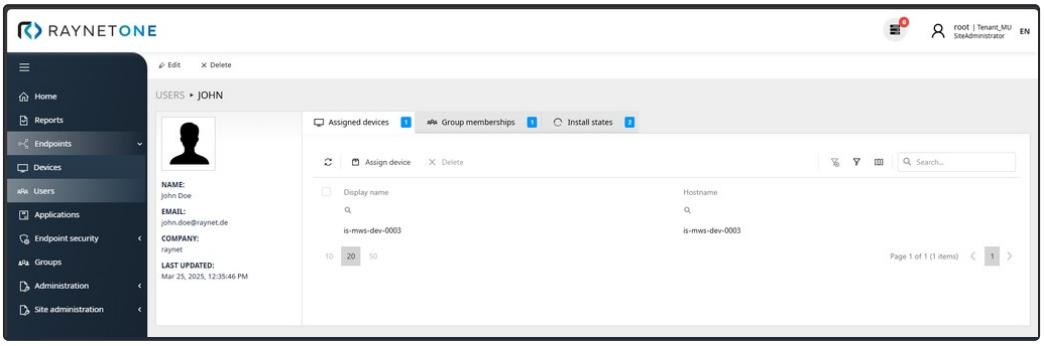
Raynet One UEM 3.2

3.2.4027.781 [RTM]

Release on Apr 17, 2025

User-based Deployment/Assignment of Packages RDEP-6 RDEP-26

Raynet One UEM now offers the option to assign software packages to users rather than directly to devices. This provides administrators with more flexibility, allowing them to manage assignments at a higher level without needing to track which user owns which machine. Raynet One UEM handles the dynamic user-device assignment process, simplifying deployment workflows.



Assigned devices to a user

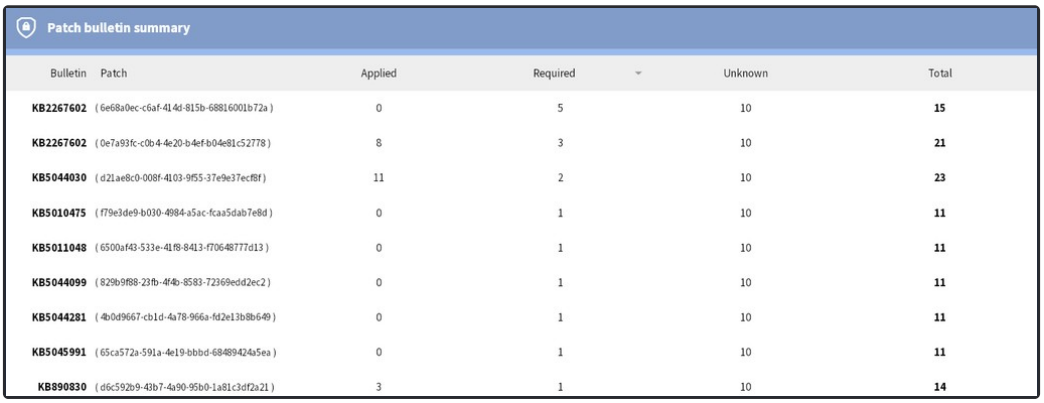
Users can be imported or manually configured, and during inventory, devices are discovered, with their primary users identified. This ensures that software assignments are automatically linked to users, rather than specific devices. Administrators can further customize the behavior through the following options:

- Direct configuration of the associations between users and their devices.
- Importing Relationships from Active Directory.
- Integrate with third-party systems for more advanced user-device relationship management via a dedicated REST API.

This feature is fully integrated with existing deployment tools, meaning administrators can continue using the same interface for both user and device group management without the need for additional tools. This ensures a consistent and efficient experience when managing package assignments.

Advanced Security Patch Reporting RDEP-1 RMSC-2695 RMSC-2696

Raynet One UEM now provides detailed and comprehensive reporting on the installation status of OS-level patches for Windows, ensuring feature parity with classic RayManageSoft implementations. Windows devices are scanned using an online mode (Windows Update Agent scan), delivering up-to-date insights into patch compliance. This allows IT administrators to proactively identify missing updates, track deployment progress, and address potential security risks before they become critical issues.



Patch bulletin summary

Bulletin	Patch	Applied	Required	Unknown	Total
KB2267602	(6e68a0ec-c6af-414d-815b-68816001b72a)	0	5	10	15
KB2267602	(0e7a93fc-c0b4-4e20-b4ef-b04e81c52778)	8	3	10	21
KB5044030	(d21ae8c0-008f-4103-9f55-37e9e37ecf8f)	11	2	10	23
KB5010475	(f79e3de9-b030-4984-a5ac-fcaa5dab7e8d)	0	1	10	11
KB5011048	(6500af43-533e-41f8-8413-f70648777d13)	0	1	10	11
KB5044099	(829b9f88-23fb-4f4b-8583-72369edd2ec2)	0	1	10	11
KB5044281	(4b0d9667-cb1d-4a78-966a-fd2e13b8b649)	0	1	10	11
KB5045991	(65ca572a-591a-4e19-bbbd-68489424a5ea)	0	1	10	11
KB890830	(d6c592b9-43b7-4a90-95b0-1a81c3df2a21)	3	1	10	14

Patch bulletin summary report

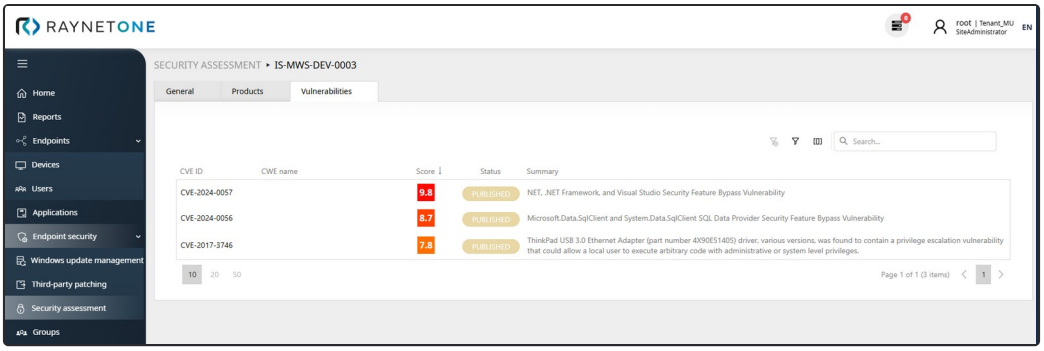
The results can be reviewed and analyzed through standard reports available in the default installation. These reports offer structured overviews of installed patches, making it easier for system administrators to maintain compliance with security policies and regulatory requirements.

For even more flexibility, you can leverage Raynet One Data Hub to customize reports, enabling the creation of tailored dashboards, cockpits, and executive summaries that align with specific business and security needs.

Security and Patch Analyzer and Vulnerability Recommendations for Third-Party Patches

RDEP-200 RDEP-3

This release further enhances the consolidation of data from patch detection tools, the Technology Catalog, and the Package Store. Raynet One UEM 3.2 thus provides a streamlined approach to vulnerability management, enabling faster responses to security risks and improving overall patch management efficiency, all within a single, unified view for administrators.



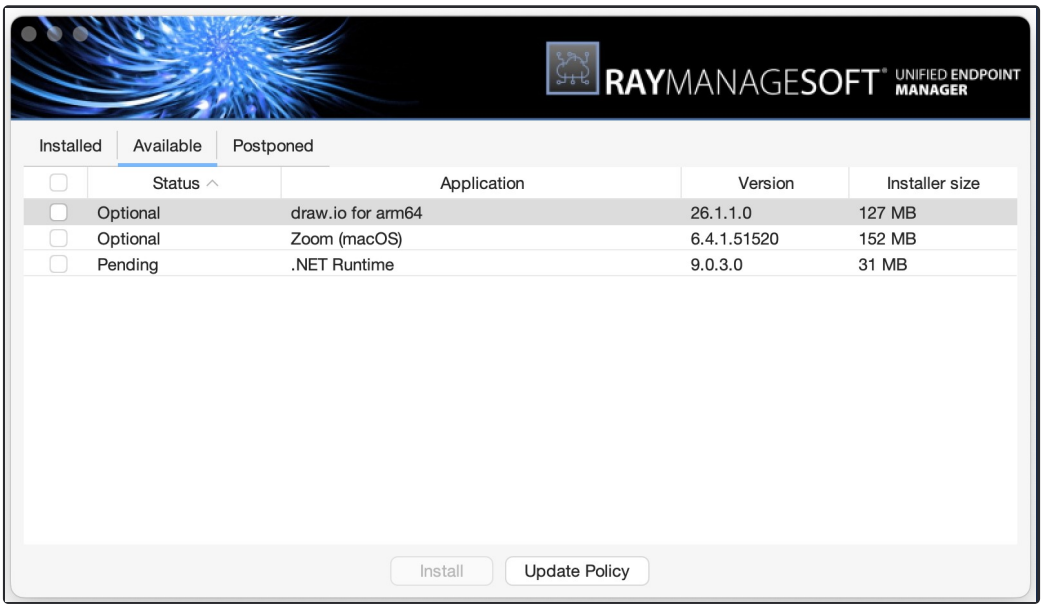
Detected vulnerabilities of a device

The new consolidated view includes:

- Unpatched software and detected vulnerabilities
- Available patching options, which highlights any newer software versions that are available and could resolve vulnerabilities.
- Devices needing inspection, informing which devices require further inspection or may be vulnerable due to outdated versions.
- Vulnerabilities closed by a newer version, which shows which new software versions address the detected vulnerabilities.

Native Support for Apple Silicon Processors RMSC-2670

Raynet One UEM now runs natively on Apple Silicon (M1, M2, and later) processors.



RMS UEM App Center running on MacOS

By eliminating the need for emulation or translation layers, this enhancement provides better responsiveness and stability, making software deployment and management on macOS more efficient than ever.

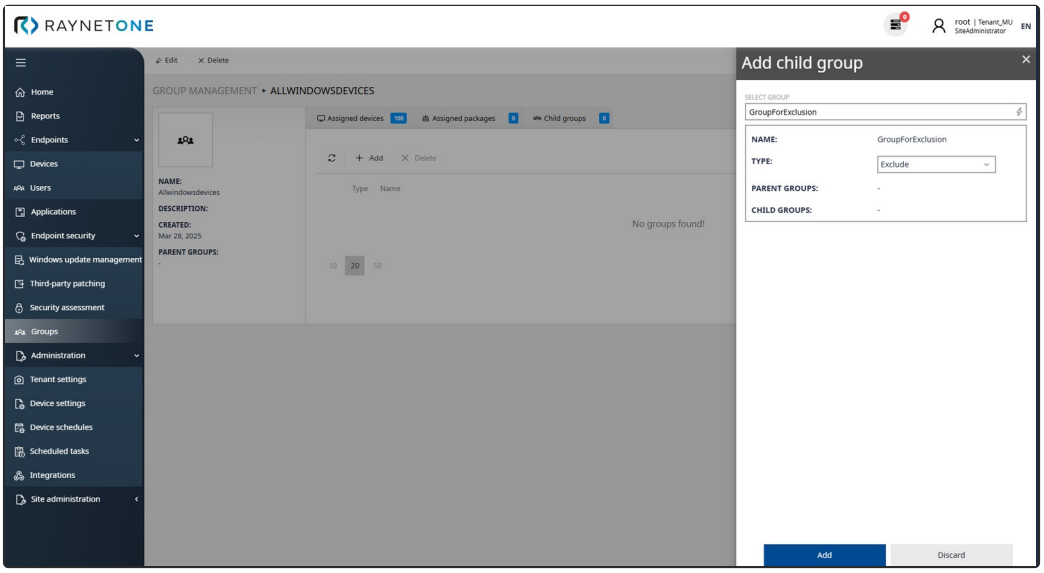
Import of Packages from RMSi or other UEM instances RMSC-2750

Raynet One UEM now includes an advanced automation tool designed for the batch import of software packages from a local directory into a UEM instance.

This tools provides an easy way for migration from classic RMSi Software Library, while preserving existing configurations. Additionally, the tool can be used to transfer packages between different UEM systems or environments, enabling efficient replication of deployment packages across test, staging, and production.

Device Groups Can Be Now Configured as Exclusions RMSC-2125 ZEN-24178

Raynet One UEM now supports exclusion groups for software deployment policies. Previously, UEM only allowed inclusion groups, providing a basic level of control over package deployment.



Adding a child group as exclusion

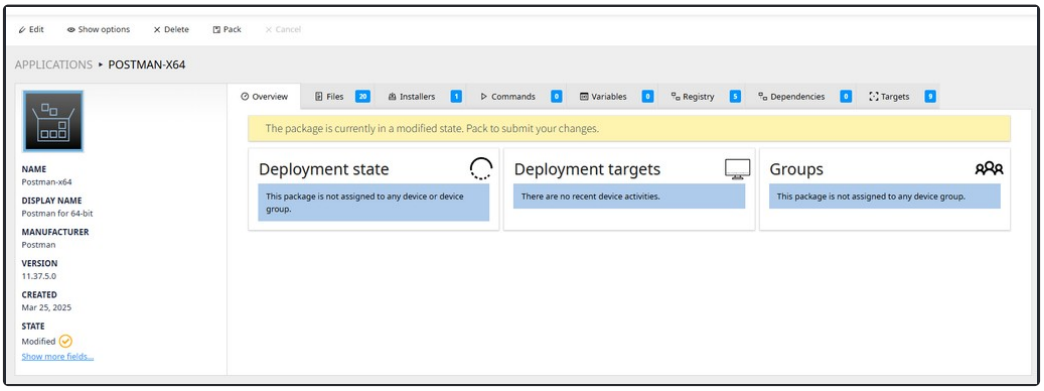
- Devices or other exclusion groups can now be assigned to new excluding groups, preventing unintended deployments.

- During policy generation, the system now verifies exclusion groups and ensures that devices assigned to them are not included in the final deployment list.
- When an assignment includes an exclusion rule, the affected devices will be marked with the “Excluded” state, making it clear which devices are intentionally omitted from the deployment.

For RMSi users, this addition closes the parity gap between RMS UEM and RMSi, making the migration to UEM smoother.

Deferred Package Preparation RMSC-2726 RMSC-2742

Raynet One UEM now offers configurable package preparation settings, allowing administrators to optimize the packaging workflow based on their deployment needs. In previous versions, every modification to a package—such as adding a file or changing a property—immediately triggered the packaging process, consuming resources and potentially delaying further edits.



A new badge that informs about the deferred package preparation.

With this update, two different packing models are available:

- **Automatic packing enabled**
  The default behavior remains unchanged: RMS UEM 3.2 will automatically prepare the package for deployment after every modification, just like in previous versions.
- **Automatic packing disabled**
  RMS UEM will defer package preparation until the user explicitly confirms that the package is ready by clicking the new "Pack" button. This prevents unnecessary repackaging and allows changes to be canceled before deployment.

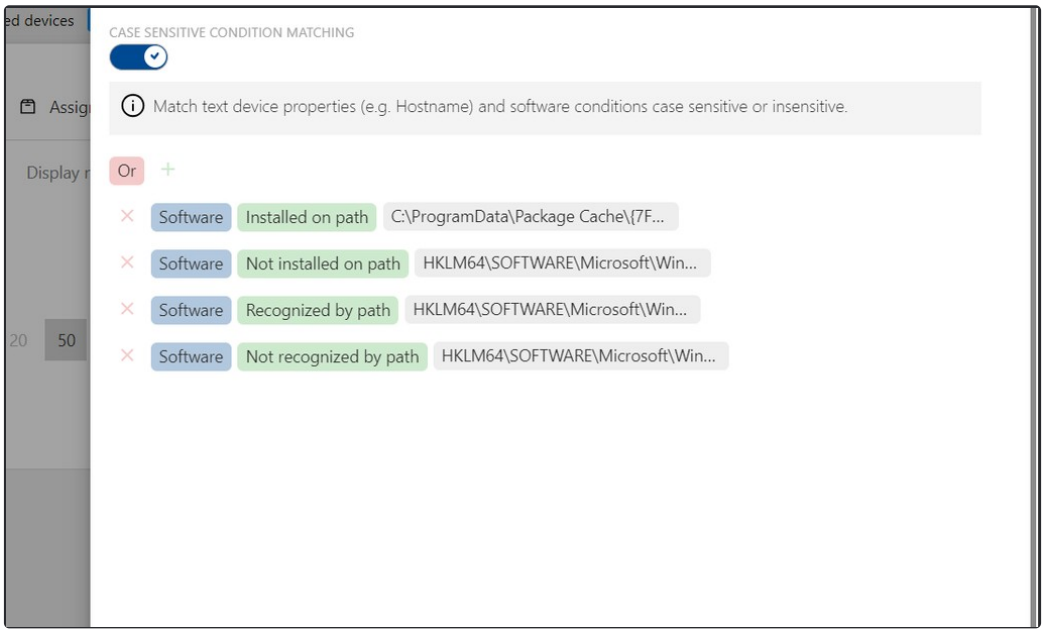
This improvement is particularly beneficial in scenarios where multiple edits or batch modifications are applied to a package in quick succession. Correct uses of this feature reduces backend workload and enhances system performance.

New Operators for Dynamic Conditions RMSC-2688 RMSC-2571

Raynet One UEM 3.2 enhances dynamic condition filtering by introducing four new operators for software- and hardware-based targeting.

New operators are:

- Product is installed in a specific location
- Product is not installed in a specific location
- Product has been recognized by its install location
- Product has not been recognized by its install location
- Device architecture



Visual designer of device conditions, involving some of the newly added operators.

These new conditions significantly improve detection accuracy and dynamic grouping, enabling more granular software deployment and policy enforcement. Additionally, they simplify UI configuration by reducing the need for complex scripting or manual filtering.

Support for Deadline Settings for Windows Update Configuration RMSC-2652 RMSC-2645

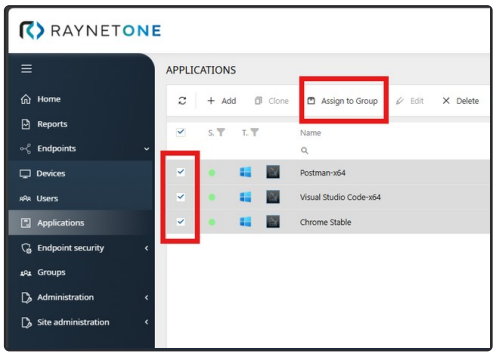
Raynet One UEM now supports deadline settings for Windows Update configurations, giving administrators more control over how and when updates are enforced.

- **Auto-Reboot Enforcement**
  Automatically restart devices after an update is installed, ensuring compliance with security policies.
- **Deadline for Feature and Quality Updates**
  Define mandatory installation deadlines, preventing prolonged delays in applying important updates.
- **Grace Periods**
  Allow users a buffer period before enforcement, reducing the risk of unexpected reboots and ensuring smoother update adoption.

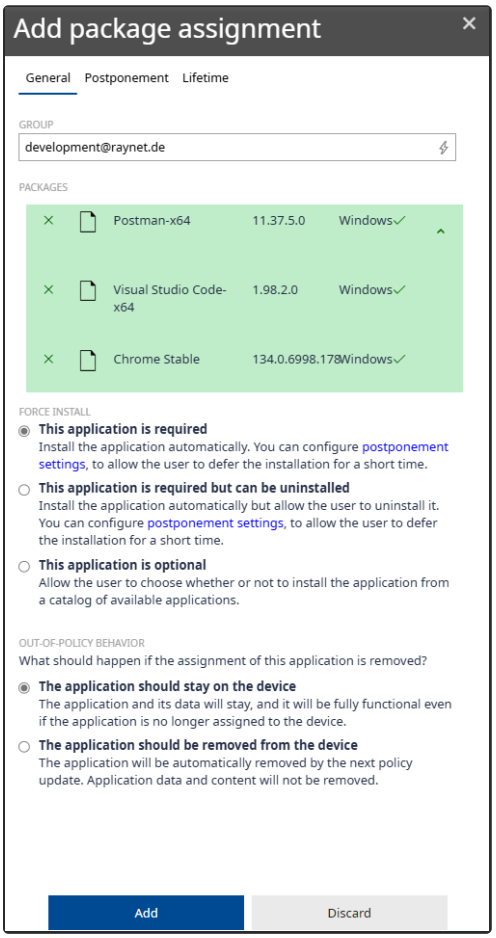
To improve usability and configuration clarity, these new options—alongside existing update-related settings—have been relocated from "Update Compliance" to the new "Windows Update Management" page.

Batch Assignment to Groups RMSC-2492 RMSC-2493 RMSC-664

Raynet One UEM now supports batch assignment of packages to deployment groups, allowing administrators to select multiple packages at once and add them to a group for streamlined deployment. The enhanced dialog provides all relevant settings, including requirement definition, postponement options, deployment lifetime etc.



First mark the applications to be assigned…

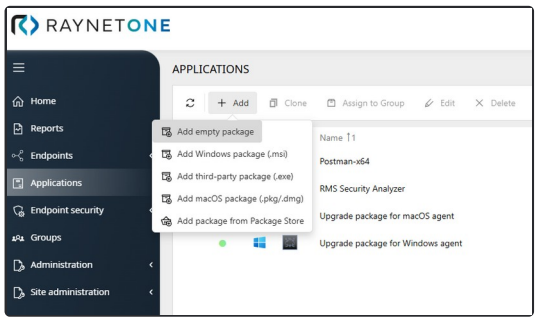


… and finally have them assigned with a single click.

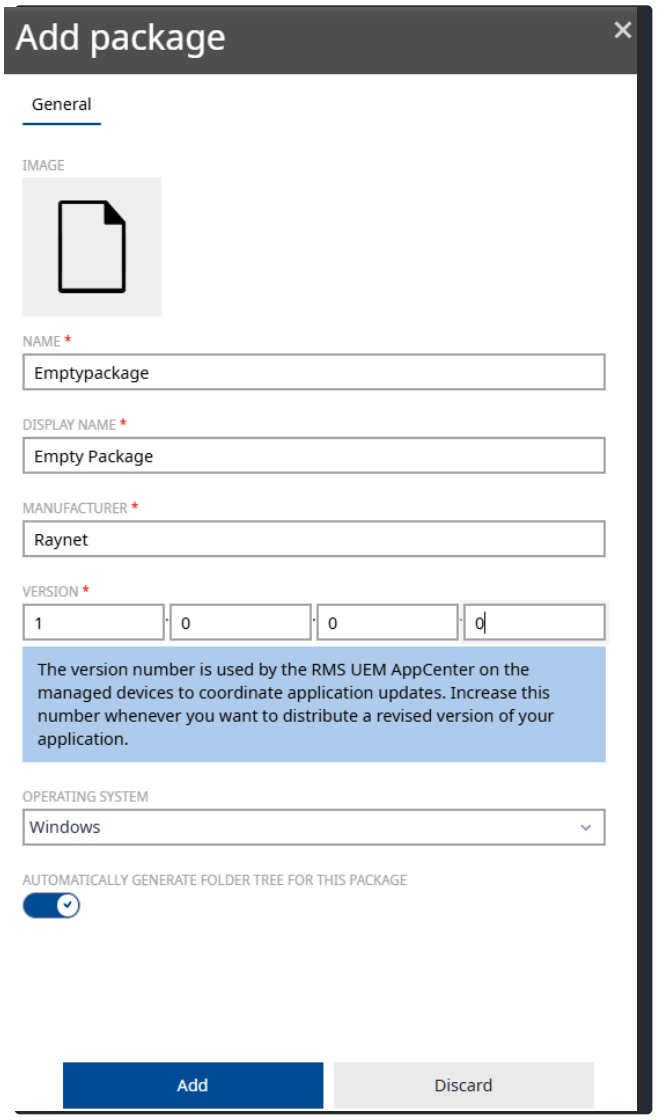
Support for Creation of Empty Packages RMSC-1318

Raynet One UEM now supports the creation of empty packages, allowing administrators to create packages without providing an installer or files. This new feature is particularly useful in the following scenarios:

- Creating packages that will be configured and populated with content at a later time, allowing for early planning and setup without needing immediate details.
- Defining packages that do not deploy files or installers but instead execute custom commands or scripts, enabling the deployment of configuration tasks or system changes without traditional software installation.



New menu item for empty packages.



Adding an empty package requires only a minimal set of options.

Support for Package Variables RMSC-1317

Raynet One UEM now supports the ability to set variables at the package level. This feature, ported from RMSi based on user feedback, allows administrators to define custom variables that can be easily applied across multiple deployment packages.

Located in the Package Details page, the new interface enables straightforward creation and management of variables, making it easier to configure and customize deployments in complex scenarios and for tailored needs.

Support for Custom Scripts (.csm) in Device Inventory RDEO-69 RDEP-151 RDEP-152

Raynet One UEM now supports the use of custom inventory scripts for macOS, offering compatibility with other Raynet products such as Raynet One and RayVentory. The data generated by these custom scripts will now be seamlessly integrated into the inventory, ensuring that all relevant information is captured.

Other Changes and Improvements

- New standard report *Hardware Evidence Report*. RDEP-116
- Target selection now has buttons to select/unselect all targets. RDEP-168
- Better recognition of standard macOS apps. RDEP-270
- Windows 11 23H2, 24H2 and macOS 15 are now available as one of targets. RMSC-2456 RDEP-19
- When a package is removed, its parent empty folders are now also deleted. RMSC-2617

- Redesigned Package Details page, withe emphasis on packing status, validation, warnings and more. RMSC-2742
- In various places where package selection is required, the lists are now sorted by name and version. It is therefore easier to locate the desired target. RMSC-2756
- Software path is now displayed as one of supported properties for Windows device inventories. RMSC-2749
- Performance improvements of the data enrichment process (powered by Raynet One Technology Catalog). RMSC-2728
- Type of Operating System (Windows / macOS) is now displayed next to the name and version when selecting a package for third-party patching. RMSC-2656
- Updates of Catalog signatures now automatically trigger re-validation of dynamic group assignments. RMSC-2634
- Improved handling of obsolete resource upload, which are now removed if not needed by any other package. This conserved disk space and has an overall positive impact on the performance of the system. RMSC-2610
- For multi-tenant instances, the name of the tenant is displayed in the right top corner. RMSC-2499
- Performance improvements especially with large data. RMSC-2561 RMSC-2455
- Redesigned UI for the configuration of automatic updates. RDEP-147
- The field ‘Postpone by' now has a date picker editing capability. RMSC-2797
- After adding a package, the data table with the list is now automatically refreshed. RMSC-2794
- The system now prevents deletion of folder with sub-folders, that would cause name conflicts after the deletion. This could happen for example, if both the root folder and any of deleted sub-folder would have a conflicting name. In this version, such conflicts must be resolved manually (by renaming or moving) before the folder can be deleted. Similarly, the same logic is now applied to drag and drop functionality. RMSC-2674 RMSC-2673
- It is now possible to modify targets of upgrade packages. RMSC-2609
- Improved performance of deletion of large number of groups with many assignments. RMSC-2548
- Background job processing now skips inactive tenants. RMSC-2576
- Improved performance of package assignments for large, nested groups. RDEP-85
- Azure AD import failures now stop the associated scheduled task, preventing repeated errors. The scheduled task should now be halted upon import failure. RMSC-2467
- Scheduled tasks now support time zones. RMSC-1393
- When logging into an inactive tenant via Keycloak, the user receives now informative notification about the issue. RMSC-2376

Resolved Issues

- Resolved an issue with changes to email addresses within the ‘Profile’ section being not persisted. This issue also affected the user details area. RDEP-264
- Resolved an issue where the system incorrectly displayed uninstall records when the display name was unavailable. These records should be now suppressed to maintain data integrity. RDEP-258
- Resolved an issue with the system logs that contained unnecessary messages related to proxy configuration changes during the communication with Package Store. RDEP-197
- Resolved issues with DMG Package Import Error where some application names could not be parsed during content processing, causing the import of `.dmg` file to fail. RDEP-196
- Resolved an issue where attempts to edit files in "Inventory scripts" under MD Settings resulted in the loss of previously saved files. RDEP-155
- Lifted restriction on maximum number of days for the Windows Update management setting The ‘Quality update deferral period (days)’. RDEP-121
- Resolved inconsistency in bundle deployment and installation reporting. This issue involved the standardization of folder structure for bundle deployment and installation reports, dashboard/report renaming, and the refinement of data fields within reports. RDEP-84
- Resolved issues with redundant package assignments in Default Device and Schedule Settings. Previously packages could be assigned multiple times when new devices were created and default packages were assigned. RDEP-55
- Improved dynamic group condition processing with a large number of devices, where some changes could not trigger the re-evaluation of assignments. RMSC-2529

- Resolved an issue with DMG package installations failing due to an unresolved license agreement check that interrupted the installation process. RMSC-2508
- Resolved issues with inadequate filtering of active installation states, leading to incorrect device numbers in the ‘Deployment Details’ report in Data Hub. RDEP-88
- It is now not possible to upload duplicate files in a single session, which could result in deletion of the entire directory. RDEP-66
- Resolved an issue where modifications to multiple triggers were not saved correctly, with changes being lost when editing a subsequent trigger without saving the prior one. RMSC-2621
- Resolved issues with package naming conflicts during simultaneous patching between same Windows and macOS packages. RMSC-2619
- Improved package filtering mechanism in the Package Store view, which prevented certain packages from being displayed. RMSC-2468
- Resolved an issue where renaming display name could reset the device serial number property. RMSC-2452
- Resolved a visual issue where scrolling through lists could cause selection loss and where switching between tabs was not closing opened edit menus. RMSC-2421 RDEP-214
- Device settings are not inheriting default target configurations anymore. RDEP-239
- Resolved incorrect values (RAM = 0) displayed in the ‘UEM Device Hardware’ report. RDEP-232
- Resolved various minor visual issues and glitches in the presentation of the Third-Party Patching interface. RDEP-177
- Resolved an issue where it was not possible to disable a tenant with invalid connection strings. RDEP-173
- Resolved validation and display issues in Windows Update management settings window. RDEP-142 RDEP-123 RDEP-8
- Resolved various visual glitches and sub-optimal spacing and alignment with responsive design. RDEP-11 RMSC-2818 RMSC-2723 RMSC-2719 RMSC-2714 RMSC-2682
- Toast notifications about updates are not shown anymore for entries, where no change was done. RDEP-48 RDEP-10
- Resolved an issue with clean-up job, that lead to removal of packages being initialized. RMSC-2784
- Resolved issues with not working filter in the ‘Update available’ column. RMSC-2746
- Resolved an issue with missing tenant icons on the login page. RMSC-2707
- Resolved an issue with invalid failover settings written to the index file for macOS agent. RMSC-2683
- Removed the option to set the trigger ‘When connected to network’ for macOS devices. RDEP-54
- Resolved issues with sorting of the application tree view with folders. RMSC-2668
- Parsing of incoming data now works properly for machines, lacking the `MGS_PROCESSOR` entry. RMSC-2655
- Resolved a possible conflict and data corruption when uploaded installer files overlapped with manually created files and folders. RMSC-2647
- Changed the incorrect UI wording for the ‘source folder’ input fields in the package editor (section Commands). RMSC-2625
- Resolved an issue with handling of file / folder names containing unsupported null termination character. RMSC-2623
- Resolved issues with handling of package files containing space characters, which led to incorrect file names being written on the client. RMSC-2588
- Resolved an error with additional parameters set for the "Apply Machine Policy" event being not persisted in settings after a package upgrade. RMSC-2575
- Resolved an issue where the log import process was unable to correctly process the ‘posponed’ event result. RMSC-2565
- Resolved inconsistent priority handling for UEM package run commands. RMSC-2558
- Improved import processes with data, that result in self-referential folder loops. Previous it caused issues with group deletion and updates of install states. RMSC-2550
- Resolved an issue with Windows agent crashing on corrupted package cache files. RMSC-2534
- Resolved an issue where it was not possible to search for Package Store packages using a `+` character in their name. RMSC-2526
- Resolved an issue where the "Not Install" operator in dynamic group conditions failed to correctly remove devices from groups when the specified application was installed. This lead to inaccurate group memberships. RMSC-2522
- Resolved issues with missing or incomplete data validation for schedule event time and data fields. RMSC-2520 RMSC-2511 RMSC-2504 RMSC-2375

- Resolved several issues with broken sorting functionality in various reports. RMSC-2501
- Resolved an issue with UI freezes when deleting an installer that was already associated with files. RMSC-2465
- Resolved potential deadlocks with adding package assignments and heavy concurrency of other tasks. RMSC-2440
- Resolved issues with searching for direct assignments and install states where the search string was a numeric value. RMSC-2359
- Package validation error messages are now correctly localized. RMSC-2088
- Resolved incorrect display of optional packages with expired package assignments for Windows users.
- Resolved an issue with grouping in RMS UEM V `ulnerabilityInformation` and `ITVisibility` not accounting for device uniqueness, causing inaccurate reports. Device ID is now used for accurate grouping. RDEP-24
- Resolved issues with incorrect time displayed in the Site Administration download log. RMSC-1259

Security improvements

- The Enqueue Operation now requires API key and does not allow anonymous traffic. RDEP-29
- Standard users are now able to upload files for packaging and access the security assessment page. RMSC-2577 RMSC-2622
- Resolved an issue where it was possible to see sensitive information in the system log when deleting a tenant database. Password Exposure in System Logs RMSC-2666

Requirements

Raynet One UEM 3.2 requires Raynet One DataHub 14.1 Update 1 (`14.1.6298.172`) for reporting. Some of the newly developed features won't be visible when working with older versions of the Data Hub platform.

Breaking changes

UI and front-end controls have been migrated to Angular 18. Note that this affects the list of supported web browsers (see https://angular.dev/reference/versions#browser-support for more details). RMSC-2680 RMSC-2611

- Chrome and other Chromium-based browsers (Edge, Opera, Vivaldi, Brave etc.): 2 most recent versions
- Mozilla Firefox: latest and extended support release (ESR)
- Apple Safari: 2 most recent major versions

> ⚠ Other and older browsers may still work, but since they are not officially supported by the Angular framework, they are not supported by the Raynet One UEM

Migration

- The application database migration is handled automatically during the initial launch of the UEM console.
- Raynet One UEM 3.2 introduces new environment properties that require your attention. Please use the provided templates to update your existing Docker Compose configuration accordingly. Before initial launch make sure to
  - update the port mappings, for example, change `80:80` to `80:8080`
  - add new environment properties to the configuration file (ensure the initial tenant ID is synchronized),
  - adjust the existing connection strings by appending `Encrypt=False;`.
- After the initial launch, additional configuration of existing tenants is required:
  - Update connection strings by editing each tenant in the ‘Site Administration Tenant’ section and appending `Encrypt=False;` to each string.
  - Recreate integrations and their corresponding schedules to apply the newly available settings.