

Application Catalog

Last Modified on 2026-09-17

Overview

The Application Catalog, also known within Recast as the Setup Store, is a continuously maintained library of commonly used Windows and macOS applications. Instead of manually sourcing, packaging and validating applications, IT teams can retrieve ready-to-use setups directly from the Application Catalog and integrate them into their deployment workflows.

The Application Catalog supplies installers and application metadata to Recast’s [Application Workspace](#) and [Right Click Tools Patching](#).

Deployment-ready Packages

Standardized application packages include fully defined install and uninstall commands, detection logic, and requirement rules. Package metadata is consistent across applications, regardless of when content was added to the catalog.

Enriched Application Data includes basic deployment metadata and additional details, including categorization, CVE (vulnerability) data, and knowledge base articles.

Catalog Content & Updates

The Application Catalog includes the latest software releases from major vendors. Application entries are constantly updated to reflect the most recent releases and versions, delivering 80–90% of updates within 24 hours.

The catalog continues to expand based on customer demand and application usage trends. As an IT admin, you can request additions to the catalog [via the Ideas Portal or the Application Workspace Setup Store connector](#).

[Ways to explore the Application Catalog](#)

Application Security

For an explanation of the validation and security framework Recast applies to all Application Catalog content, see our Application Media Verification articles for [Right Click Tools Patching](#) and [Application Workspace Release & Patch Management](#).

Application Catalog FAQ

How can I see which applications are in the Application Catalog?

There are a few ways of exploring what’s in the Application Catalog:

Right Click Tools customers (with and without Patching licensing)	View the Application Catalog in your Recast Management Server View and Search the Application Catalog in Configuration Manager
Application Workspace customers	View Setup Store Connector Resources
Everyone	Browse Top 100 Supported Applications

Recast

How quickly after a vendor release do new application versions appear in the Application Catalog?

Recast continuously monitors new application releases and adds them to the catalog in a timely manner, with 80–90% of updates becoming available within 24 hours of a vendor release.

Speed never comes at the expense of quality. Every application version must pass multiple metadata, integrity, and validation checks before publication, ensuring that you receive deployment-ready content you can trust.

How does Recast ensure that applications aren't tampered with in transit to the catalog?

When sourcing, screening, and releasing application content for the Application Catalog, Recast's application management team applies a number of controls that ensure the accuracy, reliability, and security of installation media.

Malware Screening and Release Policy: After downloading installation media directly from a software vendor, Recast performs comprehensive malware screening on all vendor-provided binaries. This involves scanning the application files with VirusTotal's multi-engine antivirus scanning service to ensure the binaries are intact, originate from trusted sources, and contain no malicious payloads, corrupted files, or invalid digital signatures. If the scan indicates that an application version exceeds a predefined malware detection threshold, it is withheld from release.

Application Execution and Behavior Validation: The application is installed and uninstalled within a virtual machine, generating results, logs, and artifacts. The focus is on validating runtime behavior, not just static files. Dynamic evaluation identifies unexpected system changes, unsafe persistence mechanisms, and behavior that does not align with enterprise deployment standards.

Data Integrity and Secure Delivery: All files and installers leaving the Setup Store are hashed to detect alterations, and metadata delivered via the Consumer API is digitally signed to ensure it isn't tampered with in transit. All data is distributed over secure connections (standard TLS) to guarantee authenticity and prevent man-in-the-middle attacks. Additionally, an isolated, read-only customer access layer separates the packaging environment from consumer delivery as an extra defense-in-depth measure.

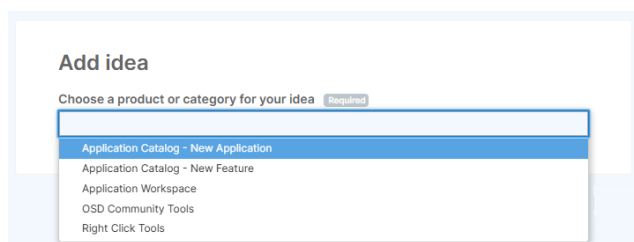
To learn more about how Recast ensures application security, see [Application Media Verification steps for Right Click Tools Patching](#) and [Application Workspace Release & Patch Management](#).

How do I request a new application be added to the catalog?

For Recast customers and partners, the primary way to request a new application is using the Recast Ideas Portal. Application Workspace administrators can also request a new product via the Setup Store Connector. Both methods send your request to the application management team for review. You'll receive updates as your request moves through the approval process.

To request an application using the Recast Ideas Portal:

1. Open the [Ideas Portal](#) in your web browser.
2. Click **Add a New Idea**.
3. Select **Application Catalog – New Application** from the drop-down.

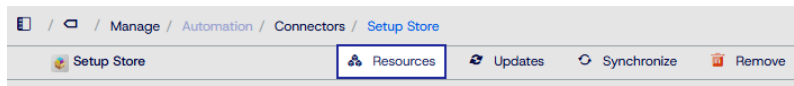


Recast

4. Fill in the application name, required details, and explain why you'd like it added.
5. Click **Add Idea**.

To request an application using the Application Workspace Setup Store Connector:

1. In the Application Workspace user interface, navigate to **Manage > Automation > Connectors**.
2. Double-click on the Setup Store connector and click **Resources**.



3. On the Resources page, click **Request product** on the table toolbar.
4. Complete the request form with the application details and submit your request.

Application Media Verification

Prior to creating applications and deployments for Configuration Manager or Intune, Right Click Tools Patching always verifies that the application media it downloads is valid and remains unchanged from the version that Recast's application management team downloads from the vendor and publishes to the Application Catalog (also known within Recast as the Setup Store).



The Application Catalog (or Setup Store) contains the thousands of curated applications available via Right Click Tools Patching.

Applications are published to the catalog once our application management team establishes the validity of their content. The Recast Application Catalog then consumes Setup Store metadata added by the team, allowing Patching to confirm that the content remains unchanged.

[Learn more about the Application Catalog](#)

Content Verification Process:

1. Recast's application management team downloads the installation media from the vendor and adds application metadata to the Setup Store. The metadata includes the download link to the installer and the hash checksum calculated from the installation media downloaded from the vendor.
2. The Recast Application Catalog consumes the Setup Store metadata and downloads the installation media from the Setup Store storage account. After download, the checksum is calculated and compared with the checksum in the Setup Store metadata.

NOTE: Should the installation media fail to download directly from the Setup Store, the Application Catalog downloads the installation media from the vendor using the download link in the Setup Store metadata. The checksum validation steps are identical.

3. When the checksum matches (confirming that we are using the same installation media the Setup Store team used when generating the metadata), Patching creates a ZIP file from the installer, calculates the hash checksum from the ZIP file, and stores it within the application catalog metadata.

Recast

4. When the Recast Management Server contacts the Recast Catalog, it receives the checksum for the ZIP file.
 5. The Recast Management Server requests the download URL from the Recast Application Catalog. The URL to the Azure storage account uses a short-lived SAS token.
 6. The Recast Proxy downloads the ZIP file from the Azure storage account using the download URL. After download, the hash checksum is calculated from the downloaded ZIP file and compared with the checksum in the Recast Application Catalog metadata.
 7. When the checksum matches the value received from the Application Catalog, meaning that the ZIP file is unchanged and the content matches what the application management team used when generating the original metadata in the Setup Store, Patching continues to create applications and deployments for ConfigMgr or Intune.
-
-