. The `VirusScanCommand` setting defines the virus checking mechanism that is being used. If set to `False`, RayManageSoft Unified Endpoint Manager does not scan the files for viruses.

Values / Range:	Boolean (True or False)
Default value:	False

Command-line



Tool:	Installation agent
Example:	-o VirusScan=True

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)
User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	VirusScan
Reference as:	\$(VirusScan)

VirusScanCommand

Command-line | Registry | Project Variable

This option is only available if `VirusScan` is set to `True`.

Determines the virus scan application that is being used and the location of its binaries. RayManageSoft Unified Endpoint Manager uses this value to run the virus scanning application. The value should either be enclosed in quotes or use short file names for folder names that are long or contain spaces.

Values / Range:	Valid executable file and path
Default value:	No default
Example value:	C:\PROGRA~1\Vet\vet.exe

Command-line

Tool:	Installation agent
Example:	-o VirusScanCommand=C:\PROGRA~1\Vet\vet.exe

Registry

Installed by:	Installation of RayManageSoft Unified Endpoint Manager on a managed device (Computer setting)



User setting:	HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp\ ManageSoft\Launcher\CurrentVersion
Computer setting:	[Registry]\ManageSoft\Launcher\CurrentVersion

Project Variable

Define as:	VirusScanCommand
Reference as:	\$(VirusScanCommand)

WANAverageingTime

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (AllowPeerToPeer is True).

It is used in conjunction with [WANMaxRate](#) to limit bandwidth used for downloading files from the distribution server. It specifies the average period of time (in minutes) used to smooth the estimate of transfers to and from the distribution server. For information on how to use these settings together, see [WANMaxRate](#). Increasing the value of this setting means, that the estimate takes longer to change as the actual transfer rate changes. In normal use, changing this value will not be necessary.

The value of this setting is being retrieved from the registry every five seconds. Therefore, it is not necessary to restart RayManageSoft Unified Endpoint Manager on managed devices after changing the value of this setting.

Values / Range:	Integer between 1 - 60
Default value:	10

Command-line

Tool:	Peer download agent
Example:	-debug -o WANAverageingTime=10

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader



WANMaxRate

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

It specifies the maximum allowable rate (in bytes per second) for transfers from distribution servers across all peers in this subnet. `WANMaxRate` is used in conjunction with `WANAveragingTime` to limit the bandwidth used between the distribution server and the group of managed devices that is downloading the files.

RayManageSoft Unified Endpoint Manager calculates the sum of file transfers that have occurred between the distribution server and the peer group of managed devices to which this device belongs. Since transfers occur in blocks and not as a continuous stream, RayManageSoft Unified Endpoint Manager will smooth out the variation in transfer rates using the `WANAveragingTime` settings and a simple exponential algorithm. The result is an estimate of the transfer rate. Transfer rates will be decreased if the estimated rate exceeds the specified `WANMaxRate` and will be increased if they are below the specified `WANMaxRate` (Transfers can creep up to the `WANMaxRate`, but will drop back rapidly when the estimated rate is greater than `WANMaxRate`).

The value of this setting is being retrieved from the registry every five seconds. Therefore, it is not necessary to restart RayManageSoft Unified Endpoint Manager on managed devices after changing the value of this setting.

Values / Range:	Integer between 1,024 - 134,217,728
Default value:	16777216

Command-line

Tool:	Peer download agent
Example:	<code>-debug -o WANMaxRate=2048</code>

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader



WANProgressInterval

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

It specifies the frequency (in seconds) with which to send the progress announcements to the peer managed devices about file downloads from the distribution server. This setting only controls the frequency of progress messages while the download operation is in progress. The messages sent at the completion of a download are sent immediately.

Values / Range:	Integer between 1 - 90
Default value:	10

Command-line

Tool:	Peer download agent
Example:	<code>-debug -o WANProgressInterval=30</code>

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

WANRetries

Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

It specifies how many times a failed WAN download is immediately retried from each distribution server at each WAN retry interval.

Values / Range:	Integer between 0 - 10
Default value:	1

Registry

Installed by:	Manual configuration



User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

WANRetryDuration

Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (AllowPeerToPeer is True).

It specifies how long (in minutes) to continue to allow a file to be retried for download since it was last requested by the installation agent.

Values / Range:	Integer between 0 - 43,200
Default value:	1440

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

WANRetryInterval

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (AllowPeerToPeer is True).

It specifies how long (in seconds) RayManageSoft Unified Endpoint Manager will retry the download after a WAN download has failed.

Values / Range:	Integer between 10 - 86,400
Default value:	300

Command-line

Tool:	Peer download agent
Example:	-debug -o WANRetryInterval=30



Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

WANSearchCurrency

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer is True`).

If peer-to-peer file sharing is enabled, files that are available from a peer managed device will always be downloaded from the peer rather than from the distribution server. This setting specifies how frequently a device will ask if it peers for a file. For example, if a managed device called BOSTON asks its peers for the file `MyDownload.txt` and `WANSearchCurrency` is set to 30, the managed device will not reissue a request for `MyDownload.txt` within 30 seconds of its first request. Instead of requesting the file again, BOSTON would download the file from the closest distribution server.

Avoiding Lock Conditions

The interactions between `ParentConnectionWindows`, `PeerConnectionWindows`, and `WANSearchCurrency` need to be taken into consideration in order to avoid lock conditions. For example, if using the following settings for the settings, a lock condition might occur:

- `ParentConnectionWindows` allows file downloads between 3 am and 6 am.
- `PeerConnectionWindows` allows file downloads between 10 am and 12 pm.
- `WANSearchCurrency` is set to 4 hours.

Under this configuration the peer download agent might:

- Request a file from peers at 12 pm and fail to option it.
- Do nothing until the start of the permitted parent connection time window at 3 am.

At 3 am it will check `WANSearchCurrency` and then find that it must perform a peer search before downloading the file from a parent managed device, since the time interval since the last conducted peer search is greater than 4. The peer download agent must now wait until the next permitted peer connection time window to request the file.

Values / Range:	Integer between 1 - 600
Default value:	30

Command-line



Tool:	Peer download agent
Example:	-debug -o WANSearchCurrency=100

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

Project Variable

Define as:	AddRemove
Reference as:	\$ (AddRemove)

WANTimeout

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

It specifies the time (in seconds) after which to abort stalled transfers of files from distribution server.

Values / Range:	Integer between 1 - 600
Default value:	30

Command-line

Tool:	Peer download agent
Example:	-debug -o WANTimeout=10

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader



WANTransferLimit

Command-line | Registry

This setting is only used if managed devices are configured for peer-to-peer file sharing (`AllowPeerToPeer` is `True`).

It specifies the number of managed devices that can simultaneously download files from a distribution location.

Before downloading any files from a distribution location, the managed device checks how many peers in this subnet are currently downloading across the network. The managed device will not start downloading across the network, if the number of managed devices currently downloading is equal to or greater than the `WANTransferLimit` setting for the device.

Values / Range:	Integer between 1 - 100
Default value:	3

Command-line

Tool:	Peer download agent
Example:	<code>-debug -o WANTransferLimit=10</code>

Registry

Installed by:	Manual configuration
User setting:	Not available
Computer setting:	[Registry]\ManageSoft\Downloader

WMI

Command-line | Registry | Project Variable

This option is Windows only!

When set to `True`, the Windows Management Instrumentation (WMI) tracking is specified as the preferred option of tracking hardware. In this case, if WMI is not available (and the Hardware preference is set to `True`), RayManageSoft Unified Endpoint Manager will attempt to track hardware using a native API.

When set to `False`, RayManageSoft Unified Endpoint Manager will use another tracking mechanism instead of WMI.

Values / Range:	Boolean



Default value:	The default when running in machine context is <code>True</code> . The default when running in user context is <code>False</code> .

Command-line

Tool:	Inventory agent
Example:	<code>-o WMI=True</code>

Registry

Installed by:	Manual configuration
User setting:	<code>HKEY_CURRENT_USER\SOFTWARE\ManageSoft Corp \ManageSoft\Tracker\CurrentVersion</code>
Computer setting:	<code>[Registry]\ManageSoft\Tracker\CurrentVersion</code>



Appendix II: Logging on Managed Devices

This section contains information about logging in RayManageSoft Unified Endpoint Manager. It is divided into two different parts.

- [Windows agent](#)
- [macOS agent](#)

Windows Agent

The following chapter describes how logging works for the Windows agent.

The significant registry values for logging are as follows:

- **LogFile** - The filename in which the log is saved.
- **LogLevel** - The categories of information that are to be logged. Set this value to **A-Z** in order to log everything.
- **LogModules** - The modules through which RMS UEM AppCenter events are logged.
- **LogMsgCatPath** - The location of the messages catalog to use for log message translation (only 8 bit locales are supported).
- **LogFileSize** - The maximum size for the log file. When the file reaches this size, it will be moved to **LogFileOld** and a new file will be created.
- **LogFileOld** - The name under which the old log files are stored.

Feature	Registry Key
Application usage agent	HKLM\SOFTWARE\ManageSoft corp\ManageSoft\Usage Agent\CurrentVersion
Data reporting agent	HKLM\SOFTWARE\ManageSoft corp\ManageSoft\Uploader\CurrentVersion
Installation agent	HKLM\SOFTWARE\ManageSoft corp\ManageSoft\Launcher\CurrentVersion
Inventory agent	HKLM\SOFTWARE\ManageSoft corp\ManageSoft\Tracker\CurrentVersion
RMS UEM AppCenter	HKLM\SOFTWARE\ManageSoft corp\ManageSoft\Selector\CurrentVersion
Policy agent	HKLM\SOFTWARE\ManageSoft corp\ManageSoft\Policy Client\CurrentVersion



Feature	Registry Key
Scheduling agent	HKLM\SOFTWARE\ManageSoft corp\ManageSoft\Schedule Agent \CurrentVersion

Logging Types and Sublevels

The following tables describe each of the logging types and sublevels available. For example, in order to request icon logging, the `LogLevel` setting should be configured as `G7`.

It is possible to combine different sublevels. The following ways of combining exist:

- References to different logging types can be separated with semi-colons. It is not possible to include more than one reference of the same logging type to the list. For example:
 - `G0;N4` - This is a valid combination.
 - `G0;N4;G1` - This is invalid as there are two references of the `G` logging type.
- References to different sublevels can be separated by commata. For example: `G0, 5, 9`.
- A range of sublevels (within the same type) can be expressed with a hyphen. For example: `G1-3, 9;N4;A`.

General Logging - G

Sublevel	Description
0	Miscellaneous general information
1	Base URL information
2	Versioning
3	Digital Signatures information
4	Virus Checking
5	Staging of downloaded files
6	Status information
7	Icon information
8	Auto
9	File / Directory information

User Interface Logging - U

Sublevel	Description
0	Miscellaneous user interface information

Network Logging - N



Sublevel	Description
0	Miscellaneous network information
1	Dialup information

Verification Logging - V

Sublevel	Description
0	Miscellaneous verification information

Security Logging - S

Sublevel	Description
0	Miscellaneous security information
1	Security matching (such as trusted URL location)

Preference Logging - P

Sublevel	Description
0	Miscellaneous preference information
1	Retrieval (Get)

Schedule Logging - A

Sublevel	Description
0	Miscellaneous schedule information

Callout Logging -C

Sublevel	Description
0	Internal callout information
1	External callout information

MacOS Agent

The following chapter describes how logging works for the MacOS agent.



Appendix III: Update Policies for Windows Devices

Name	Source	Type
Notify to download updates	Administrator	Group Policy
Set when Active Hours start	Administrator	Group Policy
Set when Active Hours end	Administrator	Group Policy
Specifies target server to host updates	Administrator	Group Policy
Branch readiness level	Administrator	Group Policy
Enable quality update deferral	Administrator	Group Policy
Quality update deferral period	Administrator	Group Policy
Enable feature update deferral period	Administrator	Group Policy
Feature update deferral period	Administrator	Group Policy
Enable drivers from Windows quality updates	Administrator	Group Policy
Set Automatic Update options	Administrator	Group Policy

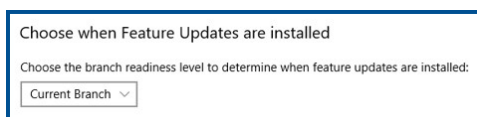
Service Channel Configuration

Policy	Registry Key
GPO for Windows 10 version 1607 or later: Computer Configuration > Administrative Templates > Windows Components > Windows Update > Windows Update for Business > Select when Feature Updates are received	HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\BranchReadinessLevel
GPO for Windows 10 version 1511: Computer Configuration > Administrative Templates >	HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\DeferUpgrade



Policy	Registry Key
Windows Components > Windows Update > Defer Upgrades and Updates	
MDM for Windows 10, version 1607 or later: .../Vendor/MSFT/Policy/Config/Update/BranchReadinessLevel	HKLM\SOFTWARE\Microsoft\PolicyManager\default\Update/BranchReadinessLevel
MDM for Windows 10 version 1511: .../Vendor/MSFT/Policy/Config/Update/RequireDeferUpgrade	HKLM\SOFTWARE\Microsoft\PolicyManager\default\Update\RequireDeferUpgrade

Windows 10 version 1703 and later enables users to configure the branch readiness level for a device using **Settings > Update & security > Windows Update > Advanced options**.





Note:
If configured by policy, this setting cannot be changed by the user.

Feature Updates Reception Configuration

The maximum number of days that a feature update can be deferred is 365 days from the date of their availability from Microsoft on Windows Update.

Policy	Registry Key
GPO for Windows 10 version 1607 or later: Computer Configuration > Administrative Templates > Windows Components > Windows Update > Windows Update for Business > Select when Feature Updates are received	HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\DeferFeatureUpdates HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\DeferFeatureUpdatesPeriodInDays
GPO for Windows 10 version 1511:	HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\DeferUpgradePeriod



Policy	Registry Key
Computer Configuration > Administrative Templates > Windows Components > Windows Update > Defer Upgrades and Updates	
MDM for Windows 10, version 1607 or later: .../Vendor/MSFT/Policy/Config/Update/DeferFeatureUpdatesPeriodInDays	HKLM\SOFTWARE\Microsoft\PolicyManager\default\Update\DeferFeatureUpdatesPeriodInDays
MDM for Windows 10 version 1511: .../Vendor/MSFT/Policy/Config/Update/DeferUpgrade	HKLM\SOFTWARE\Microsoft\PolicyManager\default\Update\RequireDeferUpgrade



Note:

It is possible for individual users to defer feature updates by using **Settings > Update & security > Windows Update > Advanced options** if not configured by policy.

Pause Feature Updates Configuration

When a pause has been configured, the pause setting will automatically expire after a period of 35 days.

Policy	Registry Key
GPO for Windows 10 version 1607 or later: Computer Configuration > Administrative Templates > Windows Components > Windows Update > Windows Update for Business > Select when Feature Updates are received	1607: HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\PauseFeatureUpdates 1703 and later: HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\PauseFeatureUpdatesStartTime
GPO for Windows 10 version 1511: Computer Configuration > Administrative Templates > Windows Components > Windows Update > Defer	HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\Pause



Policy	Registry Key
Upgrades and Updates	
MDM for Windows 10, version 1607 or later: .../Vendor/MSFT/Policy/Config/Update/PauseFeatureUpdates	1607: HKLM\SOFTWARE\Microsoft\PolicyManager\default\Update\PauseFeatureUpdates 1703 and later: HKLM\SOFTWARE\Microsoft\PolicyManager\default\Update\PauseFeatureUpdatesStartTime
MDM for Windows 10 version 1511: .../Vendor/MSFT/Policy/Config/Update/DeferUpgrade	HKLM\SOFTWARE\Microsoft\PolicyManager\default\Update\Pause

The date feature updates were paused can be found in the `PausedFeatureDate` registry key under `HKLM\SOFTWARE\Microsoft\WindowsUpdate\UpdatePolicy\Settings`.

If a device has resumed feature updates or not, can be checked in the `PausedFeatureStatus` registry key under `HKLM\SOFTWARE\Microsoft\WindowsUpdate\UpdatePolicy\Settings`.

Value	Status
0	Not paused
1	Paused
2	Automatically resumed after being paused



Note:

It is possible for individual users to pause feature updates by using **Settings > Update & security > Windows Update > Advanced options** if not configured by policy.

Quality Updates Reception Configuration

The reception of quality updates can be deferred for a period of up to 30 days from their release. Usually, quality updates are published monthly on the second Tuesday of the month.

Policy	Registry Key
GPO for Windows 10 version 1607 or later: Computer Configuration > Administrative Templates >	HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\DeferQualityUpdates HKLM\SOFTWARE\Policies\Microsoft\Windows\



Policy	Registry Key
Windows Components > Windows Update > Windows Update for Business > Select when Quality Updates are received	WindowsUpdate\DeferQualityUpdatesPeriodInDays
GPO for Windows 10 version 1511: Computer Configuration > Administrative Templates > Windows Components > Windows Update > Defer Upgrades and Updates	HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\DeferUpgradePeriod
MDM for Windows 10, version 1607 or later: .../Vendor/MSFT/Policy/Config/Update/DeferQualityUpdatesPeriodInDays	HKLM\SOFTWARE\Microsoft\PolicyManager\default\Update\DeferQualityUpdatesPeriodInDays
MDM for Windows 10 version 1511: .../Vendor/MSFT/Policy/Config/Update/DeferUpgrade	HKLM\SOFTWARE\Microsoft\PolicyManager\default\Update\RequireDeferUpgrade



Note:

It is possible for individual users to defer quality updates by using **Settings > Update & security > Windows Update > Advanced options** if not configured by policy.

Pause Quality Updates Configuration

When a pause has been configured, the pause setting will automatically expire after a period of 35 days.



Note:

IT administrators are able to prevent users from pausing updates starting with Windows 10, version 1809.

Policy	Registry Key
GPO for Windows 10 version 1607 or later: Computer Configuration >	1607: HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\PauseQualityUpdates



Policy	Registry Key
Administrative Templates > Windows Components > Windows Update > Windows Update for Business > Select when Quality Updates are received	1703 and later: HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\PauseQualityUpdatesStartTime
GPO for Windows 10 version 1511: Computer Configuration > Administrative Templates > Windows Components > Windows Update > Defer Upgrades and Updates	HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\Pause
MDM for Windows 10, version 1607 or later: .../Vendor/MSFT/Policy/Config/Update/PauseQualityUpdates	1607: HKLM\SOFTWARE\Microsoft\PolicyManager\default\Update\PauseQualityUpdates 1703 and later: HKLM\SOFTWARE\Microsoft\PolicyManager\default\Update\PauseQualityUpdatesStartTime
MDM for Windows 10 version 1511: .../Vendor/MSFT/Policy/Config/Update/DeferUpgrade	HKLM\SOFTWARE\Microsoft\PolicyManager\default\Update\Pause

The date quality updates were paused can be found in the `PausedQualityDate` registry key under `HKLM\SOFTWARE\Microsoft\WindowsUpdate\UpdatePolicy\Settings`.

If a device has resumed quality updates or not, can be checked in the `PausedQualityStatus` registry key under `HKLM\SOFTWARE\Microsoft\WindowsUpdate\UpdatePolicy\Settings`.

Value	Status
0	Not paused
1	Paused
2	Automatically resumed after being paused



Note:

It is possible for individual users to pause quality updates by using **Settings > Update & security > Windows Update > Advanced options** if not configured by policy.



Windows Insider Preview Configuration

Windows 10 version 1709 and later:

- **Group Policy: Computer Configuration > Administrative Templates > Windows Components > Windows Update > Windows Update for Business > Manage preview builds**
- **MDM:** Update/ManagePreviewBuilds
- **Microsoft Endpoint Configuration Manager:** Enable dual scan, manage through **Windows Update for Business** policy



Note:

This policy replaces the **Toggle user control over Insider builds** policy which is only supported up to Windows 10, version 1703.

- **Group Policy: Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds > Toggle user control over Insider builds**
- **MDM:** System/AllowBuildPreview

It is possible to defer or pause the delivery using the policy setting used to **Select when Feature Updates are received**.

- **Group Policy: Computer Configuration > Administrative Templates > Windows Components > Windows Update > Windows Update for Business > Select when Preview Builds and Feature Updates are received**
- **MDM:** Update/BranchReadinessLevel



Exclusion of Drivers from Quality Updates

Drivers can be excluded from quality updates starting with Windows 10, version 1607. This does not apply to drivers which are critical for the operating system.

Policy	Registry Key
GPO for Windows 10 version 1607 or later: Computer Configuration > Administrative Templates > Windows Components > Windows Update > Do not include drivers with Windows updates	HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\ExcludeWUDriverInQualityUpdate
MDM for Windows 10 version 1607 or later: .../Vendor/MSFT/Policy/Config/Update/ExcludeWUDriverInQualityUpdate	HKLM\SOFTWARE\Microsoft\PolicyManager\default\Update\ExcludeWUDriverInQualityUpdate

Summary Group Policy Settings Windows 10 version 1703 or later

HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate

GPO Key	Key Type	Value
BranchReadinessLevel	REG_DWORD	2: Feature updates for the <i>Windows Insider built - Fast</i> (added in Windows 10 version 1709) are used 4: Feature updates for the <i>Windows Insider built - Slow</i> (added in Windows 10 version 1709) are used 8: Feature updates for the <i>Windows Insider built</i> (added in Windows 10 version 1709) are used 16: Windows 10 version 1703 - Feature Updates for the Current Branch are used Windows 10 version 1709, 1803, and 1809 - Feature updates from the Semi-Annual Channel (Targeted) (SAC-T) are used Windows 10 version 1903 or later - Feature updates from the Semi-Annual



GPO Key	Key Type	Value
		Channel are used 32: Feature updates from the Semi-Annual Channel are used Other value or absent: All applicable updates are used
DeferQualityUpdates	REG_DWORD	1: defer quality updates Other value or absent: do not defer quality updates
DeferQualityUpdates PeriodinDays	REG_DWORD	0 - 35: defer quality updates by given days
PauseQualityUpdates StartTime	REG_DWORD	1: pause quality updates Other value or absent: do not pause quality updates
DeferFeatureUpdates	REG_DWORD	1: defer feature updates Other value or absent: do not defer feature updates
DeferFeatureUpdates PeriodinDays	REG_DWORD	0 - 365: defer feature updates by given days
PauseFeatureUpdates Starttime	REG_DWORD	1: pause feature updates Other value or absent: do not pause feature updates
ExcludeWUDriverIn QualityUpdate	REG_DWORD	1: exclude Windows Update drivers Other value or absent: offer Windows Update drivers

Summary MDM Settings Windows 10 version 1703 or later

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default\Update

GPO Key	Key Type	Value
BranchReadinessLevel	REG_DWORD	2: Feature updates for the <i>Windows Insider built - Fast</i> (added in Windows 10 version 1709) are used 4: Feature updates for the <i>Windows Insider built - Slow</i> (added in Windows 10 version 1709) are used 8: Feature updates for the <i>Windows Insider built</i> (added in Windows 10 version 1709) are used 16: Windows 10 version 1703 - Feature



GPO Key	Key Type	Value
		Updates for the Current Branch are used Windows 10 version 1709, 1803, and 1809 - Feature updates from the Semi-Annual Channel (Targeted) (SAC-T) are used Windows 10 version 1903 or later - Feature updates from the Semi-Annual Channel are used 32: Feature updates from the Semi-Annual Channel are used Other value or absent: All applicable updates are used
DeferQualityUpdatesPeriodinDays	REG_DWORD	0 - 35: defer quality updates by the given number of days
PauseQualityUpdatesStartTime	REG_DWORD	1: pause quality updates Other value or absent: do not pause quality updates
DeferFeatureUpdatesPeriodinDays	REG_DWORD	0 - 365: defer feature updates by the given number of days
PauseFeatureUpdatesStarttime	REG_DWORD	1: pause feature updates Other value or absent: do not pause feature updates
ExcludeWUDriverInQualityUpdate	REG_DWORD	1: exclude Windows Update drivers Other value or absent: offer Windows Update drivers

WSUS Environment Options

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate

Entry Name	Data Type	Values
ElevateNonAdmins	Reg_DWORD	Range = 1 0 1 = Updates can be allowed or disapproved by users in the Users security group. 0 = Updates can be allowed or disapproved by users in the Administrators group only.
TargetGroup	Reg_String	Name of the group of which the device is a part of. This is used for client-side targeting. Paired with the TargetGroupEnabled policy.



Entry Name	Data Type	Values
TargetGroupEnabled	Reg_DWORD	Range = 1 0 1 = Client-side targeting is used. 0 = Client-side targeting is not used. Paired with the <code>TargetGroup</code> policy.
WUServer	Reg_String	The URL (http or https) of the WSUS server used by API callers by default and by Automatic Updates. Paired with the <code>WUStatusServer</code> policy. In order to be valid, they must contain the same value.
WUStatusServer	Reg_String	The URL (http or https) of the server to which client computers send their reporting information if using the WSUS server configured by the <code>WUServer</code> key. Paired with the <code>WUServer</code> policy. In order to be valid, they must contain the same value.

Automatic Update Configuration Options

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU

Entry Name	Data Type	Values
AUOptions	Reg_DWORD	Range = 2 3 4 5 2 = Notify before download 3 = Download automatically and notify of installation 4 = Download automatically and scheduled installation (only valid if <code>ScheduledInstallDay</code> and <code>ScheduledInstallTime</code> exist) 5 = Automatic updates that can be configured by the end-user
AutoInstallMinor Updates	Reg_DWORD	Range = 0 1 0 = Minor updates are treated the same way as other updates 1 = Install minor updates silently
DetectionFrequency	Reg_DWORD	Range = 1 - 22 (time in hours) This value represents the time between the detection cycles.
DetectionFrequency Enabled	Reg_DWORD	Range = 0 1 0 = <code>DetectionFrequency</code> disabled (default



Entry Name	Data Type	Values
		value [22] is used) 1 = DetectionFrequency enabled
NoAutoRebootWithLoggedOnUsers	Reg_DWORD	Range = 0 1 0 = User will be notified about a restart (restart will occur after 5 minutes) 1 = Logged-on user can choose to restart the computers
NoAutoUpdate	Reg_DWORD	Range = 0 1 0 = Automatic Updates enabled 1 = Automatic Updates disabled
RebootRelaunchTimeout	Reg_DWORD	Range = 1 - 1440 (time in minutes) This value represents the time between prompts for a scheduled restart.
RebootRelaunchTimeout Enabled	Reg_DWORD	Range = 0 1 0 = RebootRelaunchTimeout disabled (default value [10] is used) 1 = RebootRelaunchTimeout enabled
RebootWarningTimeout	Reg_DWORD	Range = 1 - 30 (time in minutes) This value represents the time for the restart warning countdown after updates with a deadline or scheduled updates have been installed.
RebootWarningTimeout Enabled	Reg_DWORD	Range = 0 1 0 = RebootWarningTimeout disabled (default value [5] is used). 1 = RebootWarningTimeout enabled
RescheduleWaitTime	Reg_DWORD	Range = 1 - 60 (time in minutes) This value represents the time the Automatic Updates wait after startup before applying missed updates. This only applies to scheduled installations not to updates with an expired deadline.
RescheduleWaitTime Enabled	Reg_DWORD	Range = 0 1 0 = RescheduleWaitTime disabled (the missed installation will be reattempted during the next scheduled installation time) 1 = RescheduleWaitTime enabled
ScheduledInstallDay	Reg_DWORD	Range = 0 1 2 3 4 5 6 7 0 = every day 1 = Sunday

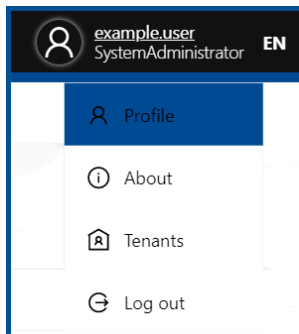


Entry Name	Data Type	Values
		2 = Monday 3 = Tuesday 4 = Wednesday 5 = Thursday 6 = Friday 7 = Saturday In order to apply, the value of <code>AUOptions</code> has to be 4.
<code>ScheduledInstallTime</code>	<code>Reg_DWORD</code>	Range = 0 - 23 (time of day in 24h-format)
<code>UseWUService</code>	<code>Reg_DWORD</code>	Range = 0 1 0 = <code>WUService</code> disabled 1 = <code>WUService</code> enabled



Appendix IV: API Key Creation

In order to create an API key it is necessary to select the **Profile** option from the context menu that is shown when hovering over the user name shown at the top right of the screen. It is necessary to be logged in with the same account that should be used with the software for which the API key is needed.



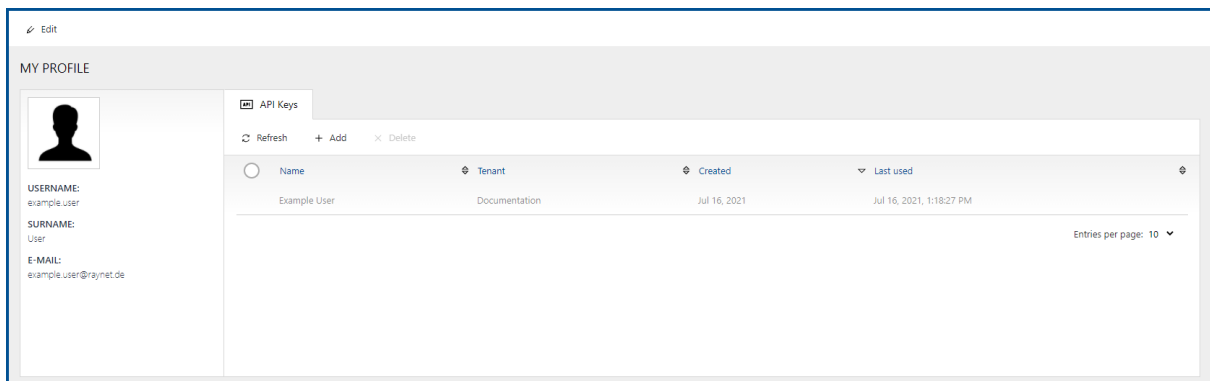
The **My Profile** page will open. This page contains a tab which is called API Keys. The tab contains a list of the API keys that already exist for the user. It can be used to either delete an already existing key or to add a new key.



Be aware:

The key itself will only be shown when created. If a key has been lost, it cannot be retrieved. Delete the entry for the old key and create a new key.

In order to delete a key, select the key and click on **Delete**. It is necessary to confirm the deletion once more in the confirmation dialog. To add a new API Key, click on **Add**.



When clicking on **Add** the **Add API Key** dialog will be opened.



The following fields are available in this dialog:

- **NAME:** Enter a name for the API key. For example, the name of the application for which the API key will be used.
- **TENANT:** Select the tenant for which the API key will be used. It is only possible to select one of the the available tenants for each key. In order to use API keys with multiple tenants, it is necessary to create multiple keys.
- **API KEY:** This field contains the automatically generated API key. After the dialog has been closed it will not be possible to retrieve the key. Use the button at the end of the field in order to copy the key to the clipboard.

After all fields have been filled and after copying the API key click on the **Add** button in order to finalize the creation of the key. It is now possible to use the key to create a connection to the selected tenant.



Appendix V: Supported OS

The following OS can be managed using RayManageSoft Unified Endpoint Manager.

- [Windows Desktop](#)
- [Windows Server](#)
- [MacOS](#)

Windows Desktop

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2019
- Windows Server 2022

MacOS

- Apple Mac OS 10.12
- Apple Mac OS 10.13
- Apple Mac OS 10.14
- Apple Mac OS 10.15
- Apple Mac OS 11
- Apple Mac OS 12
- Apple Mac OS 13



Appendix VI: Silent Installation for Managed Devices

In order to install the RayManageSoft Unified Endpoint Manager Windows Agent silently it is necessary to create a script and execute the following steps:

- The first step is the installation of the managed device using the `ManageSoft for managed devices.msi` with:
 - `INSTALLDIR, /L*V, and /qn.`
- The second step is the installation of the schedule package using the `ndschedag.exe` that can be found in the `Schedule Agent` folder of the installation directory defined in the first step:
 - `-t machine <.../Managed Device Default Machine Schedule/Default Machine Schedule.nds> -o UserInteractionLevel=Quiet`
- The final step is the installation of the default policy using the `mgspolicy.exe` that can be found in the `Policy Client` folder of the installation directory defined in the first step.
 - `-t machine -s "$(ScheduleRootURL)/Policies/Merged/$(URLComputerDomain) Machine/$(MachineId).nlp" -o UserInteractionLevel=Quiet`



Why Raynet

As a global software vendor with market-leading solutions and complementary managed services, we make successful end-to-end management of IT projects and operations possible.

Following the mission “**Discover to Manage**”, our vision is that all companies worldwide achieve transparency and security as well as optimization of their IT investments by using our technologies..

Get in touch

For more information, call our sales team at **+49 5251/54009-0** or write to **sales@raynet.de**.



Discover to Manage

www.raynet.de