Recast

Application Media Verification for Right Click Tools Patching

Last Modified on 05.20.26

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 Setup Store.

> *The Setup Store contains the thousands of curated applications available via Right Click Tools Patching. Applications are published to the Setup Store 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.*

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.

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 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 Recast 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.