

# RMS UEM 2.4

## 2.4.1981.712 [Update 02]

Release on 24 Feb 2023

### Resolved Issues

- Azure-AD import failed with token expired message. [RMSC-1580](#)
  - Local-AD import integration failed on creation. AD scan and import got refactored. [RMSC-1507](#)
- 

## 2.4.1974.698 [Update 01]

Release on 21 Feb 2023

### Resolved Issues

- Downloading big packages from the package store. [RMSC-1578](#)
- 

## 2.4.1972.690 [RTM]

Released on 13 Dec 2022

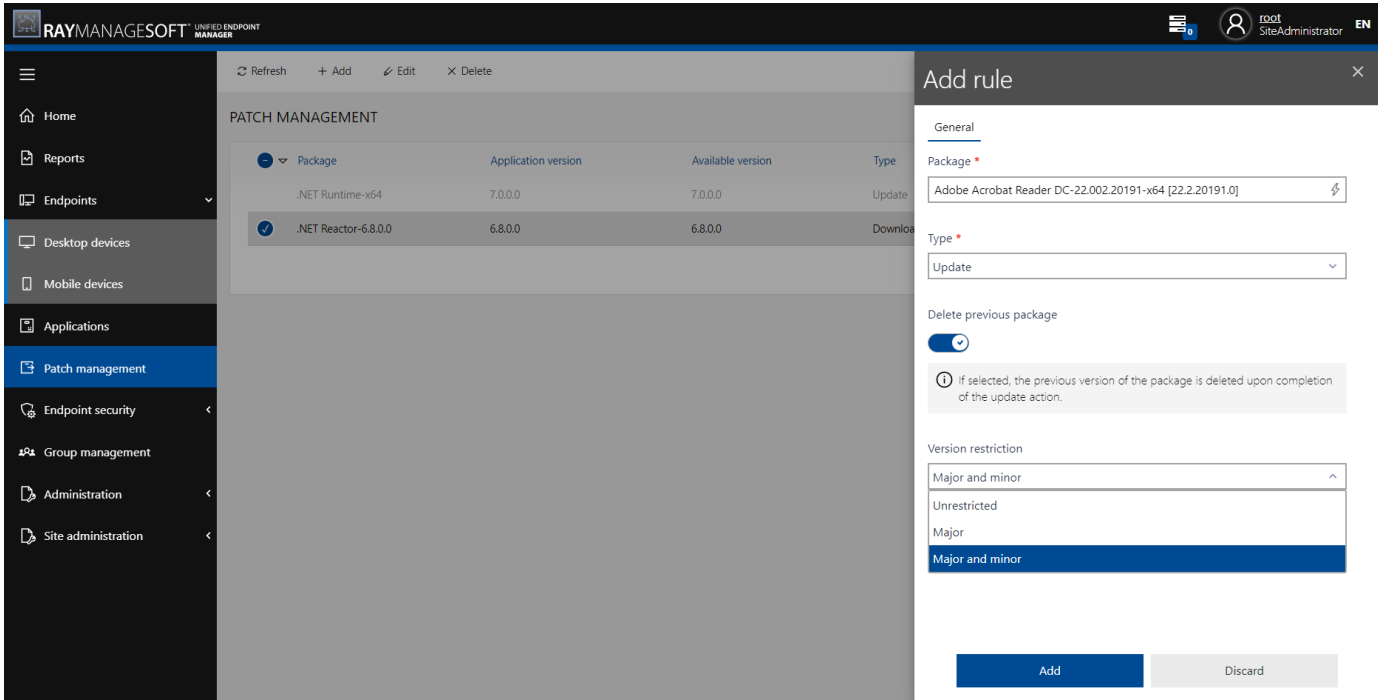
### Package Store Integration with 10K+ Packages

The relaunched Package Store platform offers several thousands of apps in 10K different versions, most of them with further configuration options. Package Store has a simple interface, which guides through the complete process, from searching the application, through selecting the version, to the configuration of the package. [RMSC-882](#)

Once a package from the Package Store has been selected, the user can configure the options and continue with the processing, which includes downloading the sources and do the magic in order to create a ready to use package.

### Automatic Patching of Third Party Software Products

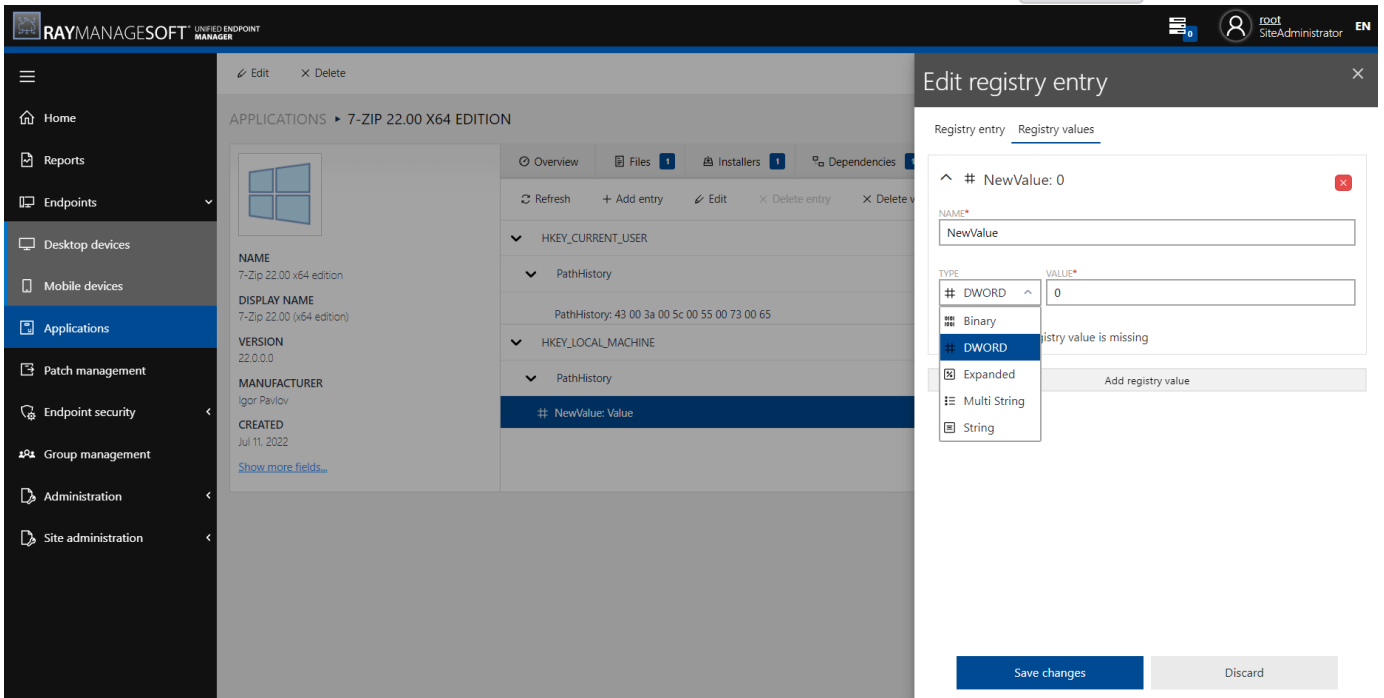
It is now possible to automatically manage patches and updates for all packages from the Package Store using easy to define update rules. Once a new version of a package is available it is possible to automatically download the sources, create the package and then update it. The packaging options for the Package Store will be reused for updates. [RMSC-608](#)



Micromanage the automated patch management by using the new dialogs for creating and editing the patch management rules.

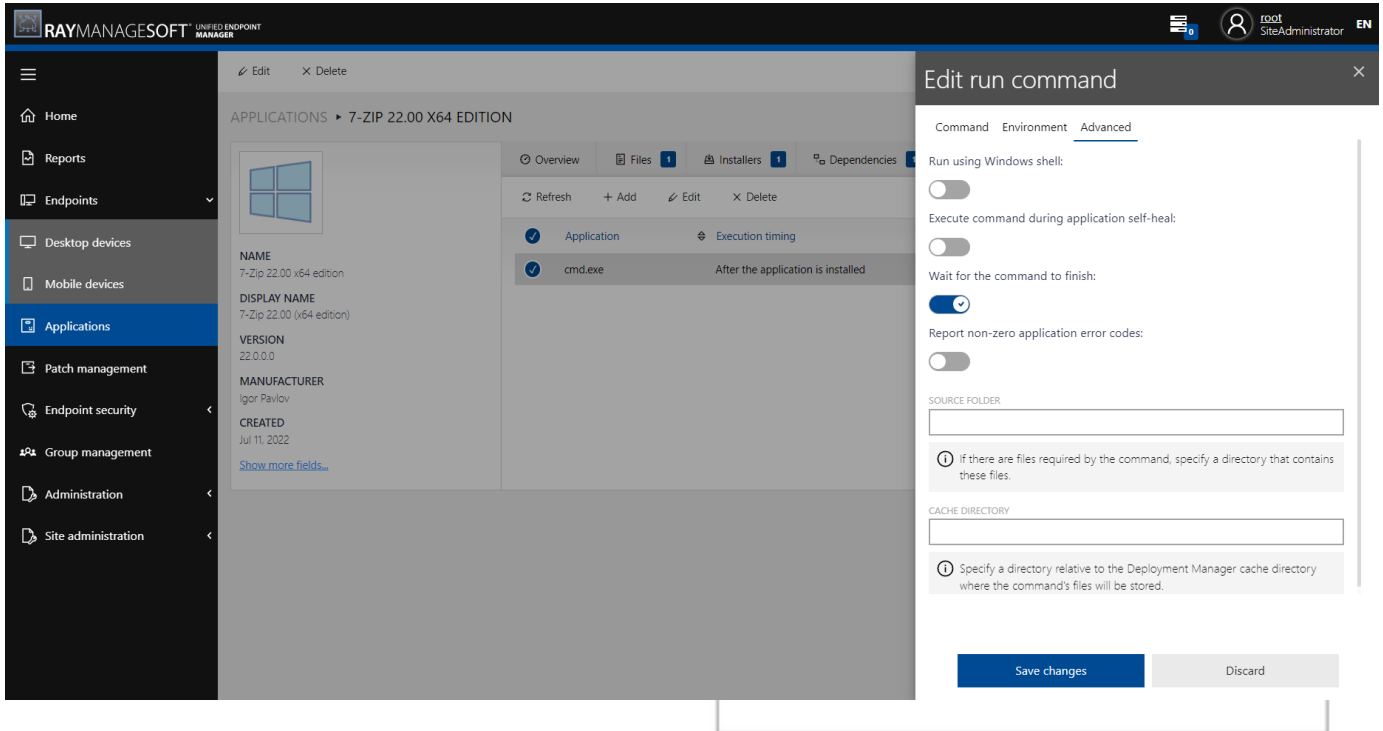
### Deploy Registry Keys to Managed Applications

It is now possible to deploy registry keys to managed applications using the built-in package editor. **RMSC-451**



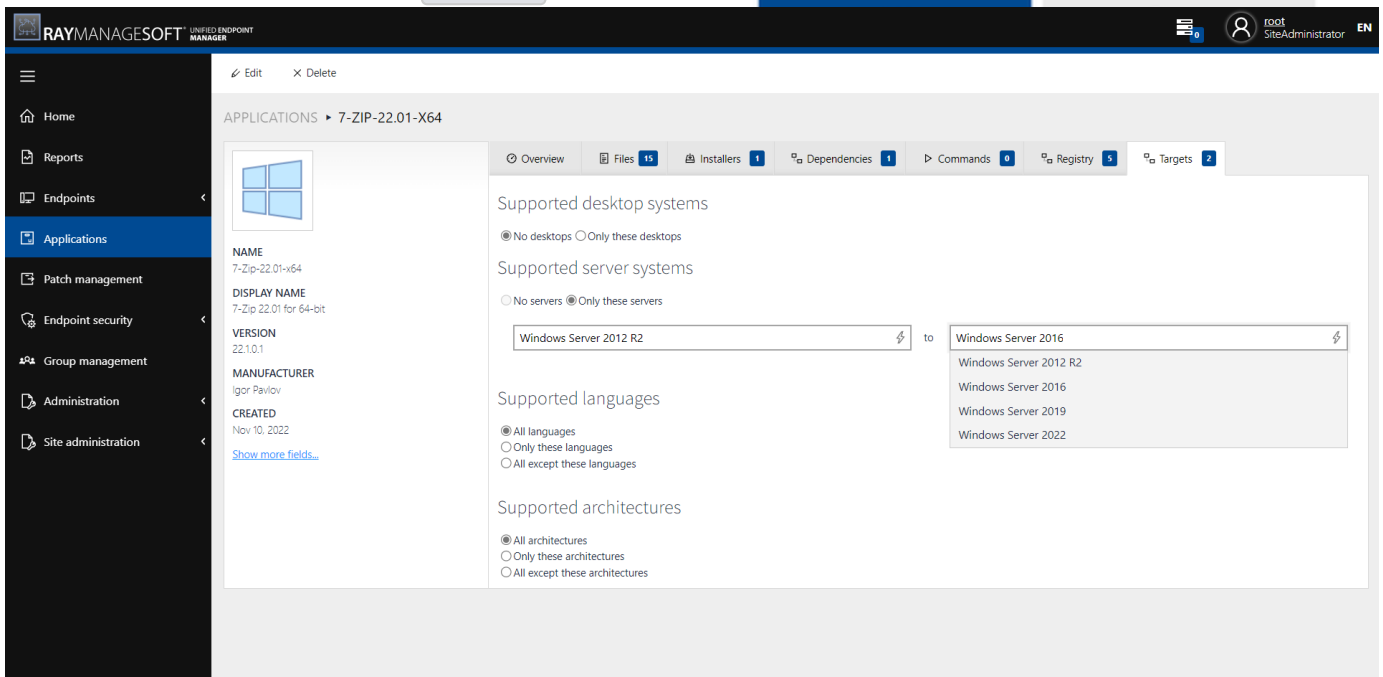
### Run Custom Commands on Managed Applications

It is now possible to run custom commands on managed packages using the built-in package editor. **RMSC-453**



## System-Specific Deployment of Software Packages

It is now possible to define the targets for applications based on the specific systems, architectures and/or languages. This can be easily configured using the built-in package editor. **RMSC-452**



## Automatic Normalization and Data Enrichment of the Software Inventory

Inventory data will automatically be processed and based on the raw data collected. The inventory data will be processed and products and editions will be identified. **RMSC-1006**

DESKTOP DEVICES ▸ DE01-SRV01

Inventory | Direct assignments 2 | Install states 2 | Device logs

SUMMARY | SOFTWARE 118 | HARDWARE | SERVICES 170 | Vulnerabilities 846

Products 64 | Raw data 118

visu

Product name	Product version	Vendor	Vulnerabilities
Visual C++ Redistributable	2008.x	Microsoft	0
Visual C++ Redistributable	2010	Microsoft	0
Visual C++ Redistributable	2005.x	Microsoft	0
Microsoft Visual Studio 2010 Tools for Office Runtime	10.x	Microsoft	0
Visual C++ Additional Runtime	2012	Microsoft	0
Visual C++ Minimum Runtime	2012	Microsoft	0
Microsoft Visual J# 2.0 Redistributable Package - SE	2.x	Microsoft	0

For all identified products, potential vulnerabilities will be determined and shown according to their vulnerability score.

DESKTOP DEVICES ▸ DE01-SRV01

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, 2015.006.30493 and earlier, and 2015.006.30493 and earlier have a use after free

## Other Improvements

- With this release, HTTP Basic authentication has been implemented. Managed devices must now provide a user and password combination for download and upload actions towards the server. **RMSC-632** **RMSC-1015**
- A CLI tool that can be used to allocate packages in addition to create users and groups has been added. **RMSC-797**
- The add package dialogs have been reworked. **RMSC-816** **RMSC-840** **RMSC-848**
- A "hidden" flag for packages has been implemented. If activated, the selector will not display the package in the Installed tab. **RMSC-859**
- All package changes are now validated before creating OSD/NDC files. **RMSC-853**
- The handling of bad requests has been improved and the messages that will be displayed have been unified and translations for all supported languages have been implemented. **RMSC-1016**
- The RayManageSoft UEM agent has now received a RayManageSoft UEM branding. **RMSC-1163**

- Groups support now priority. It is used during policy file generation. Duplicated package assignment will result to one assignment with the highest priority. [RMSC-860](#) [RMSC-883](#)
- The **Device Settings** UI has been reworked. [RMSC-1298](#)
- The **Tenant Settings** UI has been reworked. [RMSC-879](#)
- Default reports update. [RMSC-1287](#)

## Resolved Issues

- An issue with the uninstallation of packages with the type .exe has been fixed. [RMSC-800](#)
- An issue with the database clean-up task running in the background has been fixed. [RMSC-791](#)
- Issues with the license activation via file and order number have been fixed. [RMSC-846](#) [RMSC-1257](#)
- There have been fixes regarding the failover package generation. [RMSC-416](#)
- Issues with the policy file generation have been fixed. [RMSC-860](#)
- There had been an issue regarding the configuration of monthly triggers. This has been fixed. [RMSC-923](#)
- An issue with package naming when uploading folders has been fixed. [RMSC-891](#)
- Managed devices will no longer lose the Machine GUID while upgrading. [RMSC-1058](#)
- The Windows 11 and the Server 2022 logo are now shown properly. [RMSC-952](#)
- There have been fixes on the load indicator on multiple RayManageSoft UEM pages. [RMSC-1069](#)
- There have been fixes and improvements to translations on multiple RayManageSoft UEM pages. [RMSC-1094](#) [RMSC-1101](#)  
[RMSC-1118](#) [RMSC-1119](#) [RMSC-1127](#)
- The merge logic for existing devices by device name and domain has been fixed. [RMSC-1304](#)
- The assignment of packages to the devices and the group dialog has been fixed. [RMSC-1276](#)

## Breaking Changes

- RayManageSoft UEM has been migrated to .NET 6.0 [RMSC-801](#)
- RayManageSoft UEM is now fully Linux based [RMSC-367](#) [RMSC-799](#)