

True IT Asset Visibility

You can't **protect** & **manage** what you can't see.



Raynet One 2026.4

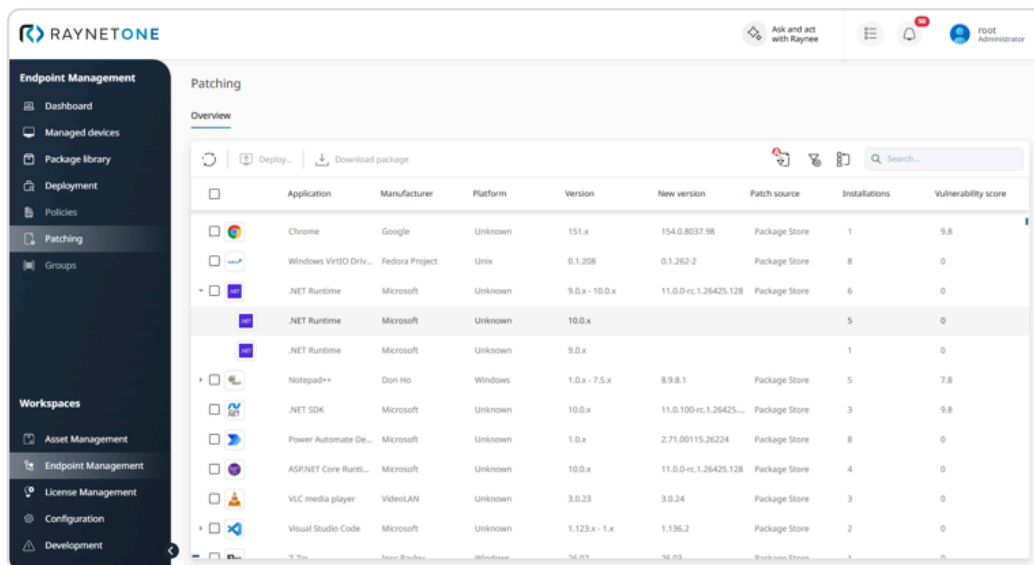
What's new in 2026.4?

Released on Oct 28, 2026

Automated Endpoint Management Capabilities PMD-7 PMD-106 PMD-201

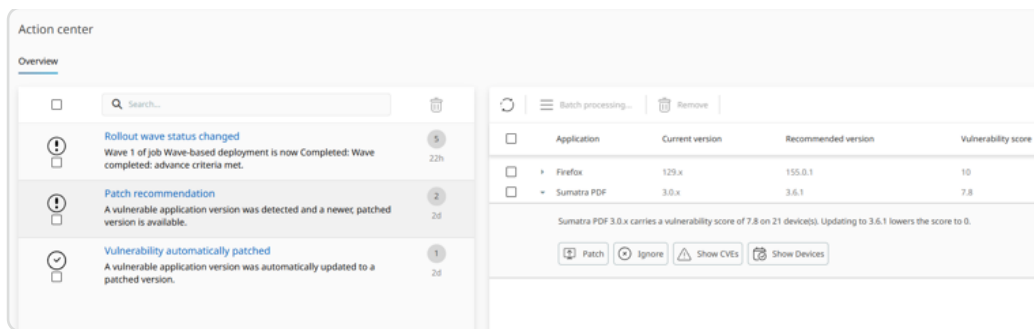
Endpoint Management now works through the same AI chat used for asset and license questions, letting administrators ask Raynée to find, patch, or remove software directly, in plain language, instead of working through the classic UI step by step.

For example, asking "show me the top vulnerabilities in my environment" and following up with "download a patch for this" and "deploy it" takes a multi-step engineering workflow (download, package validation, device targeting, rollout) and turns it into a short conversation. Any action that changes something on a device, such as installing a patch or uninstalling software, still requires explicit user confirmation before Raynée carries it out.



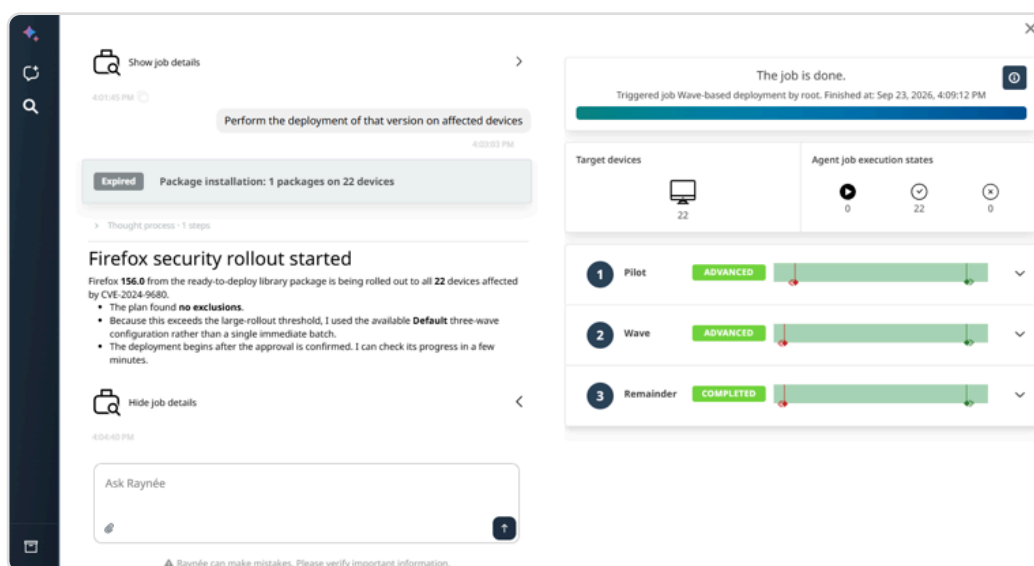
The new patching view shows which apps can be updated and the potential impact.

The functionality is tightly integrated with the internal notification mechanism. New vulnerabilities, patches, and software can trigger notifications, turning administrators' focus to new threats and solutions with readily available actions.



The Action Center screen now includes action callouts. For example, the user is informed that automatic Sumatra PDF patching can be started and that it lowers the risk score from 7.8 to zero, effectively closing the security hole.

Deployments triggered this way use staged rollout waves rather than pushing to every device at once. A patch goes first to a small pilot group, and only expands to the rest of the fleet once that group crosses a defined success threshold; if failures exceed a defined threshold, the rollout halts automatically. This limits the blast radius of a bad patch to a handful of devices instead of the whole fleet, and the wave strategy is configurable (fixed pilot devices, random sampling, percentage-based expansion) for teams that want to tune it beyond the default.



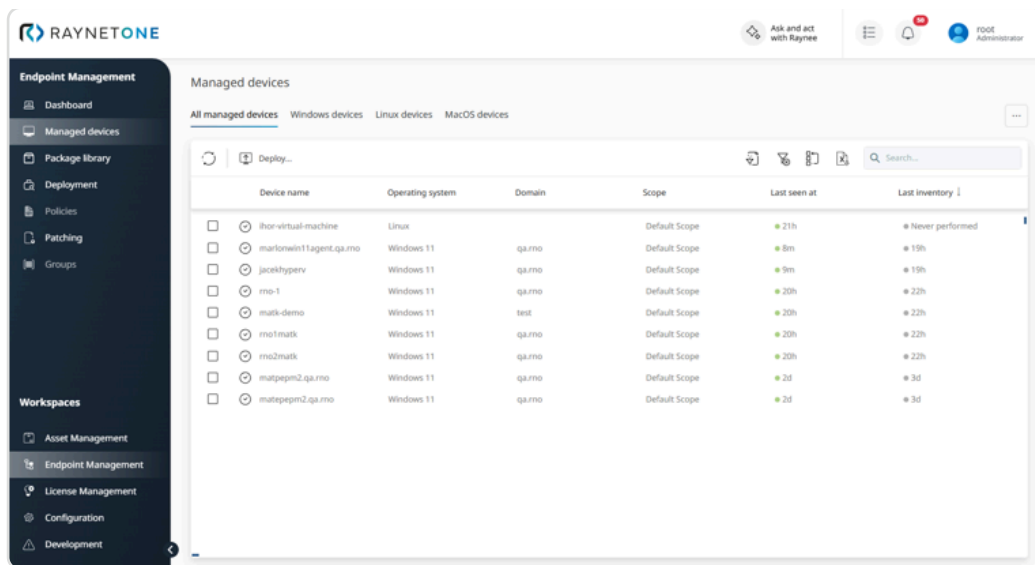
This is a chat-triggered deployment showing the progress of a ring-based deployment.

This capability is rolling out to a limited set of early-access customers first, with broader availability following as coverage expands.

Behind the Scenes: New Raynet One Agent PMD-8 PMD-141 RCOR-3628

Raynet One now has its own lightweight agent, built from the ground up on .NET, that does two things Zero-Touch scanning alone couldn't: it keeps a persistent presence on a device for faster, deeper inventory, and it can execute deployment tasks like package installation, patching, and command execution directly on that device.

The agent runs the same instruments and plugins as the Zero-Touch Runner, rebuilt this release to be shared between both. When a device is already agent-managed, the Runner routes its inventory collection through the agent instead of Zero-Touch, but the output lands in the exact same data model and goes through the same downstream processing. Results are queued locally and uploaded the next time the agent connects, so a laptop that's offline overnight doesn't lose its inventory run.



The list of managed devices.

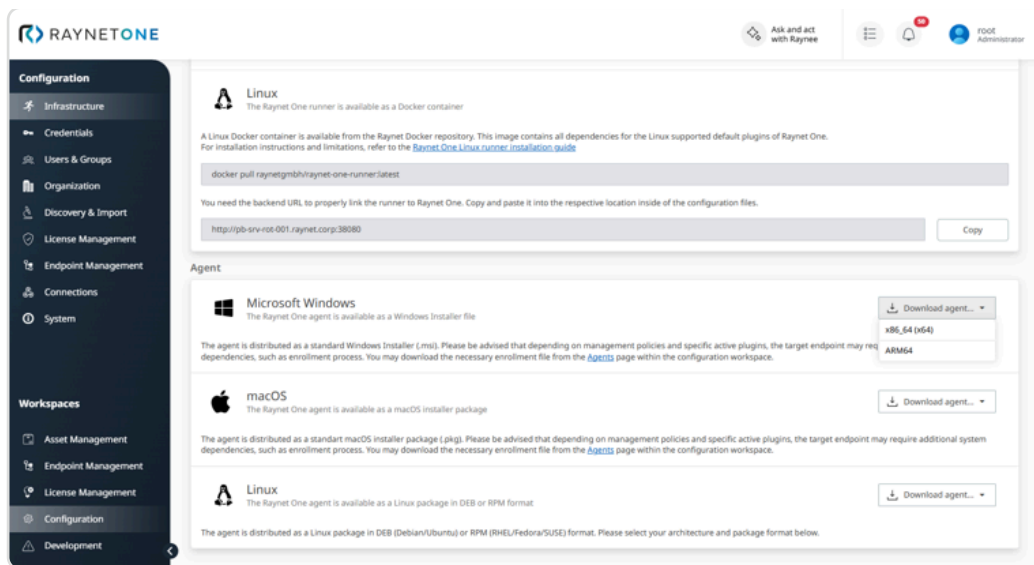
The agent can run defined tasks on managed devices - installing a package, applying a patch, executing a command - with centralized task creation, progress tracking, and logging back in Raynet One. Agent task assignments are tracked the same way as any other job, with a details view for progress and logs, so a deployment run is visible end-to-end instead of disappearing into a black box on the endpoint.

IP address	Managed	Name	Operating system	Services	Last inventory
10.69.69.173	Managed	matepepm2	Windows 11		Oct 6, 2026, 1:55:44 PM Current
10.69.69.171	Managed	matpepm2	Windows 11		Oct 6, 2026, 1:55:44 PM Current
10.69.69.111	Managed	rno2matk	Windows 11		Oct 8, 2026, 12:40:09 PM Current
10.69.69.175	Managed	rno1matk	Windows 11		Oct 8, 2026, 12:40:09 PM Current
10.69.69.112	Managed	matk-demo	Windows 11		Oct 8, 2026, 12:40:09 PM Current
10.69.69.107	Managed	rno-1	Windows 11		Oct 8, 2026, 12:40:12 PM Current
10.69.69.134	Managed	jacekhyperv	Windows 11		Oct 8, 2026, 3:30:15 PM Current
10.69.69.182	Managed	marlonwin11agent	Windows 11		Oct 8, 2026, 3:30:16 PM Current
172.19.0.1	Managed	ihor-virtual-machine	Linux		Never performed

Managed devices (having the agent installed) use the native agent capability to perform the inventory scan.

Devices join the agent fleet through enrollment tokens - named, scoped, with configurable expiry and a usage limit. Agent settings (serving endpoints, sync schedule, log levels) are centrally managed and pushed to connected agents through a revision-based update mechanism, so a configuration change propagates without reinstalling anything.

The agent installs on Windows (x64 and ARM64), macOS, and Linux - with native packages for each: MSI on Windows, and .deb / .rpm on Linux across the major distributions (RHEL/CentOS Stream, openSUSE/SLES, Ubuntu, Fedora) in both x86_64 and arm64 builds. All platforms are available from one centralized downloads page, so getting an agent onto any device in a mixed fleet is the same two-minute flow regardless of OS.



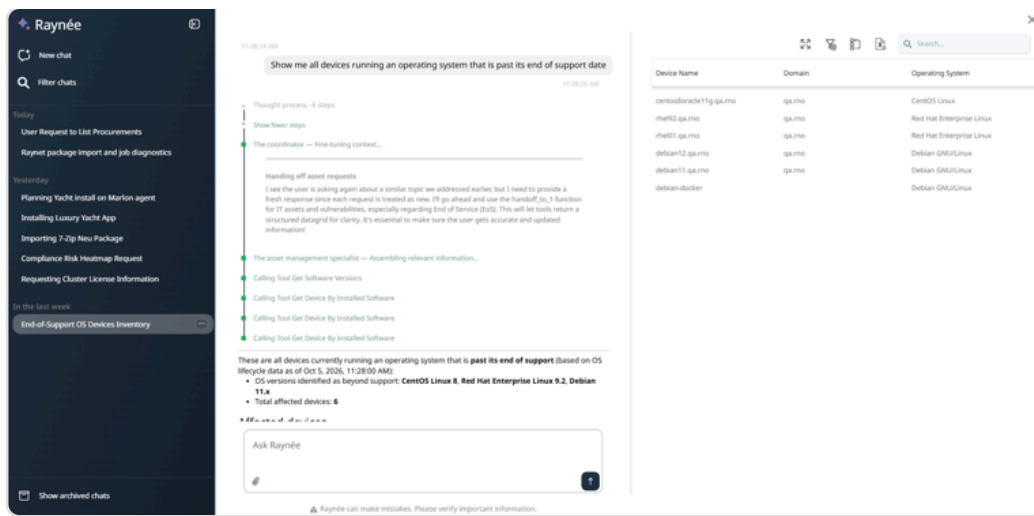
The centralized place for downloads: get your agent for the following target platforms: Windows, macOS, and Linux.

The new Raynet One Agent serves as an alternative to traditional zero-touch scanning while enabling robust software deployment capabilities. It has reusable instruments and plugins (same like the Zero-Touch server), supports secure end-to-end enrollment, and is our foundation for modern endpoint management and upcoming features.

Smarter AI Chat with Dedicated Experts, Visible Reasoning, and a More Capable Model PMD-14

Raynée's AI chat now works like a team of specialists instead of one generalist trying to cover every topic at once. Questions about assets, license entitlements, or endpoint management are handed off to a dedicated expert for that area, with a separate expert handling direct data lookups. For users, this means more accurate and more consistent answers, especially for complex or multi-part questions - for example, "which devices are out of compliance and which contracts cover them" now draws on the right expertise for each half of the question, and the system plans and sequences the steps needed to answer it rather than attempting everything in one pass.

Raynée now shows its thinking as it works through a question - the plan it formed, which area it's checking, and why - instead of just producing a final answer. Users can follow and challenge the reasoning behind a response rather than taking it on faith, which matters most for compliance and licensing answers where the "why" behind a number is as important as the number itself.

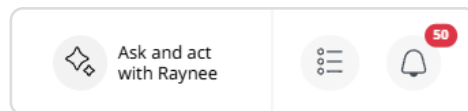


A new view of Raynée, showcasing features such as reasoning, a list of thoughts, an artifact panel, and a more detailed description and improved performance.

Raynée also runs on an upgraded, more capable underlying AI model, improving the quality of its answers and its ability to work through complex requests that involve multiple steps or multiple areas of the product.

Any action with real consequences - installing software, running a script, removing an entitlement - still requires explicit confirmation from the user before Raynée carries it out.

Not sure how to start? Click the redesigned "Ask and Act with Raynée" button to get started.



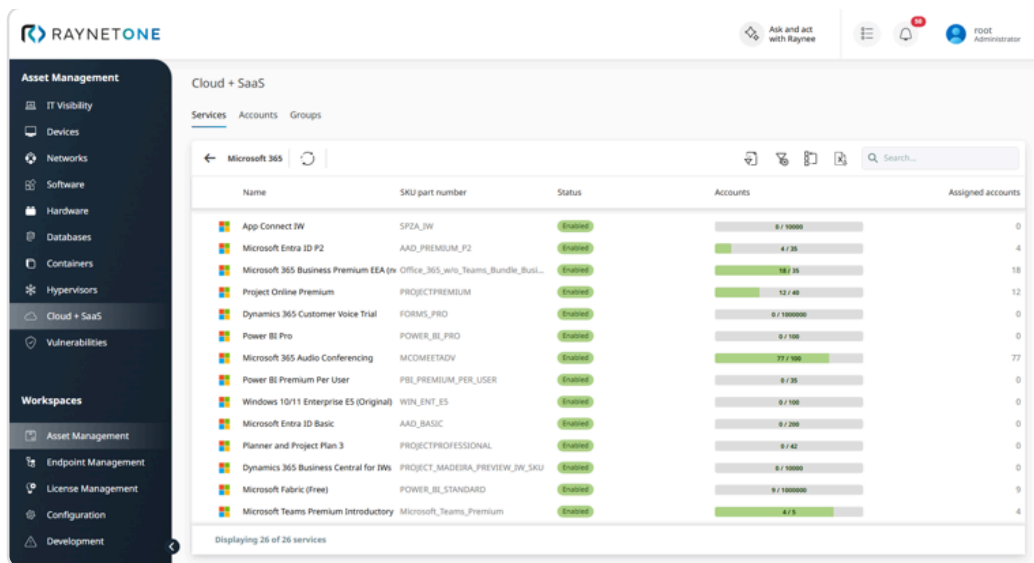
Cloud + SaaS Management and Unified Integration Management

Cloud and SaaS platforms used to show up in Raynet One as whatever a Data Hub connector happened to feed in, with no dedicated screen, no shared data model, and no consistent way to add a new one. This release gives cloud and SaaS data its own home: a generic data model that any SaaS connector can plug into, a management screen for the first provider built on it, and a redesigned way to add, configure, and monitor every integration in one place.

Microsoft 365 as a first-class data source PMD-17

Microsoft 365 is usually the largest license line item for an enterprise customer, split across EA subscriptions, E3/E5 tiers, and add-ons like Copilot, Defender, or Teams Rooms. Until now, that data lived in Raynet One Data Hub.

From this release, M365 is now a first-class connector inside Raynet One. The new Microsoft 365 Management screen shows product allocation, license status, and the user accounts each license is assigned to. Behind it, users, groups and services, and usage activity (sign-ins, mailbox, Teams, OneDrive signals) all flow into a generic SaaS data model, not an M365-only one, so the next SaaS connector built on top of it inherits the same structure instead of starting from scratch.



The Microsoft M365 Management screen shows product allocation, status, and assigned accounts (users).

Other new connections PMD-15

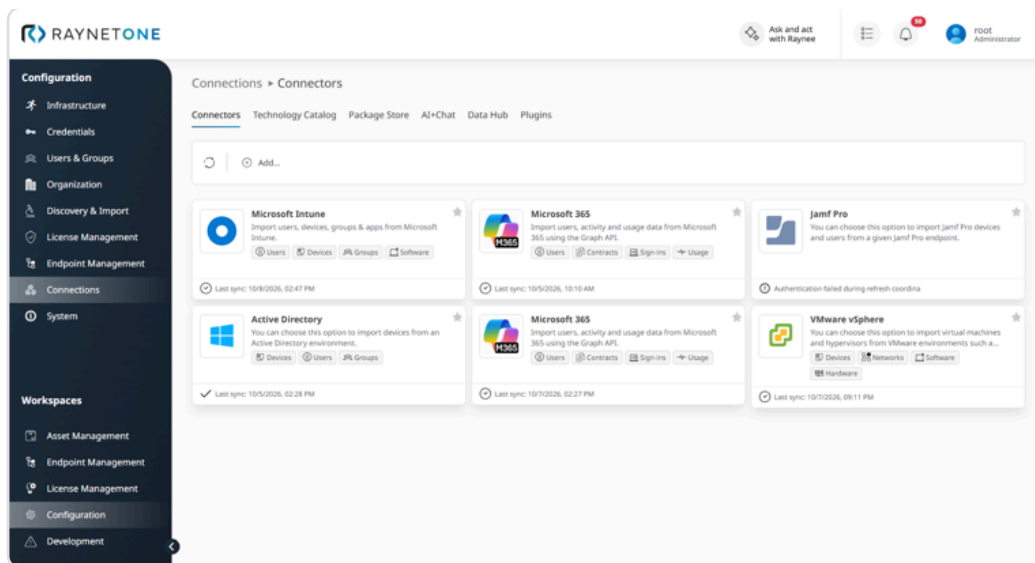
Alongside M365, Raynet One ships a first wave of native connectors covering endpoint and cloud security tools that previously required a Data Hub platform:

- Adobe Admin Console - users and groups RCP-828
- Microsoft Intune - devices, users, groups, apps RCP-835
- Microsoft Defender - devices RCP-840
- Cisco Meraki - devices RCP-830
- Jamf Pro - devices, users, apps RCP-836
- Jamf School - devices, apps RCP-837
- Nutanix Prism - devices, users, groups RCP-841
- Prisma Cloud - devices, apps RCP-843

i Some of these are in a preview state and need to be toggled on with a dedicated switch.

Unified integration management PMD-13

Adding or managing an integration used to mean finding it buried under Devices. It now lives under Configuration → Integrations, a dedicated settings screen that shows what's already connected (or suggested), and the full connector catalog opens when you click the "Add..." button.



The configuration screen is now home to your active integrations and connections. You can add new items from here.

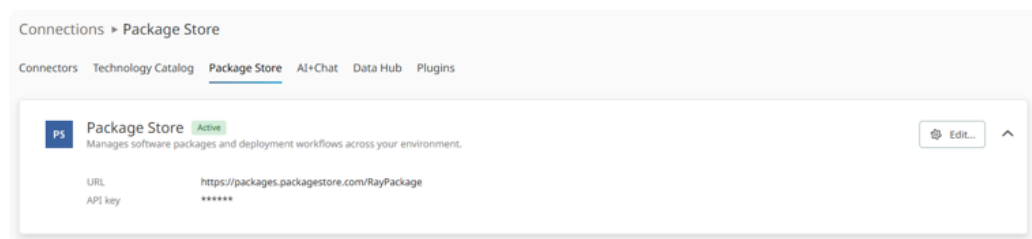
Adding a new connector walks through a short wizard: pick the provider, fill in its specific credentials (tenant ID, client secret, certificate, depending on the connector), tag the instance for environments that need more than one (Production vs. Test), and run a test before saving. Once saved, the integration runs on its own schedule and shows up in the list with inline status. Removing an integration gives the option to also purge the data it imported, instead of leaving orphaned devices or accounts behind.

Seamless integration of previously available data sources PMD-15

Several previous integrations have been remodeled to use the new integration pattern:

- VMware vSphere
- Microsoft Endpoint Configuration Manager
- Active Directory
- Integrations with Raynet products: Technology Catalog, Package Store, Data Hub
- AI services

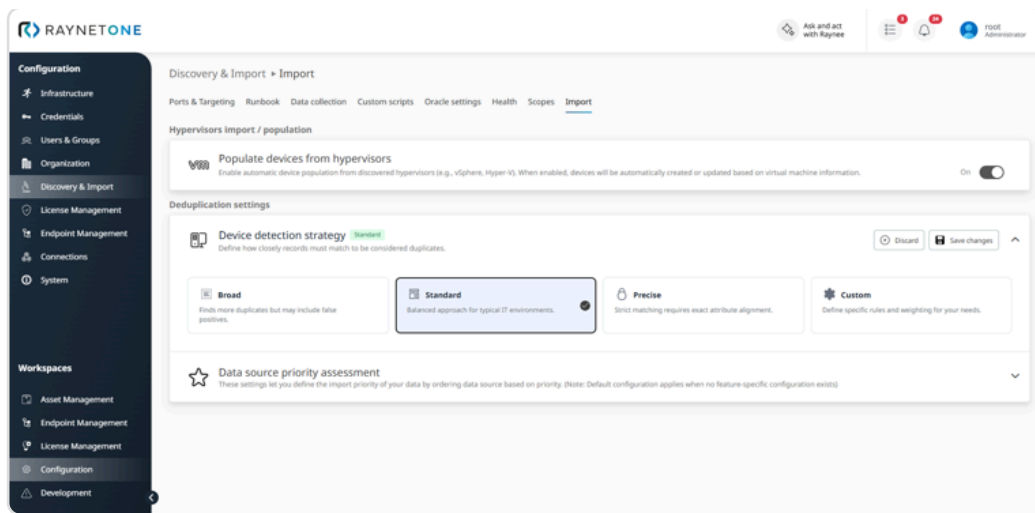
The new pattern replaces the previous integration screen and several device-oriented controls with a single source of truth.



The connection screen has become a central hub for all cloud connectors, integrations, and plugins.

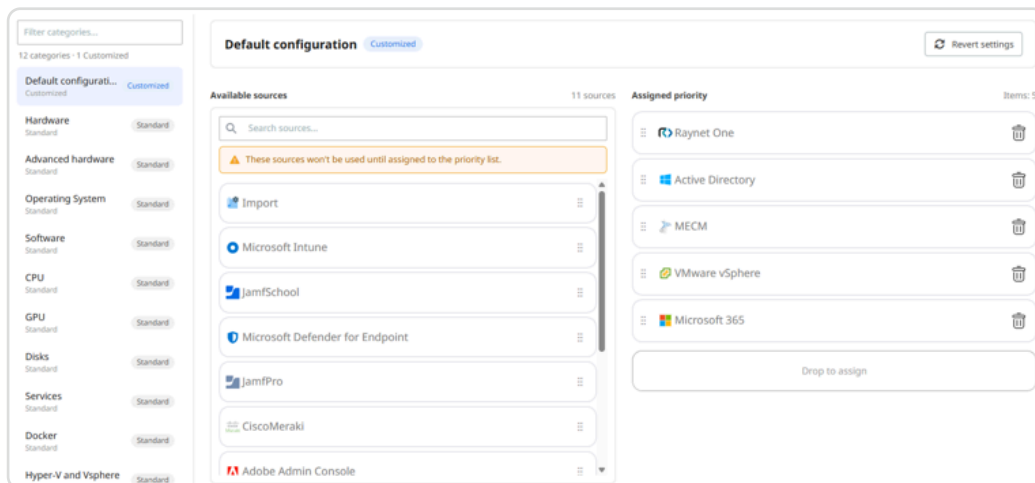
Configurable, Enterprise-Specific De-duplication and Reconciliation Options PMD-142

Raynet One now exposes the deduplication and source reconciliation controls that previously lived only in Raynet One Data Hub. Admins and SAM managers can see exactly how conflicting data from multiple sources gets resolved, instead of treating reconciliation as a black box or escalating routine adjustments to professional services.

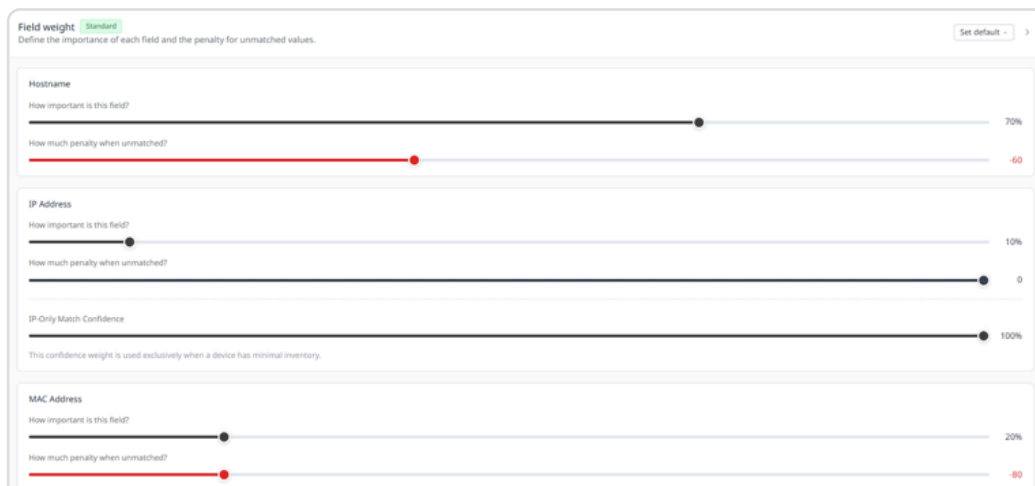


Standard presets are available to reconcile discovered items.

For each entity type, admins can reorder source priority by drag and drop (for example, promoting Raynet One above Active Directory when AD is overwriting a correct hostname), choose the active deduplication strategy, and configure which source wins for individual fields when values conflict. A reset-to-default option restores Raynet's recommended priority order at any time.



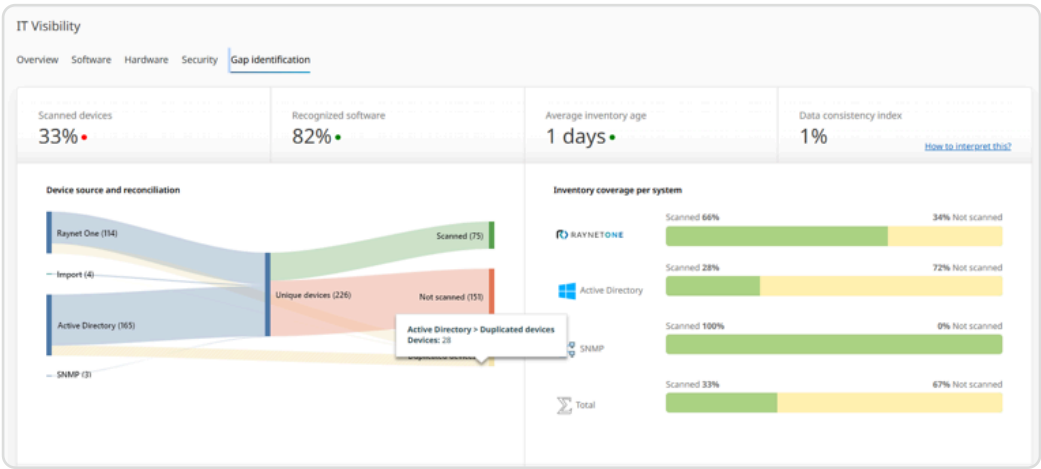
It is easy to use the drag-and-drop configuration to select which sources matter most and which do not. The default values are reasonable for most enterprises.



Every field can be adjusted to match the specific details of the enterprise environment perfectly.

A read-only reconciliation trace, available from the device, software, and user detail views, shows which source provided each field's current value and which rule decided it. This turns a "why does this record look wrong"

question into a two-click answer instead of a support ticket.



The IT Visibility Sankey chart helps users to understand which sources were deduplicated and which resources are relevant for SAM.

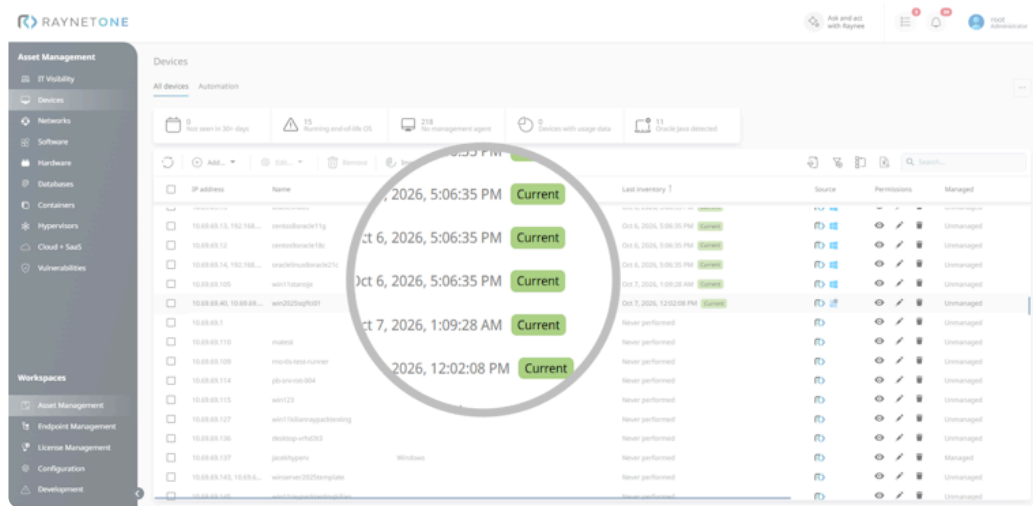
Inventory Health: Know When Your Device Data Is Stale RCOR-3538 RCOR-3741 RCOR-4243

Raynet One now gives administrators direct control over what counts as "fresh" versus "stale" inventory data. Instead of a single fixed inventory date, admins can define their own health statuses - for example **Current**, **Expiring**, and **Obsolete** - each with its own age threshold (how many days since the last successful inventory) and a color of their choosing.

Health assessment			
Inventory health status assessment These settings let you define assessment of an inventory health by assigning a maximum age of inventory data to a corresponding color and status. (Note: It might take a while for the changes to take effect.) Add new status...			
Status	Color	Inventory age ↓	Description
Obsolete		90	After 90 days, set status to Obsolete.
Expiring		32	After 32 days, set status to Expiring.
Current		0	After 0 days, set status to Current.

The configuration area - colors and thresholds are customizable.

Up to five statuses can be configured to match how an organization actually wants to think about data trustworthiness.



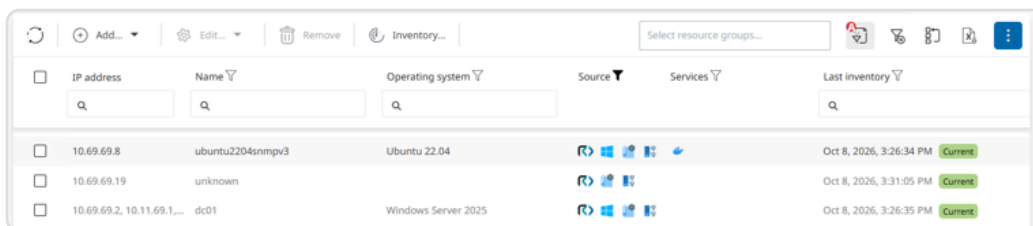
The resulting status now shows directly in the Devices list, as a colored tag next to each device's last inventory date, so administrators and SAM consultants can spot stale data at a glance instead of scanning raw dates.

The IT Visibility Gap Identification dashboard's inventory age graph reflects the same statuses and links straight through to a pre-filtered device list, making it a one-click path from "here's a data quality gap" to "here are the exact devices behind it."

The key challenge for compliance and license calculations is that a device with stale inventory data silently distorts license position, vulnerability exposure, and asset counts. Giving admins a visible, configurable health signal means data quality problems surface before they affect a report.

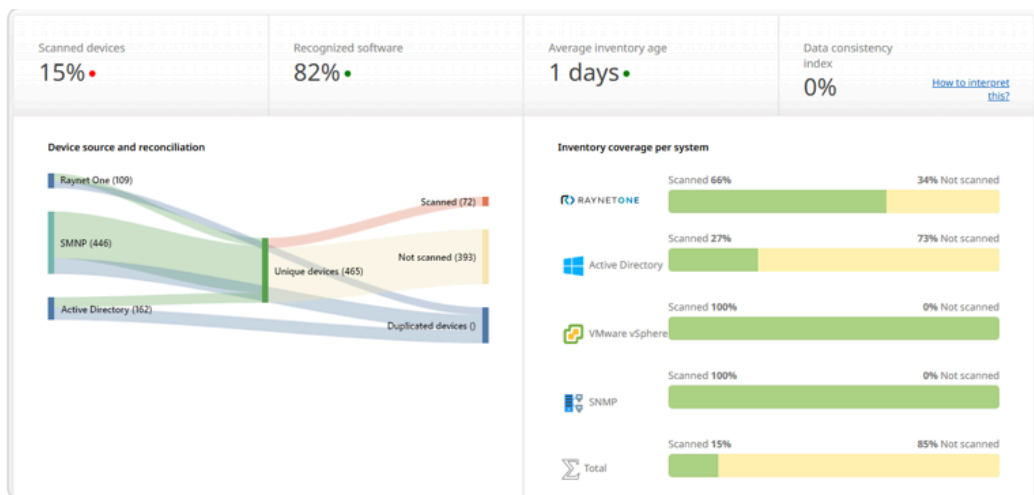
First-class Support for SNMP Devices PMD-24

SNMP-based device discovery is now natively supported in Raynet One, built on the same discovery technology that previously existed in RayVentory Scan Engine.



The list of devices combines data from different sources to avoid duplicates. In the above example, the device Ubuntu2204SNMPv3 appears in many import sources, including Active Directory, network discovery, SNMP, and manual import.

One unified instrument list. Device scan instruments - Zero-Touch Windows, Zero-Touch Unix, and now SNMP - live in a single list instead of being split by OS. Administrators can enable, disable, and reorder instruments to match how their environment actually scans; SNMP sits at the lowest default priority, after the Zero-Touch instruments, since it's typically the fallback for devices that can't be reached any other way (network gear, printers, and similar SNMP-only devices).



The IT Visibility screen shows that SNMP is part of the out-of-the-box scanning and normalization pipeline.

SNMP now has its own credential type in the Add/Edit Credentials wizard, covering community strings and SNMP v3 authentication and privacy settings.

Add credentials

1 Credential type
2 Basic settings
3 **Authentication**
4 Summary
5 Progress
6 Finished

Authentication
The settings which determine how the authentication is carried out.

Protocol version
The SNMP protocol version to use.

- ☐ SNMPv1
The default network management protocol version, which is widely used and supports a variety of network protocols. It offers no security options.
- ☒ **SNMPv2c**
An improved SNMP protocol version that improves performance and communications, while still not offering any security options.
- ☐ SNMPv3
The SNMPv3 protocol version introduced mechanisms for security and administration. It offers both strong authentication and data encryption for privacy.

Community string

public_Raynet_Monitoring_2026

[Back](#) [Next](#)

The Credentials Management Wizard now supports SNMP out of the box.

Device classification reuses the existing OID-to-vendor rule configuration from our RayVentory product family, so users moving from RayVentory Scan Engine / Inventory Agent-based SNMP scanning to native Raynet One scanning get the same device detection they're used to, without rebuilding their rule set from scratch.

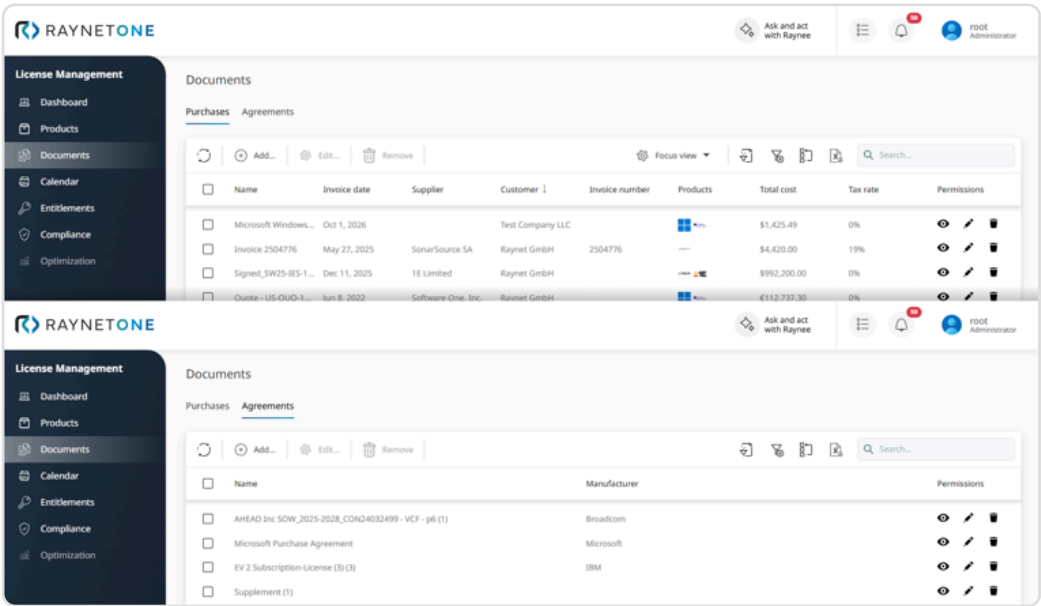
These changes in Raynet One 2026.4 bring SNMP devices - network gear, printers, and anything else only reachable via SNMP - into the same unified inventory as every other scanned device.

Reworked Contract Management PMD-34 PMD-107 PMD-122 PMD-108 PMD-109

Contract data in Raynet One used to live as flat, isolated records. A real enterprise agreement is rarely one document - a master agreement sits on top of purchase orders, which get modified by supplements, addendums, and special clauses. None of that structure was represented before, so special conditions buried in a PDF attachment were easy to miss and compliance positions could be wrong without anyone noticing. This release restructures how contracts are modeled and reviewed.

Purchases and supplements as separate record types

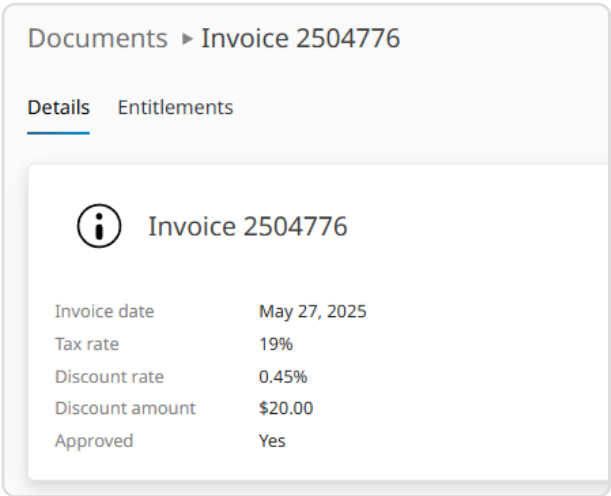
Contracts are now split into Purchase Orders and Supplements (special agreements, addendums, clauses), each a distinct, linkable record instead of one flat entry. This lets a SAM manager see exactly which supplement modifies which purchase order rather than reconstructing that relationship from memory or from scattered attachments.



In Raynet One 2026.4, the "Contract" screen has been replaced by two new screens: "Purchases" and "Agreements." Both have their own intrinsic data model - purchases are structured, but agreements are not - and they have different semantic meanings for UI and AI usage.

Discount rate on contract items

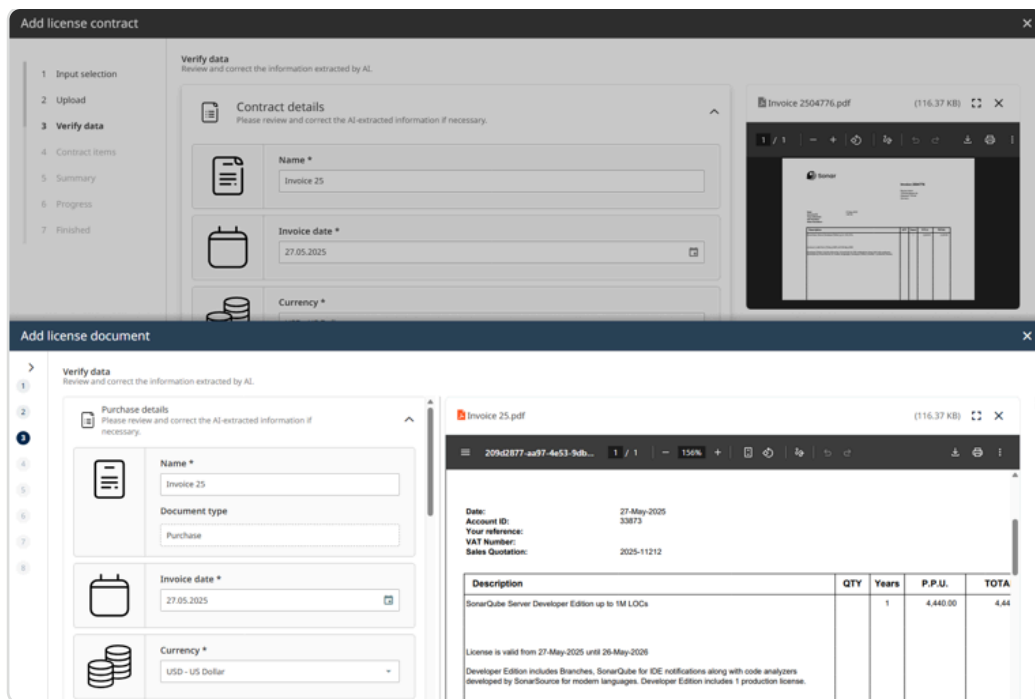
Contract items now support a discount field, entered as a percentage or a fixed amount. The total price is calculated automatically from unit price, quantity, and discount, so contract managers no longer need to pre-calculate a discounted unit price by hand before entering it.



The discount rate can now be extracted automatically or set manually.

Side-by-side document comparison

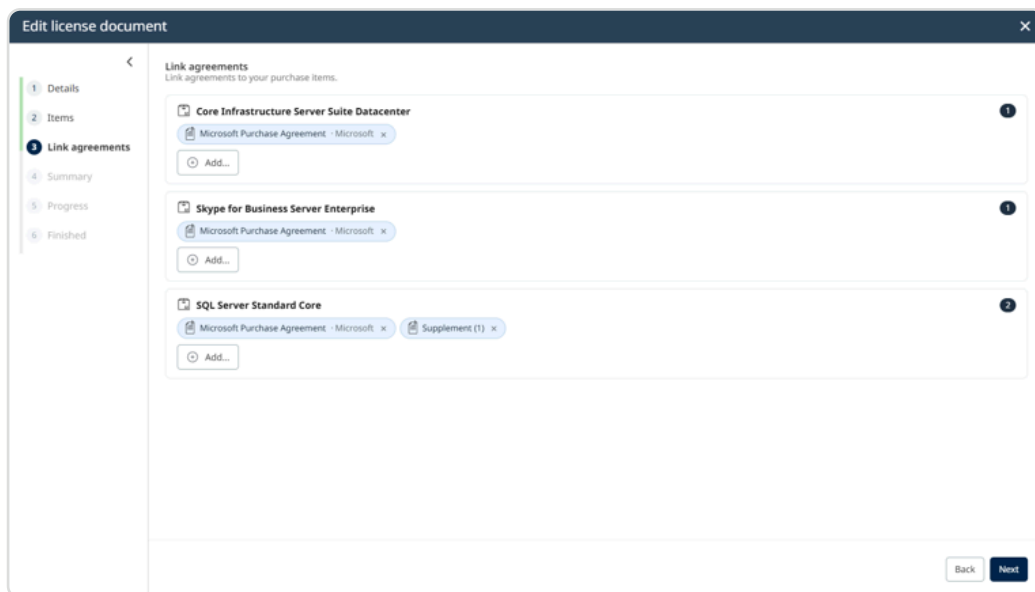
The purchase order upload comparison view has been reworked with a larger document display and a slimmed-down navigation panel, so source documents and extracted data can be reviewed side by side on one screen without constant scrolling and zooming.



Previous version 2026.2 (top) and the current 2026.4 (bottom) comparison, showing exactly the same document. The draggable splitter can now be used to easily compare the interpreted content against the source document side-by-side. The sidebar can be collapsed.

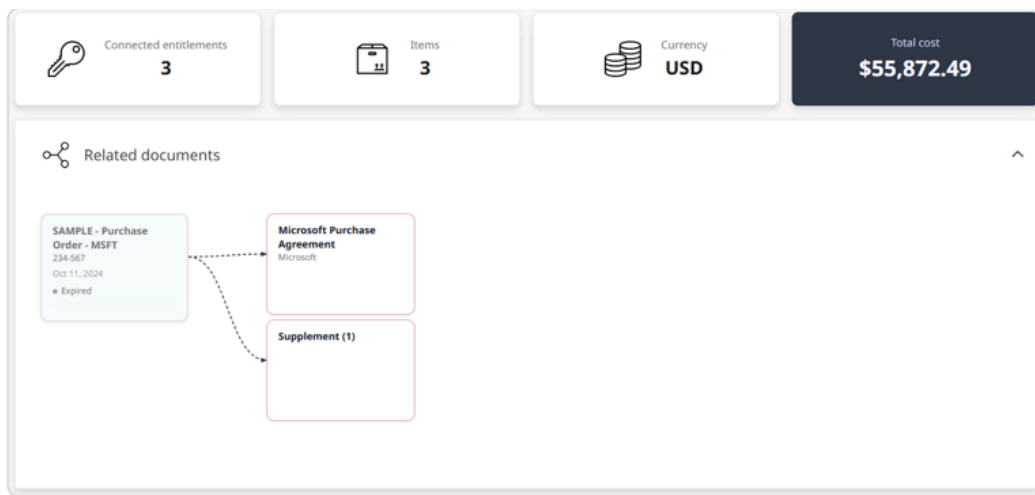
Contract linking

Purchase Orders, Supplements, and Evidences (the underlying physical documents) can now be linked to each other, building a document graph that reflects how the contract actually works. This graph feeds directly into license term and compliance calculations, so special agreements apply automatically instead of requiring manual lookup every time.



Purchase documents (contracts, invoices, Purchase Orders) can be linked to additional documentation, such as license agreements. AI-based analysis automatically suggests relationships.

These relationships are visualized using a topology diagram once imported:



The topology of the relations between contracts and documents.

These relationships provide vital information about license metrics, rights, and consumption methods to both chat and non-chat workflows. This ensures that the information is precise, reflects standard settings, and respects individual agreements.

Other contract-related improvements:

- It is now possible to attach agreement PDF to a manually entered contract.
- This release improves the extraction and logic for upgrade and downgrade rights.

Easier Entitlement Management RCOR-1455

Technical and commercial products on their own page

Products and product suites have been moved out of the general contract view onto a dedicated page, separating the technical product (what was actually discovered/normalized) from the commercial product (what the contract/licensing terms refer to). This removes the guesswork of matching a contract line to the right catalog entry inside a crowded contract screen.

The screenshot shows the Raynetone interface with a sidebar menu on the left containing options like License Management, Dashboard, Products, Documents, Calendar, Entitlements, Compliance, and Optimization. The main area displays the 'Products' page, which is split into 'Commercial' and 'Technical' tabs. A table lists products with columns: Name, SKU, Product count, Purchase item count, Entitlement count, and Permissions. The 'Adobe Acrobat Pro' product is selected and highlighted.

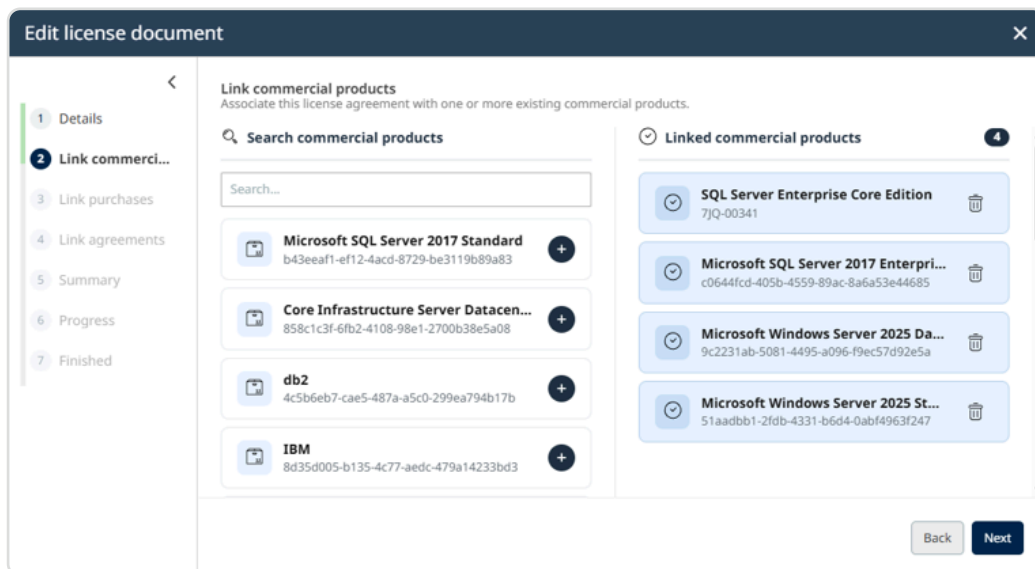
Name	SKU	Product count	Purchase item count	Entitlement count	Permissions
IBM	102506a0-2f82-4e48-b17c-0eb1278364d8	0	0	1	View, Edit, Delete
1E Service Desk Augmentation for ServiceN...	98b6d3aa-f029-4ab9-b1e7-dca4e705e9b9	1	0	1	View, Edit, Delete
Microsoft SQL Server 2017 Enterprise	c0644f0c-405b-4559-89ac-8afa53e44685	1	0	1	View, Edit, Delete
SQL	94339b30-d163-441a-9346-99ca13c92dc5	0	0	1	View, Edit, Delete
SQL Server Standard Core Edition	a6a994d2-9c3c-4a4d-95cf-07137d639dcd	1	0	2	View, Edit, Delete
Adobe Acrobat Pro	c3679130-58ac-40d4-a5c5-d1e883923a36	1	1	1	View, Edit, Delete
Windows Server 2012 R2 Standard	a7f8b014-07a4-4152-a278-360a67b88f87	1	0	1	View, Edit, Delete
Copilot	76cf019a-e2e1-4f58-8c46-0e965c7ad2cb	1	1	1	View, Edit, Delete
Microsoft SQL Server 2022 Standard	339d2037-30e2-42ef-b44c-23afbbe808b7	1	0	1	View, Edit, Delete
Excel	3efaf9b22-f860-4d3f-8bd2-fc7083402b70c	1	0	1	View, Edit, Delete
Logic Tan	5f6f6edd-d4bd-4d7d-9d5d-ea4f614fb05	1	0	1	View, Edit, Delete
db2	4c5b6eb7-cae5-487a-a5c0-299ea794b17b	0	0	1	View, Edit, Delete
Microsoft Remote Desktop Services CAL	b29983f2-f3d4-429a-9615-2eb978153c7	1	0	1	View, Edit, Delete

The new Screen Products approach clearly separates commercial and technical products, replacing the previous method of showing products only under entitlements and contracts.

Improved purchase documents management

The editing of purchase documents (invoices, Purchase Orders, contracts) has been extended. Using a simple wizard, the user is now able to verify and configure links between various items:

- Purchase document ↔ Master agreements
- Purchase document ↔ Purchase document (for example extensions)
- Purchase document ↔ Commercial product

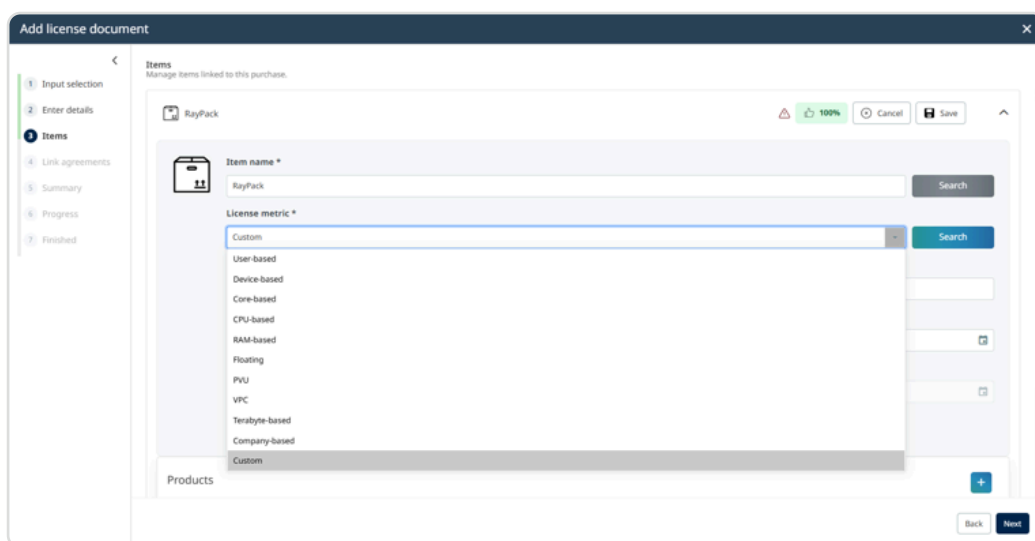


After the initial recognition, commercial products can be easily managed when adding or editing a license document.

New License Metrics (Custom / Company-Based) and Edge-Case Handling PMD-217 PMD-175

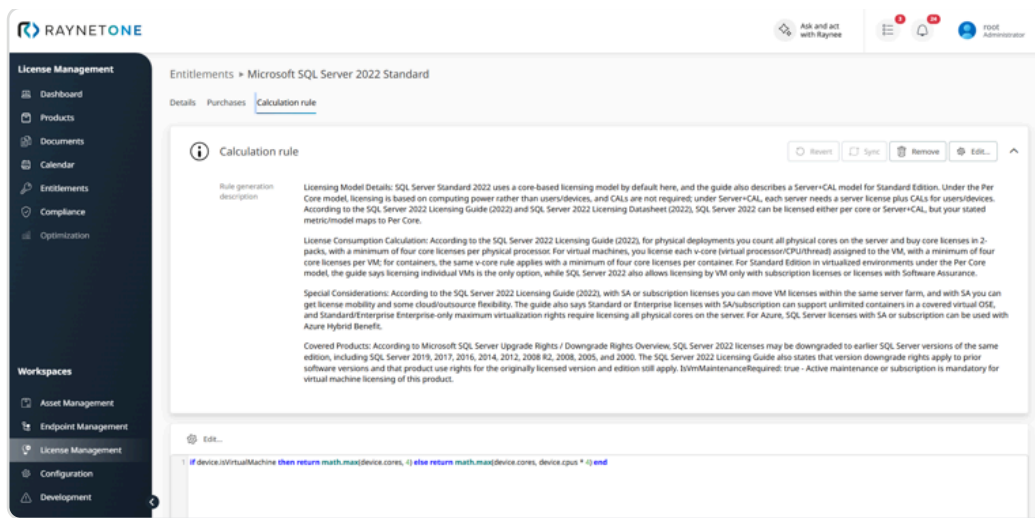
The Contract Analyzer now supports two additional license metrics beyond the standard models.

- The new **Company-based** metric covers licenses where cost or compliance is calculated per legal entity or company rather than per device, user, or processor, matching how some enterprise agreements are actually structured.
- When the Contract Analyzer can't confidently determine which metric applies to a contract line, it now assigns a **custom metric** instead of leaving the field blank or guessing incorrectly.



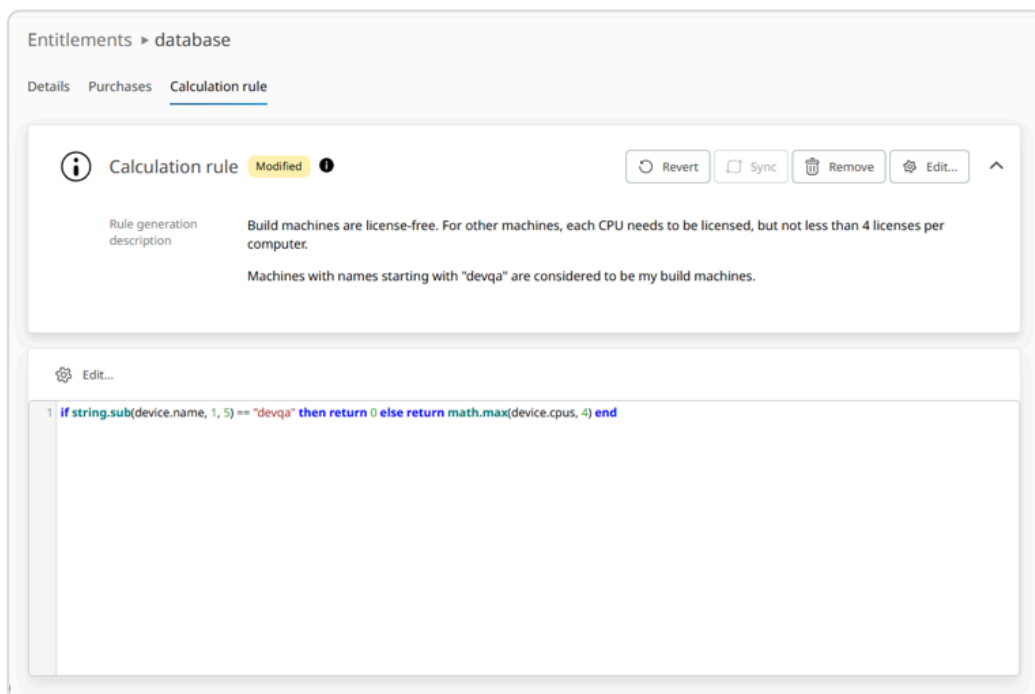
Both custom and company-based metrics are now available and can be assigned manually.

For complex licensing, there is an extended custom rule engine (previously known as DSL). This allows administrators to create license rules based on curated license information from License Codex. Users can also define their own licensing rules by writing human-friendly text, which Raynet One then converts into a precise formula that can be reviewed.



A sample license text that has been converted into a precise formula that takes care of licensing intricacies and metrics.

These rules and descriptions may be reviewed and updated retroactively if the license conditions change or if new license documents or terms are provided.

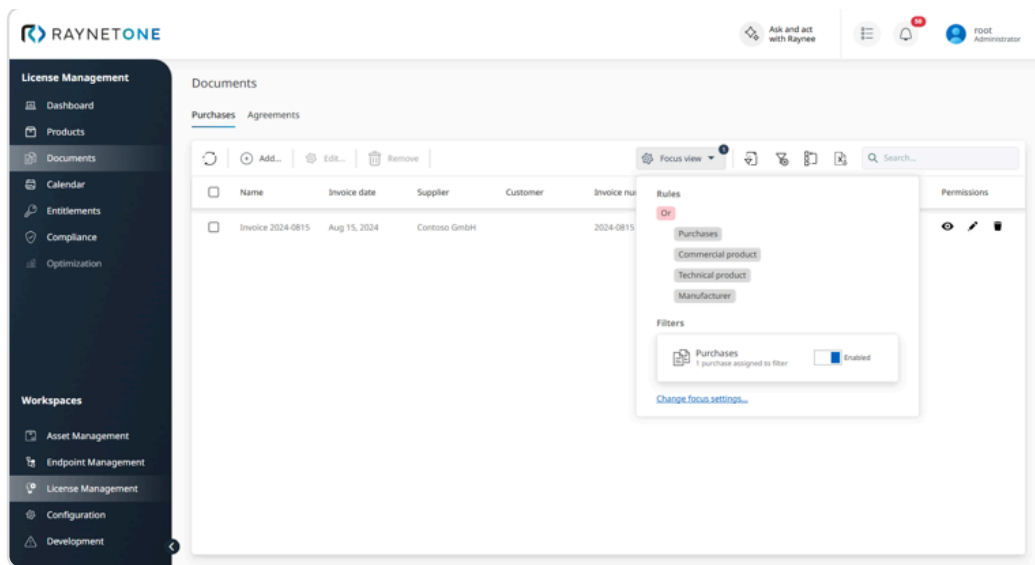


Sample use case: The user defined a rule that each development machine needs a license that meets specific conditions. The system then converts this rule into a simple formula that can be reviewed and applied to your devices.

Focus View and Permission Schemas in License Management PMD-121 PMD-124

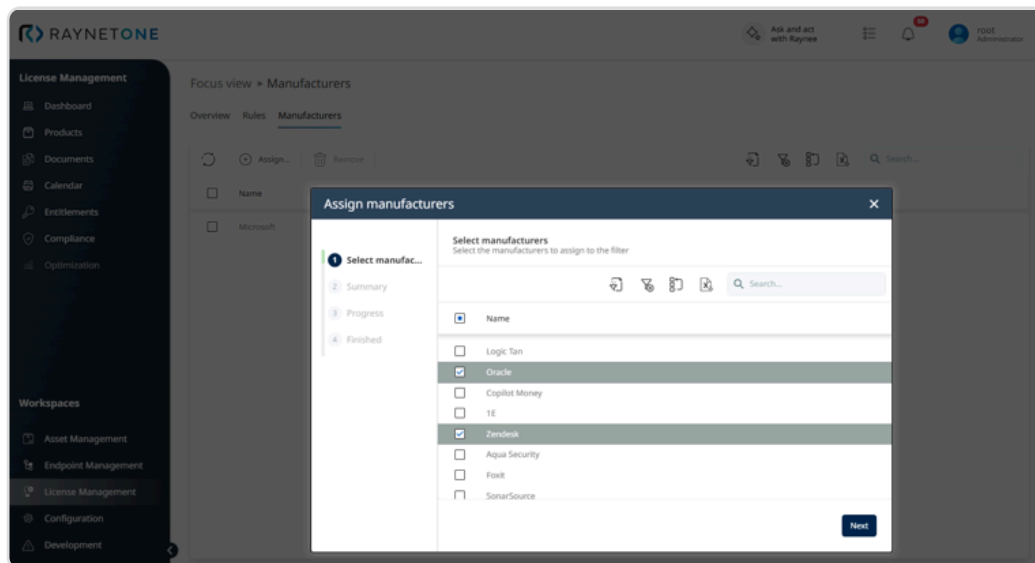
Focus View

Focus View lets a license manager narrow the entire workspace down to what they're working on right now - a specific contract, product, or vendor - instead of hunting through everything at once.



Focus on a specific purchase document with an active filter.

Once a focus is set, the Calendar, Entitlements, Compliance, and Documents grids all filter down to just that scope together, so switching focus from one contract to another doesn't mean re-filtering four separate screens by hand. A quick toggle switches between the filtered and unfiltered view at any time, so dropping back to the full picture - or confirming a focus is even active - is a single click rather than clearing filters one grid at a time.



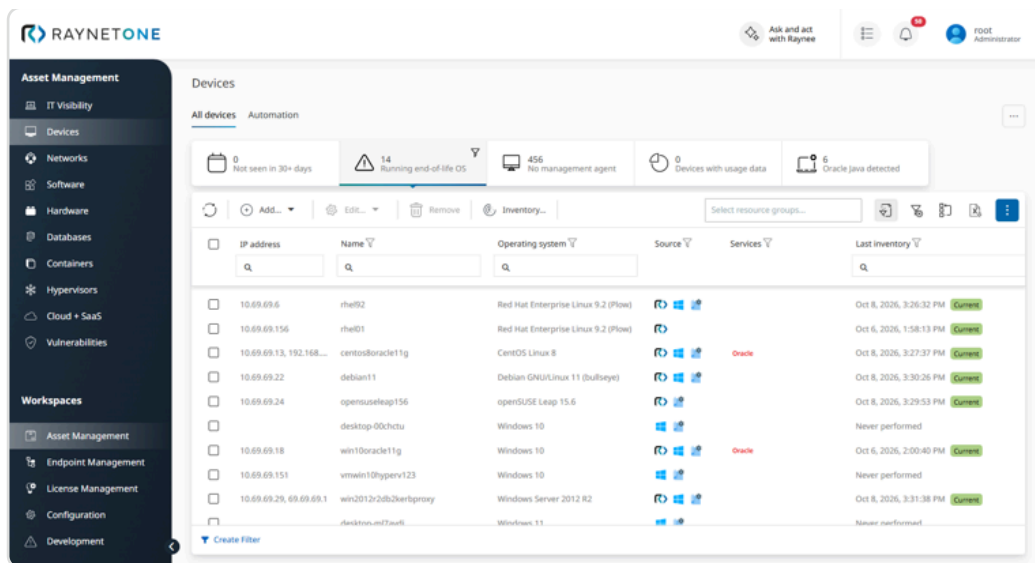
Configuring specific views of Zendesk, Oracle, and Microsoft products.

Permissions schema changes

This release includes a dedicated License Manager role, which eliminates the need for an administrator to manage license expenditures. The License Management workspace now has its own role-based access control, matching the segmentation already trusted elsewhere in Raynet One's asset management. Contracts and everything tied to them - entitlements, calendar events, compliance data - are scoped to the organizational area that created them, so teams managing separate license portfolios in parallel don't see each other's data by default.

Enhanced Data Grids PMD-129 RCOR-3659

There are several subtle improvements to the overall experience. Most data grids now have an additional panel showing three to five KPIs or characteristics with filtering options.

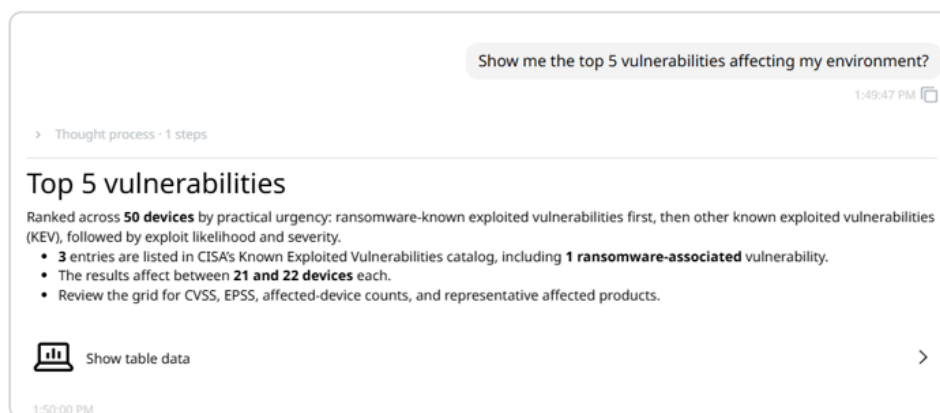


The activated filter only shows devices with an end-of-life operating system.

Improvements to Vulnerability Management PMD-18

Priority matters: CISA KEV, CVSS

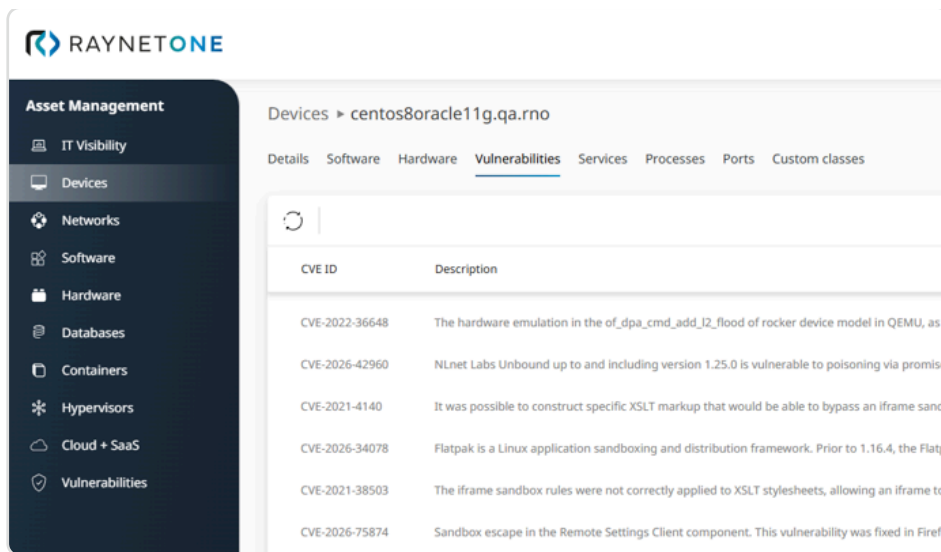
Vulnerability information now includes EPSS scoring and percentiles. The new dataset is also fully visible to AI agents. For example, asking Raynée about the priority of vulnerability patching reveals that the best practices should be followed - under the hood, it will pull KEV and CVSS metrics and organize them into meaningful insights.



Raynée has access to the underlying EPSS / KEV data.

Vulnerabilities at device- and software- level RCOR-804

The device view has been extended to show the vulnerabilities that apply to the device in question. What was previously achievable only through complex filtering is now a core feature available for each scanned device.



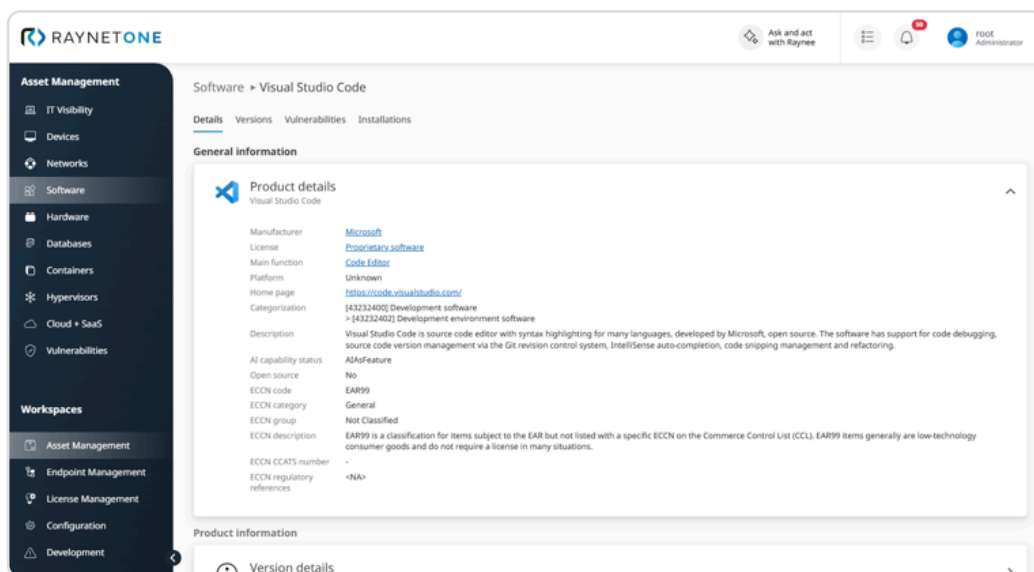
Drill-down to a specific device to see the list of vulnerabilities that affect it.

Enhanced Technology Catalog Integration PMD-18 RCOR-2607 RCOR-3932 RCOR-1551

The normalization and enrichment of software and hardware data has been substantially improved. Powered by Raynet One Technology Catalog, it can now pull a richer set of data, and the process has been refined for a smoother experience.

Security and governance enrichment

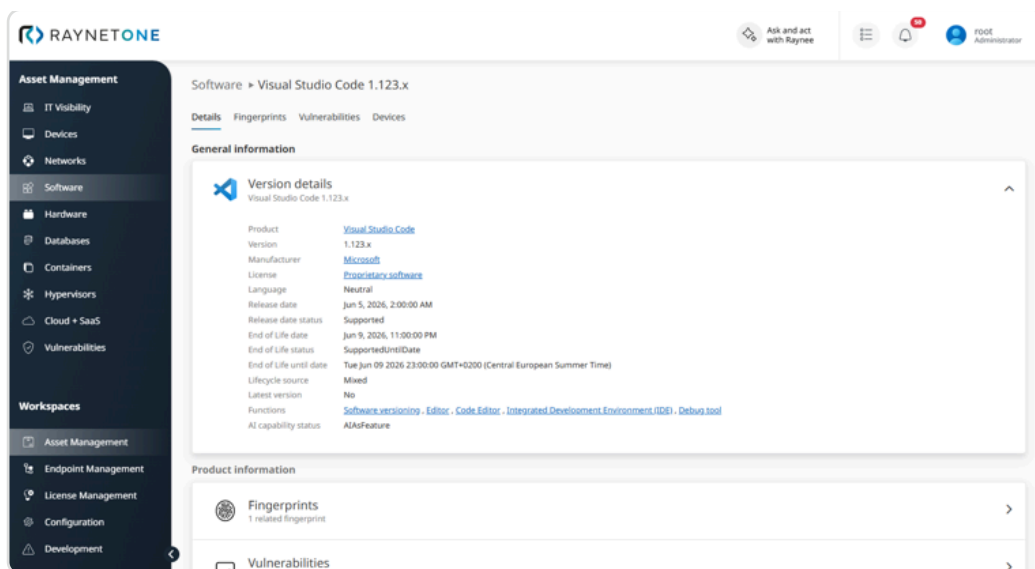
Every catalog-matched product now carries CISA KEV and EPSS exploitability scores alongside standard CVSS severity, so prioritization can be based on what's actually being exploited in the wild, not just theoretical risk. Products are also enriched with export-control classification (ECCN), an AI-capability flag, country of origin, open-source status, and package type - governance signals that previously had to be tracked outside the product.



A sample product view with various extra governance attributes, ranging from AI capability status (an optional feature in this case) to export control classification (ECCN).

End-of-life status

Many vendors do not announce an official end-of-life date, but one can be implied. In these scenarios, Raynet One distinguishes between situations in which the date is unknown and situations in which the date is implied or assumed. This status now drives IT Visibility dashboards and filtered drill-downs. This allows you to trace a device flagged as end-of-life risk straight back to the products behind it.



Each detected version now has a rich set of attributes. More context information is available for the lifecycle and dates. Other attributes inherited from the product still apply.

Hardware now gets the same treatment as software.

CPUs, GPUs, and enclosures are now matched against the Technology Catalog the same way software always has been - normalized, deduplicated, and enriched with manufacturer data and logos instead of sitting as raw, unmatched inventory.

Reliability fixes underneath.

The catalog sync is now more resilient. A handful of data-correctness bugs are also fixed in this release: vSphere services are now catalog-matched so they get real EOL dates, Oracle- and SQL Server-sourced software is correctly counted in catalog install statistics, and vendor country names display with correct casing.

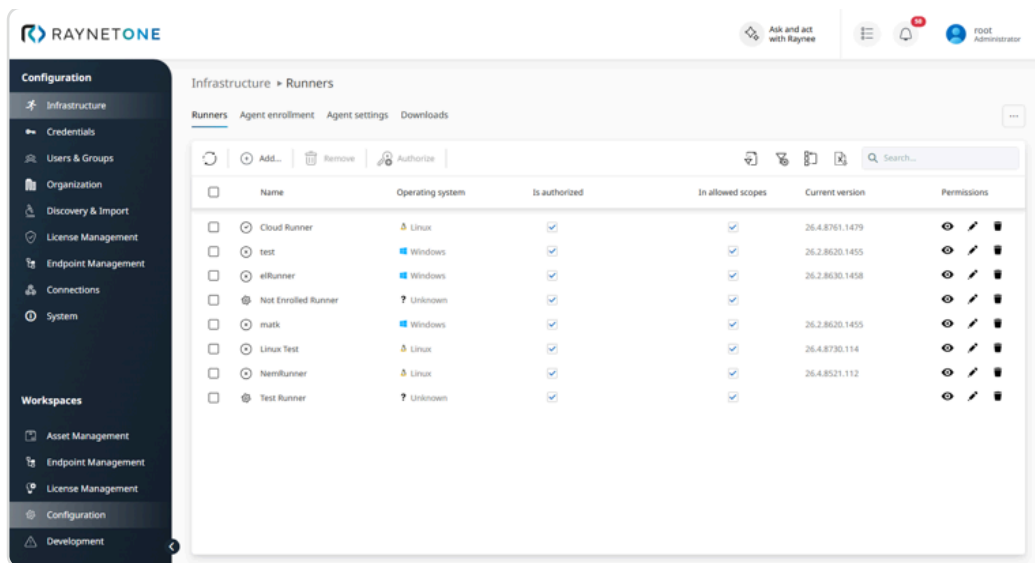
New configuration and navigation RCOR-3140 RCOR-3960 RCOR-4185

Configuration is now organized into focused sections, each with its own tabs for related sub-areas, replacing the old flat list:

- **Organization** - organization units, blacklisting, and assignment rules, grouped together since they're all about company structure, not system access.
- **Users & Groups** - system users, groups, and resource groups in one place.
- **Discovery & Import** - scan instruments, targeting, data collection, Oracle probes, Scopes, and network/port settings - everything about how and what gets scanned, previously scattered across Settings and separate sidebar items.
- **Infrastructure** - Runners, agents, enrollment tokens and runner downloads together, since they all answer the same question: how scanning infrastructure connects to Raynet One.
- **Connections** - Integrations, the Technology Catalog connection, AI Chat, Device Control, SAM Cloud, and installed Plugins, all grouped as external connections instead of scattered standalone tabs.
- **Credentials** - credentials and authentication providers together.
- **System** - version, license entitlement, health checks, and the self-service portal split into separate tabs.

License Management and Endpoint Management now get their own dedicated top-level menu entries instead of being buried inside Settings.

The result is a structure that groups by what administrators are actually trying to do - connect infrastructure, manage access, configure scanning - rather than figuring out where the knobs are.

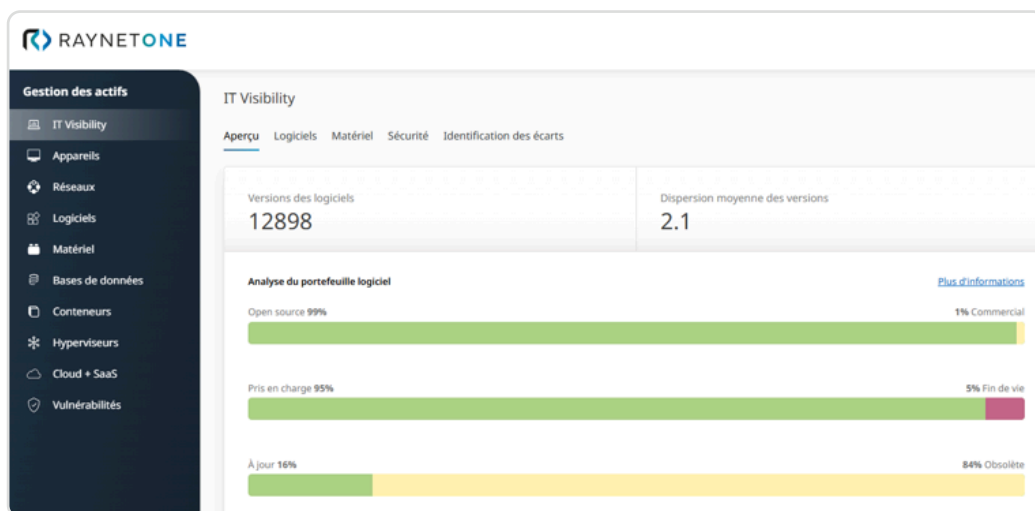


A new structure and organization of options - all settings at your fingertips, grouped logically in a new layout that helps with both initial setup and advanced system changes.

“Discover to Manage” - Now Multilanguage PMD-125

We’re expanding the language support of Raynet One. The user interface is now available in German, French and Turkish, making it easier for more users to discover, understand and manage their IT environment in their preferred language.

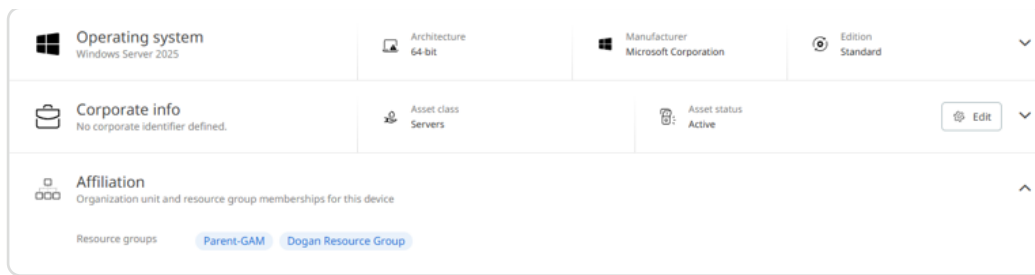
Discover to manage. Entdecke, um zu verwalten. Découvrez pour gérer. Yönetmek için keşfet.



Raynet One French UI.

Affiliation RCOR-3823

Resource Group and Organization Unit membership was already being tracked behind the scenes to power device filtering, but there was no way to see that affiliation on a device itself without going back to the filter. Device Details now shows which Resource Group and which Organization Unit a device belongs to directly on the device, so branch, unit, and authorization context is visible at a glance instead of requiring a filtering detour to confirm.



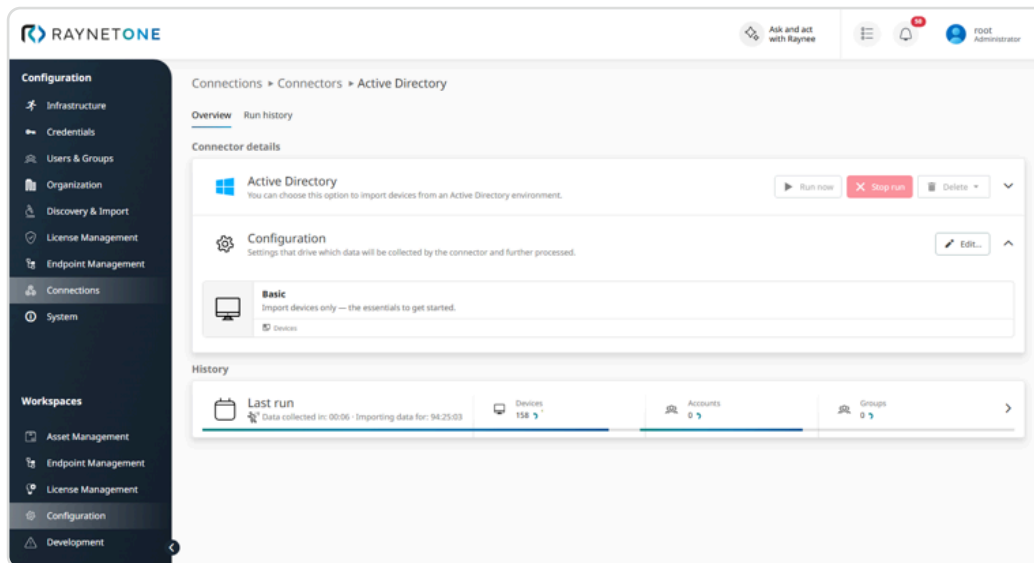
The device view now shows the affiliation.

Easier Troubleshooting of 3rd-Party Systems Connectivity PMD-15

Connections to third-party services, such as Intune, Active Directory, and VMware, are now easier to manage and more straightforward to troubleshoot. Thanks to a dedicated UI, users can determine the following with a few clicks:

- When was the last run, and did it succeed?
- What is being imported?
- What was actually imported? Which entries are new, and which were previously there?

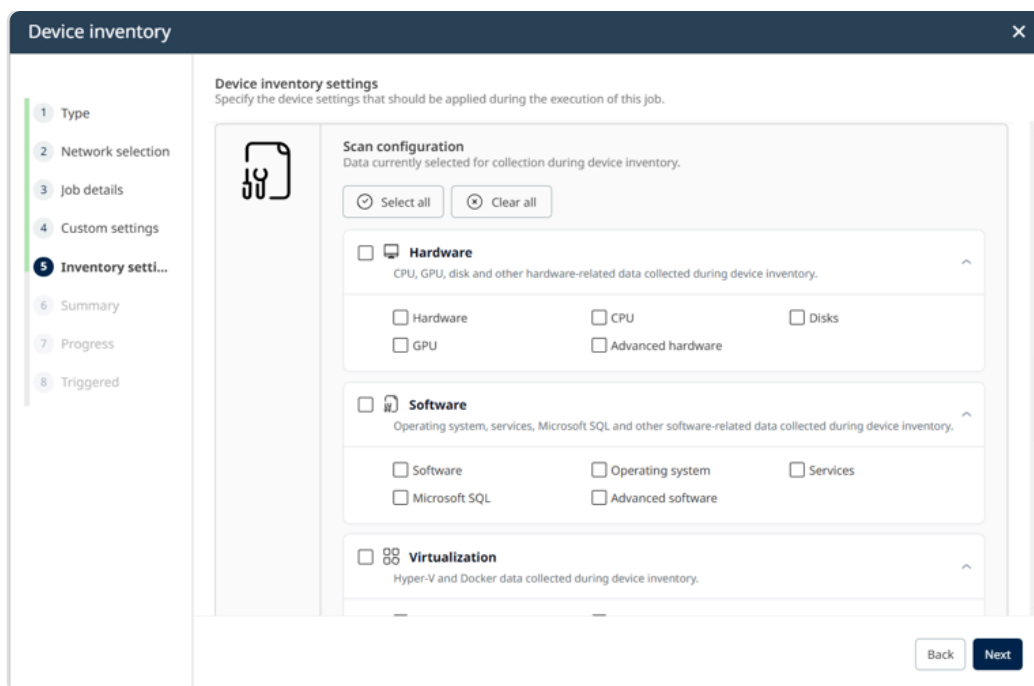
There are also functions for controlling the timing, starting and stopping the integration, and adjusting the settings.



The Active Directory import run provides precise control, manual import, a history of runs, and configuration settings. This pattern applies to all modern integrations.

Inventory Configuration Improvements RCOR-4109

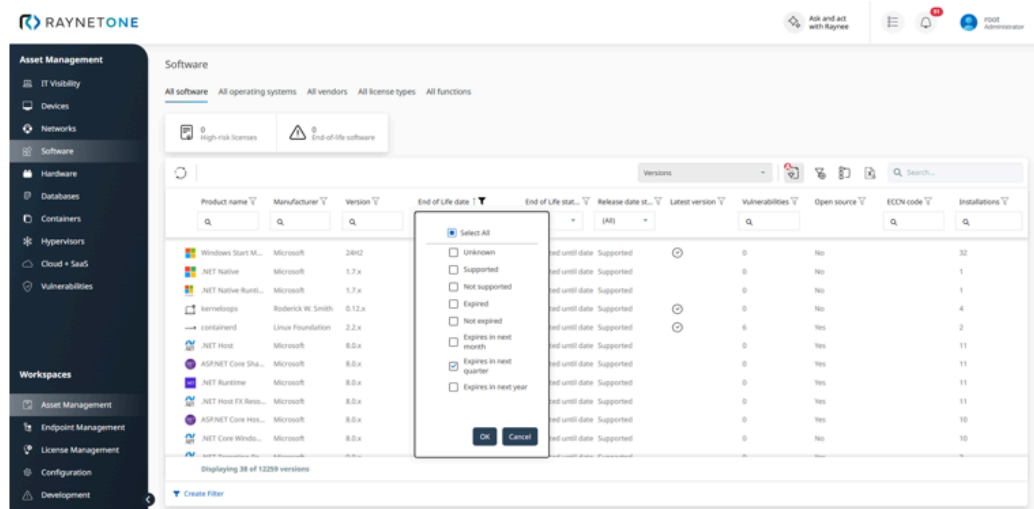
The inventory settings are configured using the new selector that groups related themes and allows users to easily select what they want to scan or exclude from the scan. This feature is available in all places involving the inventory configuration.



The new scan configuration, as displayed in the Device inventory wizard.

Filtering by End-of-Life is Now Easier

The Software Grid has been updated. There is an extra row with quick filtering options, and filtering by end-of-life date is now more user-friendly. It is possible to use general terms, such as "expires in the next quarter," instead of specifying exact date ranges.



Filtering row enabled, now showing only expiring versions.

Other Improvements

- General stability improvements and fixes for reported issues.
- Added a ping option to Advanced Network Sweep discovery. [RCP-893](#)
- Added support for Oracle ANO settings. [RCP-855](#) [RCP-715](#)
- Added support for importing users and groups from Active Directory. [RCP-827](#)
- Improved support for Click-to-Run (C2R) applications. [RCP-663](#)
- Extended the REST API to include Kubernetes and SBOM data. [RCOR-4646](#)
- Added `ScopeId` to the REST API. [RCOR-4068](#)
- Clusters are now visible on the Database page. [RCOR-3968](#)

- Updated the vSphere connector to process data through Catalog Recognition. RCOR-3806
- Unified upload controls to provide a consistent user experience. RCOR-3124
- Added device management options to Network > Devices. RCOR-2184
- Improved CPU information display on the Devices > Hardware screen. RCOR-1981
- Made the elevation password optional when configuring Unix credentials with privileged rights enabled. RCOR-1927
- Added support for an unlimited number of entitlements. COR-1067
- Added Scope and/or Device ID columns to the Databases and Containers data grids. RCOR-572
- Improved Zero-Touch scan execution speed. RCP-653
- Renamed Product Number to Article Number. COR-4587