Application Media Verification

Last Modified on 06.18.25

Prior to creating applications and deployments for Configuration Manager or Intune, Application Manager always verifies that the application media from vendor websites and in the application catalog is valid.

Content Verification Process:

1. Recast's Application Packaging team adds application metadata to the Application Manager catalog. The metadata includes the download link to the installer and the hash checksum from the vendor website used when populating the metadata.

2. The Application Manager catalog consumes the application metadata and downloads the installer from the vendor website. After download, the checksum is calculated and compared with the application metadata. The download URL and checksum both come from the metadata added by the Application Packaging team.

3. When the checksum is valid, Application Manager creates a ZIP file from the installer, calculates the hash checksum from the ZIP file, and stores it within the catalog.

4. When the Recast Management Server contacts the Application Manager catalog, it receives the checksum for the ZIP file.

5. Application Manager or the Recast Proxy requests the download URL from the catalog. The URL to the Azure storage account uses a short-lived SAS token.

6. The Recast Proxy downloads the ZIP file. After download, the hash checksum is calculated.

7. If the checksum matches the value received from the catalog, Application Manager continues to create applications and deployments for ConfigMgr or Intune.